UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P189

Nortel Networks Alteon Switched Firewall

Version 2.0.3.0
running on specified platforms

Issue 1.0

August 2003

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
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

Alteon Switched Firewall Version 2.0.3.0, from Nortel Networks Ltd, is an accelerated firewall that provides security and controlled supervision of traffic passing between connected networks. It incorporates a FireWall Module of the 'Check Point VPN-1/FireWall-1 Next Generation' product from Check Point Software Technologies Ltd.

Nortel Networks Alteon Switched Firewall Version 2.0.3.0 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 C.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body, UK IT Security Evaluation and Certification Scheme
Date authorised	14 August 2003

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

AIM	Accelerator Interface Module
API	Application Programming Interface
ASF	Alteon Switched Firewall
BBI	Browser Based Interface
CC	Common Criteria
CD-ROM	Compact Disk - Read Only Memory
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CLI	Command Line Interface
CVP	Content Vectoring Protocol
EAL	Evaluation Assurance Level
EDS	Electronic Data Systems Ltd
ETR	Evaluation Technical Report
FP	Feature Pack
FTP	File Transfer Protocol
GUI	Graphical User Interface
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MIME	Multi-purpose Internet Mail Extensions
NAAP	Nortel Appliance Acceleration Protocol
NAT	Network Address Translation
NG	Next Generation
NIC	Network Interface Card
OS	Operating System
SFA	Switched Firewall Accelerator
SFD	Switched Firewall Director
SFR	Security Functional Requirement
SIC	Secure Internal Communication
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SoF	Strength of Function
SSH	Secure Shell
SVN	Secure Virtual Network
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UKSP	United Kingdom Scheme Publication
VLAN	Virtual Local Area Network
VNIC	Virtual Network Interface Card
VPN	Virtual Private Network

(This page is intentionally left blank)

REFERENCES

a. Common Criteria EAL4 Evaluation Alteon Switched Firewall (Version 2.0.3.0) Security Target,
Nortel Networks Ltd,
NortelASF-ST-1.2, Issue 1.2, 3 June 2003.

b. Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
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 5.0, July 2002.

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. Task LFD/T320 Evaluation Technical Report,
EDS CLEF,
P19851/EVAL/R-02/01, Issue 1.0, April 2003.

i. Letter: LFD/T320 Response To ETR Review,
EDS CLEF,
P19851/EVAL/A-02/09, 29 April 2003.

j. Letter: LFD/T320 Response To ETR Review – Further S/W Information,
EDS CLEF,
P19851/EVAL/A-02/10, 1 May 2003.

k. Letter: LFD/T320 Response To ETR and ST Complete Review,
EDS CLEF,
P19851/EVAL/A-02/11, 28 May 2003.

l. Letter: LFD/T320 Response To Further Questions,
EDS CLEF,
P19851/EVAL/A-02/13, 23 July 2003.

m. Common Criteria Certification Report No. P172: Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1),
UK IT Security Evaluation and Certification Scheme,
Issue 2.0, February 2003.

n. Alteon Switched Firewall, Release 2.0.3 - Installation and User's Guide,
Nortel Networks Ltd,
Part No. 212535-C, October 2002.

o. Alteon Switched Firewall, Release 2.0.3 - Installation and User's Guide Addendum: Nortel Networks Common Criteria Alteon Switched Firewall Software,
Nortel Networks Ltd,
Part No. 215287-A Rev01, May 2003.

p. Alteon Switched Firewall, Release 2.0.3 - Release Notes,
Nortel Networks Ltd,
Part No. 213028-E, November 2002.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Alteon Switched Firewall (ASF) Version 2.0.3.0 to the Sponsor, Nortel Networks Ltd, 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 Alteon Switched Firewall, Version 2.0.3.0 (also known as 2.0.3). The product is also described in this report as the Target of Evaluation (TOE).

4. The Developer was Nortel Networks Ltd.

5. The TOE consists of two components (i.e. a Switched Firewall Director (SFD) and a Switched Firewall Accelerator (SFA)), which each comprise software running on dedicated hardware platforms.

6. The SFD incorporates a built-in 'FireWall Module' of the 'Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 3 (FP3)' product from Check Point Software Technologies Ltd. For ease of use, this document hereinafter generally refers to:

- that manufacturer as 'Check Point'
- that product as 'Check Point VPN-1/FireWall-1'
- that module as incorporated into the TOE's 'Check Point FireWall Module'

N.B. A previous version of that product (i.e. Check Point VPN-1/FireWall-1 NG FP1) had previously been evaluated to CC EAL4 (see Certification Report [m]). However the scope of that previous evaluation had intentionally excluded some components of the 'FireWall Module' (e.g. its 'SecureXL module', which provides an Application Programming Interface (API) to enable the 'FireWall Module' to support the use of third-party accelerators such as the SFA).

7. The SFA is a Nortel Networks Alteon WebSwitch, running only custom ASF software, to accelerate sessions offloaded by the SFD.

8. The TOE is intended to be used as a firewall, to provide security and controlled supervision of traffic passing between connected networks. It uses the 'Stateful Inspection' technology of Check Point VPN-1/FireWall-1 to handle security policies, inspect packets and ensure that only communications from permitted hosts, accessing services permitted for those hosts, are allowed to pass.

9. The TOE is configured and generally administered by means of a remote connection to a Check Point VPN-1/FireWall-1 Management Server.

10. Annex A provides details of the evaluated configuration of the TOE, including its supporting guidance documentation.

11. Annex B provides an overview of the security architecture of the product.

TOE Scope

12. The security functionality provided by the TOE is described in the Security Target [a]. It includes the functionality to:

a. Enforce administration of the firewall, by commands originating from a Check Point VPN-1/FireWall-1 Management Server and its associated Management Client Graphical User Interface (GUI). This includes the ability to start/stop the firewall, elicit status reports from the firewall, and install and revise the firewall security policies.

b. Enforce firewall security policies for allowing and blocking traffic, based on the origin and/or destination of packets and the service requested.

c. Enforce firewall security policies for active and passive Network Address Translation (NAT).

d. Protect against network address spoofing attacks.

e. Protect against Internet Protocol (IP) fragmentation and source routing attacks.

f. Invoke a Secure Internal Communication (SIC) facility to establish a trusted (i.e. encrypted) communication channel between the TOE and a Check Point VPN-1/ FireWall-1 Management Server.

g. Invoke the services of external Security Server(s), to enforce:

   i. authentication of subscribers by an external server (via a Lightweight Directory Access Protocol (LDAP) interface); and

   ii. analysis of packet contents by an external server (via a Content Vectoring Protocol (CVP) compliant interface).

h. Invoke a Virtual Private Network (VPN) facility to establish a trusted (i.e. encrypted) communication channel, over an untrusted network, between the TOE and external VPN-enabled clients.

i. Generate audit reports and alerts as specified by firewall security policies, and transmit those audit reports to a Check Point VPN-1/FireWall-1 Management Server.

N.B. The above Check Point VPN-1/FireWall-1 Management Server (and its associated Management Client), the Security Server(s) services, the SIC and the VPN-enabled clients are all in the TOE's IT environment.

13. Regarding the above functionality, the following were outside the scope of the evaluation:

- authentication mechanisms
- SIC mechanisms
- VPN mechanisms
- LDAP server
- content verification server
- service servers (e.g. File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP))

14. Any functionality that did not correspond with the TOE Security Functions (TSF), defined in the Security Target [a], was outside the scope of the evaluation.

15. The following were also outside the scope of the evaluation:

a. Remote management of the TOE (other than via a Check Point VPN-1/FireWall-1 Management Server), i.e. by using the product's telnet, Simple Network Management Protocol (SNMP), Secure Shell (SSH) or Web Browser Based Interfaces (BBIs).

b. Configurations consisting of more than a single SFD and a single SFA.

c. Configurations that bypass inspection by the Check Point FireWall Module, i.e. by allowing processing of traffic by the SFA directly prior to processing by the SFD, including:

i. configuration of port filters; and

ii. configuration of multiple IP interfaces on ports that share a Virtual Local Area Network (VLAN), i.e. allowing bridging of traffic within a VLAN.

Protection Profile Conformance

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

Assurance

17. The Security Target [a] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL4 was used.

18. CC Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

19. The minimum Strength of Function (SoF) claimed for the TOE overall was SoF-Medium.

20. For the product, the only probabilistic or permutational mechanisms were the authentication and cryptographic mechanisms. The Security Target [a] specified these as part of the security requirements for the TOE's IT environment, i.e. they were outside the scope of the evaluation.

21. Hence no SoF was claimed for any of specific security functions, as none of those functions was realised by probabilistic or permutational mechanisms.

Security Policy

22. The TOE Security Policy may be deduced from the Security Target [a].

23. There are no Organisational Security Policies with which the TOE must comply.

Security Claims

24. The Security Target [a] fully specified the TOE's security objectives, the threats that the objectives counter, the Security Functional Requirements (SFRs) and the security functions to elaborate the objectives.

25. With the exception of EDT_ITT.1(1) and EDT_ITT.1(2), all of the SFRs were 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) were fully defined in the Security Target [a].

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

- access control
- remote supervision
- data exchange
- SIC
- audit

Evaluation Conduct

27. The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme, as described in United Kingdom Scheme Publication (UKSP) 01 and 02 [e, f]. The Scheme has established a Certification Body which is managed by the Communications-Electronics Security Group (CESG) 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 that Arrangement.

28. 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.

29. To ensure that the Security Target [a] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline.

30. The evaluation was performed in accordance with the requirements specified in:

- the CC Part 3 [d]
- the Common Evaluation Methodology (CEM) [g]
- the appropriate CC interpretations

31. Some results were reused from the previous evaluation of Check Point VPN-1/FireWall-1 NG FP1 to CC EAL4 (see Certification Report [m]), where such results complied with the above requirements and were valid for the TOE.

32. The Certification Body monitored the evaluation, which was performed by the EDS Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [h] to the Certification Body in April 2003. Following the CLEF's responses [i - l] to the Certification Body's requests for clarification, the Certification Body then produced this Certification Report.

General Points

33. 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 is specified in Annex A. Prospective consumers are advised to check that it matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

34. 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 report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this Certification Report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether such patches have been evaluated and certified.

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

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

36. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [h] under the CC Part 3 [d] headings.

37. The following sections note considerations that are of particular relevance to consumers of the TOE.

Delivery

38. On receipt of the TOE, the consumer should check that the evaluated version has been supplied and that the security of the TOE has not been compromised during delivery.

39. Consumers obtain the TOE software by downloading it as a TOE image file from Check Point's downloads website (i.e. at http://www.checkpoint.com/techsupport/downloads.html). (N.B. The TOE is not available from Nortel's website.)

40. Secure delivery of the TOE to the consumer is by the following method:

a. The consumer registers on Nortel's website and downloads a softcopy of:

i. The ASF Release Notes [p].

ii. The ASF Installation and User's Guide [n].

iii. The ASF Installation and User's Guide Addendum [o].

b. The consumer obtains a valid user account and password to access Check Point's downloads website, then follows the instructions in ASF Installation and User's Guide Addendum [o].

c. The consumer downloads the TOE image file (namely: tng-2.0.3.0_FP3-boot.iso) from Check Point's website, verifies its authenticity by comparing its MD5 checksum against the MD5 checksum contained in the ASF Installation and User's Guide Addendum [o] (namely: 2454e34379d5f206564590e2bc3316ea), then creates a bootable CD-ROM.

41. The ASF Installation and User's Guide Addendum [o] describes:

a. The procedures for maintaining security when distributing versions of the TOE.

b. How those procedures provide for the detection of modifications and discrepancies between the Developer's master copy and the version of the TOE received by the consumer, including detection of attempted masquerading. Detection is achieved through MD5 checksum verification of the downloaded image file.

Installation and Guidance Documentation

42. Secure installation, generation and start-up of the TOE are described in the ASF Installation and User's Guide [n] and the ASF Installation and User's Guide Addendum [o].

43. The ASF Installation and User's Guide [n] describes the steps for:

- installing the authenticated, downloaded software from a bootable CD-ROM
- initial setup, including configuring licences and interfaces
- configuring and installing firewall security policies

44. All human interaction with the TOE is by authorised administrators. Administrator guidance for the TOE is provided in the following documents:

- ASF Installation and User's Guide [n]
- ASF Installation and User's Guide Addendum [o]
- ASF Release Notes [p]

45. There are no non-privileged users or direct users of the TOE; the only other 'users' are those interacting with IP sessions controlled by the TOE (i.e. 'subscribers'). Hence user guidance is not applicable to the TOE.

Strength of Function

46. The SoF claim for the TOE was as given above under "Strength of Function Claims".

47. 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 for the TOE was upheld.

48. The Evaluators confirmed that the only probabilistic or permutational mechanisms were the authentication and encryption mechanisms, and that these were in the TOE's IT environment.

Vulnerability Analysis

49. 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

50. After due consideration of the ETR [h] produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that Nortel Networks Alteon Switched Firewall Version 2.0.3.0 meets the Common Criteria Part 3 [d] conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 [c] extended functionality when running on the platforms specified in Annex C.

51. 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

52. Prospective consumers 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 certain aspects (e.g. authentication, encryption) were outside the scope of the evaluation, as stated above under "TOE Scope" and "Strength of Function Claims".

53. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further information given above under "TOE Scope" and "Evaluation Findings".

54. The TOE should be used in accordance with a number of environmental considerations, as specified in Chapter 3 of the Security Target [a]. Particular care should be taken to ensure that the TOE is delivered, installed, configured and used in accordance with the supporting guidance documentation [n - p] included in the evaluated configuration. The above "Evaluation Findings" also include a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

55. The Security Target [a] describes two modes of operation of the product (i.e. accelerated mode and non-accelerated mode). Prospective consumers should note that the evaluated configuration of the TOE requires its operation in accelerated mode only, in accordance with the ASF Installation and User's Guide Addendum [o].

56. The CC EAL4 Certification Report for Check Point VPN-1/FireWall-1 NG FP1 [m] made recommendations regarding that product. A number of those recommendations are relevant to the use of that product in any environment. Hence the following are applicable to the ASF TOE:

a. Prospective consumers of the TOE should note that the underlying hardware platforms are required to function correctly, in order to support the method of use assumptions that contribute to the secure operation of the TOE.

b. Administrators of the TOE should be aware that Check Point VPN-1/FireWall-1 does not counter the threat that it could be bypassed by connecting the internal network directly to an external network.

c. Administrators of the TOE should ensure that it is placed in a physically secure environment, to which only authorised personnel have access, and should ensure that

internal users are prevented from connecting their workstations or servers to the external network by any link (e.g. a modem) that does not pass through the TOE.

d. Prospective consumers of the TOE should note that the administrators of Check Point VPN-1/FireWall-1 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) should be taken to counter those threats.

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

f. Administrators of the TOE should be aware that a firewall does not prevent malicious users on the internal network from colluding with hostile attackers on an external network, if those malicious users are authorised to access and send the information to external hosts.

g. Administrators of the TOE should regularly inspect the TOE's audit trails. They should also regularly inspect the firewall security policies to ensure that they remain correct.

h. 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.

i. Prospective consumers of the TOE should note that the TOE, in common with similar firewalls, does not counter the threat of session hijacking (i.e. an external attacker taking over an authenticated session initiated by another external host).

j. To reduce the potential impact of session hijacking, 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(s). Corresponding operational procedures to quarantine such software may also be required.

k. To detect whether session hijacking 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.

l. Prospective 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 Multi-purpose Internet Mail Extensions (MIME)-encoded attachments within SMTP messages should also be disabled.

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

   Nortel Networks Alteon Switched Firewall Version 2.0.3.0

TOE Documentation

2. The guidance documents evaluated were:

   - ASF Installation and User's Guide [n]
   - ASF Installation and User's Guide Addendum [o]
   - ASF Release Notes [p]

3. Further discussion of the guidance documents is given in Section II under the heading "Installation and Guidance Documentation".

TOE Configuration

4. The TOE comprised a single SFD connected to a single SFA.

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

6. The TOE software was obtained as a single image file, compiled specifically for execution on each particular hardware platform. During installation of the TOE software, the specific hardware platform(s) were identified and the appropriate code was then automatically loaded.

7. The SFD software included the following Check Point software:

   a. SVN Foundation module, Version NG, FP3, Build 53267.

   b. VPN-1/FireWall-1 module, Version NG, FP3, Build 53225.

   c. Secure XL module, Build 10.0.0.

   d. Secure XL Device module, Build 2000300.

   e. FireWall-1 API module, Version 2.1 (30/9/2002).

   f. Accelerator API module, Version 1.50 (1/5/2002).

   g. File 'FP3/cpinfo'. (This was an independent application that collected statistics and configuration information from the firewall for support and maintenance purposes.)

8. The SFA software included no Check Point software.

9. For the purposes of the evaluation, all of the TOE's software (including all of its included Check Point software) was TOE Security Policy (TSP)-enforcing.

Environmental Configuration

10. The TOE executes on dedicated ASF hardware, consisting of an SFD hardware platform and a separate SFA hardware platform (which are packaged for installation into a standard rack), as shown below:

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

11. The SFD and SFA hardware platforms are generic components that are customised by the TOE software.

12. The SFD hardware platform is based on a standard Intel x86 based PC (i.e. a Dell PowerEdge Model 1650 Server). The only differences between the two models (i.e. 5008 and 5010) are their amount of installed memory and their interface capabilities. The SFD hardware platform includes a hard drive, a CD-ROM drive (used to install the TOE) and a floppy disk drive which are both located behind a lockable bezel, and the following hardware connections:

a. A serial port, for connecting a terminal or a terminal emulator, to provide access for system initial configuration via a Unix style CLI. (The capability to collect system information and statistics via this CLI was not used for the evaluation of the TOE.)

b. A PS/2 port for a keyboard and a video port for a monitor, which provide an alternative to the above serial port for local access to the ASF.

c. For the 5010, a high speed (1000Base-SX Gigabit Ethernet) fibre-optic port used to provide the physical connection with a compatible SFA hardware platform.

d. For the 5008, a high-speed (10/100Base-T) copper Ethernet port is used to provide the physical connection with a compatible SFA hardware platform.

13. The SFA hardware platform is hosted on proprietary Nortel Alteon 5700, 5600, 5400 and 5300 ‘intelligent switches’. The only differences between the four models are their amount of installed memory and their interface capabilities. The SFA hardware platform includes the following hardware connections, whose configuration for the TOE is specified in the ASF Installation and User’s Guide Addendum [o]:

a. A serial port, for the console operator, used only for diagnostics and recovery as directed by Nortel’s technical support. (It was therefore not used for the evaluation of the TOE.)

b. For the SFA 5700 and the 5600: a set of nine paired Ethernet ports, each pair consisting of one 10/100Base-T copper Ethernet port and one 1000Base-SX Gigabit fibre-optic Ethernet port.

c. For the SFA 5400 and 5300: eight 10/100Base-T copper Ethernet ports and one 1000Base-SX Gigabit fibre-optic Ethernet port.

14. Regarding the actual NICs installed in the evaluated configuration of the TOE:

    a. For the SFD hardware platforms:

        i. The integrated NICs were 'Dual integrated Intel Pro/1000 XT', which were standard on the Dell 1650 Server platform, for both the 5010 and the 5008.

        ii. The only non-integrated NIC was the '3COM 3C985 Gigabit Ethernet' NIC, which was installed only on the 5010.

    b. The SFA hardware platforms were Nortel Networks bespoke gigabit switches, i.e. the SFA itself acted as an accelerated NIC.

15. The device driver software for the SFD and SFA is provided as part of the TOE image file; at boot time, the installed NICs are detected and the appropriate device drivers are loaded.

16. The TOE security environment assumptions are described in the Security Target [a], either as 'environment' assumptions or as 'method of use' assumptions.

17. Further details of the TOE's environmental configuration are provided in Chapter I under the heading "TOE Scope".

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

Introduction

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

Architectural Features

2. The product, consisting of software running on dedicated hardware platforms, is a high performance firewall that provides security and controlled supervision of traffic passing between connected networks. It uses the 'Stateful Inspection' technology of Check Point VPN-1/ FireWall-1 to inspect packets and to ensure that only communications from permitted hosts, accessing services permitted for those hosts, are allowed to pass.

3. The product includes a 'Check Point FireWall Module', which incorporates an accelerated (but otherwise standard) FireWall Module from Check Point VPN-1/FireWall-1. That module is responsible for the firewall functionality, i.e. handling security policies, inspecting network traffic, and blocking unwanted communications.

4. The product can also invoke a VPN to establish a secure, trusted communications channel over an unsecured network.

5. Administrators are the only users permitted to access the firewall interactively. The only other users are those interacting with IP sessions controlled by the product (i.e. subscribers).

6. Administrators perform management and administration of the product, using a separate (i.e. external) Check Point VPN-1/FireWall-1 Management Server and its associated Management Client GUI. Management and administration is independent of the network traffic flowing through the firewall, however the traffic permitted to flow is controlled and monitored by the firewall security policies that are downloaded by an administrator.

7. Administrators also configure the product's interfaces and ports locally via a CLI, using a keyboard and monitor.

8. The Check Point FireWall Module supervises the traffic passing between networks physically connected to the product and belonging to the complete 'IP' family of protocols. Supervision is based on information contained in protocol headers and the firewall security policies for the product's computer system, including state information derived from one or more associated packets.

9. The Check Point FireWall Module performs policy checking for every new connection request, manages the connection table and specifies the rules for handling subsequent packets in a session. Once a session is active, the policy checking for packets is handled by the SFA. Thus, after the SFD inspection engine accepts the setup packets in a session, subsequent packets belonging to the session are inspected by the SFA without involving the SFD. This approach is intended to accelerate significantly the firewall performance.

Design Subsystems

10. The product comprises two major components:

- the SFD
- the SFA

11. The SFD software consists of the following design components:

a. Linux Operating System (OS) (stripped down version): This is a customised Unix operating system based on standard Red Hat Linux 6.2 with 2.2.18 kernel, which has been stripped down, modified and enhanced to fulfil the requirements of the SFD.

b. Nortel Appliance Acceleration Protocol (NAAP) Driver: This provides a kernel API (which is used by the Accelerator Interface Module to send control messages to the SFA) and a user mode API (which is used by any user process that needs to communicate with the SFA) for the NAAP.

c. Accelerator Interface Module (AIM): During acceleration, this implements the Check Point accelerated Network Interface Card (NIC) interface as defined by the SecureXL software, allowing the Check Point FireWall Module to offload sessions. This also communicates new or updated session information to the SFA using NAAP, and implements certain processing of packets.

d. Virtual Network Interface Card (VNIC) Processing Module: This accepts packets from the SFA through the NAAP data protocol, unwraps them and makes them enter the Linux OS (and thus the Check Point FireWall module) through the VNIC netdevice corresponding to the port/VLAN on which the packet was originally received by the SFA. This also captures packets transmitted to each VNIC netdevice and sends them to the SFA for retransmission.

e. Check Point FireWall Module: This incorporates the 'FireWall Module' (comprising the Check Point software specified above in Annex A, Paragraph 7). This provides communication with the external Check Point VPN-1/FireWall-1 Management Server, inspects packets as per the firewall security policies downloaded from that Management Server, and offloads and manages allowed connections to the SFA using the APIs provided by the SecureXL software. This also supports the establishment of VPNs and connections to external servers, for subscriber authentication and packet content analysis.

f. Single System Image: This provides the base platform upon which the ASF is built. It includes the Linux OS kernel and user mode applications. It also provides the CLI for configuring the SFD.

g. Health Check Daemon: This is a user mode application that checks health-related parameters (e.g. it looks at available memory, disk space, and operation of subprograms). It provides the SFD health report for the NAAP heartbeat mechanism between the SFA and the SFD.

h. Configuration Daemon: This is a user mode application that listens for changes in the Registry and applies the changes to the SFA and the SFD. It is also responsible

for broadcasting its own health information and initialising the AIM and VNIC modules.

i. CLI/GUI: This provides a CLI via which the administrator can configure the ASF, in particular its network interfaces.

12. The SFA software consists of the following design components:

a. Firewall Acceleration Processing Module: During acceleration, this processes incoming packets and manages session table entries based on commands from the Check Point FireWall Module.

b. NAAP Protocol Handler: This provides communication between the SFA and the SFD using NAAP messages.

Hardware and Firmware Dependencies

13. 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.

14. For the evaluated configuration of the TOE, the actual NICs installed on the hardware platforms are specified in Annex A under the heading "Environmental Configuration".

TSF Interface

15. The external interfaces, i.e. comprising the TOE Security Functions Interface (TSFI), are as follows:

a. ASF CLI (via the serial ports and/or the keyboard and monitor ports). This external interface provides administrators with a command line to manage and monitor the SFD and the SFA, including starting/stopping the firewall and defining network connectivity in terms of configured VNICs and VLANs.

b. SFA Ports 1 - 5. The default configuration uses ports 1 – 5 for network traffic, but those ports can be reconfigured as required via the ASF CLI. This external interface provides connections to:

i. external networks, on which the ASF will receive incoming traffic and forward outgoing traffic;

ii. external security servers, for authentication of subscribers and analysis of packet contents; and

iii. the Check Point VPN-1/FireWall-1 Management Server, for the transfer of firewall security policies, audit logs and status information via its associated Management Client GUI.

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The Evaluators repeated a sample of 24% of the Developer's tests, to confirm the adequacy of the Developer's testing. The Evaluators determined that it was not necessary to perform the whole sample of tests on each hardware platform, provided that their observed test results were consistent with the Developer's supplied test results, and that those supplied test results were shown to be the same for each of the four hardware platforms.

2. The Evaluators also performed independent functional testing on the TOE, to confirm that it operates as specified.

3. The Evaluators then performed penetration testing, to confirm the SoF claimed in the Security Target [a] for the TOE overall and to confirm that all identified potential vulnerabilities in the TOE have been addressed, i.e. that the TOE in its intended environment has no exploitable vulnerabilities.

4. Security aspects of the TOE's environment relevant to the test environment were met by the use of the Check Point VPN-1/FireWall-1 Management Server software and its associated Management Client software, which was provided on a 'Check Point NG Enterprise Suite FP3' CD-ROM and installed using the standard Check Point VPN-1/FireWall-1 documentation.

Platform Issues

5. The Developer installed and tested the TOE on the four ASF hardware platforms specified in Annex A.

6. The Evaluators performed their sample repeat testing of the TOE, and their independent functional testing of the TOE, across the four ASF hardware platforms specified in Annex A.

7. The Evaluators performed their penetration testing of the TOE on two of those hardware platforms, namely:

- at the Developer's site: ASF 5308 (comprising SFD 5008 and SFA 5300)
- at the CLEF: ASF 5710 (comprising SFD 5010 and SFA 5700)

Note that those two hardware platforms included both of the claimed SFD models, and the highest and lowest specification of the claimed SFA models.

8. The Evaluators were satisfied that their penetration test results obtained on the ASF 5308 and the ASF 5710 were representative of the other two hardware platforms (ASF 5408 and ASF 5610), i.e. that all of the hardware platforms claimed in the Security Target [a] (as tabled above in Annex A under the heading "Environmental Configuration") were fully covered.

(This page is intentionally left blank)