Maintenance Report

NOKIA IP260, IP265, IP350, IP355, IP380, IP385, IP1220, IP1260, IP2250 Firewall/VPN Appliances with Check Point Technologies Incorporated VPN-1/FireWall-1 NGX (R60)

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-7-11-MR
Version: 1.0
Date: 16 November 2005
Pagination: 1 to 2

1 Introduction

On 04 November 2005, Check Point Technologies Incorporated developer of the Target of Evaluation (TOE), the Check Point VPN-1/FireWall-1 NGX (R60), submitted an Impact Analysis Report (IAR) to the CCS Certification Body on behalf of NOKIA, the developer of the NOKIA IP260, IP265, IP350, IP355, IP380, IP385, IP1220, IP1260, IP2250 Firewall/VPN Appliances which incorporate the Check Point Technologies Incorporated VPN-1/FireWall-1 NGX (R60).

The IAR is intended to satisfy requirements outlined in version 1.0 of the Common Criteria document CCIMB-2004-02-009: Assurance Continuity: CCRA Requirements. In accordance with those requirements, the IAR describes the changes made to the NOKIA IP260, IP265, IP350, IP355, IP380, IP385, IP1220, IP1260, IP2250 Firewall/VPN Appliances with Check Point Technologies Incorporated VPN-1/FireWall-1 NGX (R60) (the maintained TOE), hereafter referred to as the NOKIA Firewall/VPN Appliances, the evidence updated as a result of the changes, and the security impact of the changes.

2 Description of changes

The changes listed in the IAR comprise changes made to the Check Point VPN-1/FireWall-1 Next Generation from Feature Pack R55 with HFA_14 to NGX (R60).

The following characterizes the changes implemented in the NOKIA Firewall/VPN Appliances. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the TOE developer to ensure that the assurance in the TOE was maintained. The changes in NOKIA Firewall/VPN Appliances comprise software changes that:

- restore the expected functionality of the TOE (bug fixes); and
- add performance enhancements to the TOE.

3 Description of Changes to the IT Environment

There were no changes to the underlying IT environment.

4 Affected developer evidence

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR, and revised versions of all affected developer evidence were submitted.

Modifications to the security target were made to reflect the new product version.

5 Conclusions

All changes to the TOE were minor features changes and isolated corrections to the product. Through functional and regression testing of the NOKIA Firewall/VPN Appliances, assurance gained in the original TOE certification was maintained. As all of the changes to the TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

6 References

1. Assurance Continuity: CCRA Requirements, CCIMB-2004-02-009, version 1.0, February 2004

2. Technical Oversight for Assurance Continuity of a certified TOE, version 1.0, 18 June 2004

3. Certification Report for the EAL4 Evaluation of the Nokia IP130, IP350, and IP380 Firewall/VPN Appliances with Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation Feature Pack 2