# Certification Report

## EAL 4 Evaluation of Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation Feature Pack 1

Issued by:

**Communications Security Establishment**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**

| | |
|---|---|
| **Evaluation number**: | 383-4-41 |
| **Version**: | 1.0 |
| **Date**: | 12 July 2005 |
| **Pagination**: | i to iii, 1 to 12 |

# DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.2, r256*, for conformance to the *Common Criteria for  Information Technology Security Evaluation, Version 2.2, r256*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

# FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 12 July 2005, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html

This certificate makes reference to Check Point, FireWall-1, VPN-1 and VPN-1 SecureClient which are trademarks or registered trademarks of Check Point Software Technologies Incorporated.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

# TABLE OF CONTENTS

# Executive Summary

The Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation Feature Pack 1, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation.

The VPN-1/FireWall-1 Next Generation Feature Pack 1 provides firewall and Virtual Private Network (VPN) functionality to secure the communications between networks. It also provides the capability to securely manage and configure the product itself. The TOE supervises the traffic, belonging to the complete IP (Internet Protocol) family of protocols, which passes between networks physically connected to the computer system which hosts the TOE. Supervision is based on information contained in the protocol headers and the host computer system, including state information derived from one or more associated packets. The TOE's ability to invoke the VPN when required as per the established security policies was evaluated; however, correct operation of the VPN functionality was not included as a part of this evaluation.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 27 June 2005, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the VPN-1/FireWall-1 Next Generation Feature Pack 1, the security requirements, and the level of confidence (evaluation assurance level) to which the product is intended to satisfy the security requirements. Consumers of the VPN-1/FireWall-1 Next Generation Feature Pack 1 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report[1] for this product provide sufficient evidence that it meets the EAL 4 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 r256* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2 r256*.

The Communications Security Establishment, as the CCS Certification Body, declares that the VPN-1/FireWall-1 Next Generation Feature Pack 1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

# 1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation is the Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation Feature Pack 1.

# 2 TOE Description

The VPN-1/FireWall-1 Next Generation Feature Pack 1 provides firewall and virtual private network functionality to secure the communication between networks. It also provides the capability to securely configure and administer the product itself. The TOE's ability to invoke the VPN when required as per the established security policies was evaluated; however, correct operation of the VPN functionality was not included as a part of this evaluation.

The TOE supervises traffic, belonging to the complete IP (Internet Protocol) family of protocols, which passes between networks physically connected to the computer system which hosts the TOE. Supervision is based on information contained in protocol headers and the host computer system, including state information derived from one or more associated packets. The supervision provided by the product includes the ability to encrypt, authenticate and validate data which travels between selected IP addresses on networks protected by the VPN-1/FireWall-1 Next Generation Feature Pack 1 such that communication is established with authenticated entities. If such capability is required, the confidentiality of data is maintained, preventing unauthorized disclosure and the integrity of the data is assured through the application of an encrypted message digest covering the contents of each data packet.

The TOE may be configured and administered by means of a remote connection to the VPN-1/FireWall-1 Next Generation Feature Pack 1 Management Server and management Graphical User Interface (GUI). This remote connection is protected using encryption. The TOE's ability to invoke the establishment of a secure remote connection was evaluated; however, the cryptographic functionality was not included as a part of the evaluated functionality.

The TOE must be used in a "trusted configuration". Some of the security functionality of the TOE requires separate but communicating instances of the product to execute on separate Workstations or Servers. A trusted configuration of the product:

- Executes on any computer system from the family of Workstations and Servers which support the SUN Solaris 8.0 or Windows 2000 operating systems.

- Executes on a computer system which supports up to 128 port connections.

- Consists of:

    - A Management Server which resides on a protected Local Area Network (LAN).

    - A GUI which resides on a separate workstation running the Windows 2000 operating system and which is part of the same protected LAN as the Management Server.

    - A VPN-1 SecureClient which resides on a remote machine outside of the protected LAN but which is part of the corporate network. The VPN-1 SecureClient component must reside on a machine running the Windows 2000 operating system.

    - A number of VPN-1/FireWall-1 Modules which may or may not reside on the same protected LAN as the Management Server.

    - A Policy Server which is installed on a VPN-1/FireWall-1 machine which resides on the same protected LAN as the Management Server.

- Is configured, controlled and monitored using the Graphical User Interface which communicates with the Management Server. The Management Server in turn configures the FireWall-1 modules and via the Policy Server downloads the Desktop Policy to the SecureClient(s).

- Has been installed, configured and started as described in the Check Point Next Generation Getting Started Guide.

# 3 Evaluated Security Functionality

The complete list of evaluated security functionality for the VPN-1/FireWall-1 Next Generation Feature Pack 1 is identified in Section 5 of the Security Target.

# 4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

| | |
|---|---|
| Title: | Common Criteria EAL4 Evaluation, Check Point Software Technologies Inc., VPN-1/FireWall-1 Next Generation (Feature Pack 1) |
| Version: | 1.9.3 |
| Date: | 3 June 2005 |

# 5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2, r256*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2, r256*.

The VPN-1/FireWall-1 Next Generation Feature Pack 1 is:

a. Common Criteria Part 2 extended, with security functional requirements based upon functional components in Part 2;

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c. Common Criteria EAL 4 conformant, with all the security assurance requirements in the EAL 4 package.

# 6 Security Policies

The VPN-1/FireWall-1 Next Generation Feature Pack 1 Security Policies are identified in the ST. The following statements are representative of the Security Policies.

## 6.1 Network Traffic Flow Control

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:

a. all of the information security attribute values are unambiguously permitted by the information flow control 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

b. the presumed address of the destination subject, in the information, translates to an address on some other connected network.

## 6.2 Secure Internal Communications Flow Control

Secure use of the TOE requires a secure internal communications channel between TOE modules and the TOE's Management Server module. The TOE imposes a requirement on its IT environment to provide this secure internal communications channel. This requirement is met via an implementation of the standard Transport Layer Security (TLS) protocol defined in RFC 2246. To meet the requirement, the IT environment shall permit an information flow between a TOE module and the Management Server module if based on the X.509 certificates installed upon these components, a trusted connection can be negotiated via the TLS protocol.

### 6.3 Virtual Private Network

The TOE supports Virtual Private Network (VPN) connections between the TOE and clients running the SecureClient module. The TOE imposes upon its IT environment a requirement for cryptographic functionality to support the VPN functionality. The requirement is met via an implementation of the standard IPSec protocol. To meet the requirement, the IT environment shall permit an information flow between the TOE and a client running the SecureClient module if an encrypted connection can be established via the IPSec protocols.

## 7 Assumptions and Clarification of Scope

Consumers of the VPN-1/FireWall-1 Next Generation Feature Pack 1 product should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the product.

### 7.1 Secure Usage Assumptions

It is assumed that the product is installed, configured, operated and maintained in accordance with the procedures and guidelines defined in the Check Point Next Generation Getting Started Guide and the other Check Point documentation listed in Section 10 of this report.

It is further assumed that:

a. the product is configured with the minimum of operating system features installed and the minimum of operating system features enabled to permit operation of the product;

b. computer system privileges are assigned to programs in accordance with the site security policy;

c. physical security controls prevent unauthorized access to the product, management server, consoles and system devices;

d. the product is configured with user accounts for authorized administrators only;

e. the administrators' use of privileged accounts conforms to the site security policy;

f. restrictions imposed by site security policies concerning the choice of system passwords are enforced by the computer system configuration;

g. guidelines consistent with the site security policy are followed for operating system controlled ownership and restrictions on access to operating system and product directories and files;

h. computer system backup and recovery procedures are followed which are sufficient to restore the product to a secure state after a failure of the product;

i. appropriate use is made of the management server's facilities to examine the audit log file and ensure that the size of the log file does not exceed the file system size limits;

j. the firewall security policy will be configured to deny all network connections aimed directly at the firewall host, except from the management server; and

k. administrators have knowledge of the product, the host operating systems and networking technologies.

### 7.2 Environmental Assumptions

It is assumed that the computer system hosting elements of the TOE, along with any associated devices, functions correctly.

It is assumed that the product is operated in a 'trusted configuration' as defined in the Security Target.

It is assumed that the product is adequately protected against physical threats.

### 7.3 Clarification of Scope

The VPN-1/FireWall-1 Next Generation Feature Pack 1 can not prevent authorized administrators from carelessly configuring the TOE such that the information flow control policy is compromised.

## 8 Architectural Information

The TOE consists of a number of separate but communicating instances of the product running on separate workstations or servers. The TOE is comprised of several software modules that are further detailed in Section 9 of this report, *Evaluated Configuration*.

## 9 Evaluated Configuration

The evaluated configuration of the TOE consists of:

- The Check Point Management Server module running on a system with either the SUN Solaris 8.0 or Windows 2000 operating system and residing on a secure LAN.

- The Check Point Graphical User Interface module running on a system with the Windows 2000 operating system and residing on the same protected LAN as the Management Server.

- The Check Point VPN-1 SecureClient module running on a system with the Windows 2000 operating system and residing outside of the protected LAN.

- One or more Check Point VPN-1/FireWall-1 FP1 modules running on systems with either the SUN Solaris 8.0 or Windows 2000 operating systems and residing either on the same protected LAN as the Management Server or outside of the protected LAN.

- The Check Point Policy Server module running on a system which also has a VPN-1/FireWall-1 FP1 module installed and which resides on the protected LAN.

## 10 Documentation

a. Check Point Next Generation Getting Started Guide, Part No. 700239, June 2001.

b. Check Point Next Generation Management Guide, Part No. 700348, November 2001.

c. Check Point Next Generation FireWall-1 Guide, Part No. 700349, November 2001.

d. Check Point Reference Guide, NG, Part No. 700351, November 2001.

e. Check Point User Management, NG, Part No. 700268, June 2001.

f. Check Point Virtual Private Networks, NG, Part No. 700350, November 2001.

g. Check Point Desktop Security, NG, Part No. 700361, November 2001.

h. Check Point VPN-1/FireWall-1 NG, FP1, System Generation/Installation Guide for ITSEC E3, Version 1,2, 3 March 2002.

i. Check Pint VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1) Release Notes, November 2001.

## 11 Evaluation Analysis Activities

In some areas of the evaluation (notably configuration management, design documentation and life cycle support), the evaluators considered the results of a previous evaluation of the TOE (see References d and e in Section 16) and where appropriate reused evidence from the previous evaluation. However to ensure that the current evaluation considered up-to-date test and vulnerability information, the testing and vulnerability analysis work units were repeated completely without any reuse of results from the previous evaluation.

The evaluation analysis activities involved a structured evaluation of the VPN-1/FireWall-1 Next Generation Feature Pack 1, including the following areas:

**Configuration management:** The evaluators performed an analysis of the VPN-1/FireWall-1 Next Generation Feature Pack 1 development environment and associated documentation. The evaluators determined that the configuration items which comprise the TOE are clearly identified and labelled and that control is exercised over all modifications to the configuration items. The analysis was supplemented by a site visit to the development offices of Check Point Software Technologies Incorporated. The site visit confirmed that the configuration control procedures in place at Check Point Software Technologies Incorporated are mature and stable.

**Secure delivery and operation:** The evaluators examined the delivery documentation for the VPN-1/FireWall-1 Next Generation Feature Pack 1 product and determined that it is adequate to maintain the integrity of the TOE during delivery to the consumer. The evaluators examined and tested the installation, generation and start-up procedures for the TOE and determined that they are complete and sufficiently detailed and result in a secure installation of the TOE.

**Design documentation:** The evaluators reviewed the design documentation for the VPN-1/FireWall-1 Next Generation Feature Pack 1 including the functional specification, high-level design, low level design, security policy model and source code. In addition, the evaluators conducted a site visit to the Check Point Software Technologies Incorporated development facility in Israel. The evaluators concluded that the design documents completely and accurately describe all interfaces and security functions of the product and are internally consistent.

**Guidance documents:** The evaluators reviewed the VPN-1/FireWall-1 Next Generation Feature Pack 1 guidance documents and determined that they clearly and unambiguously describe how to securely use and administer the product and that they are consistent with the other documents supplied for the evaluation.

**Life-cycle support:** The evaluator reviewed the life cycle support documentation for the TOE. The evaluator concluded that the developers have used well-defined development tools which yield consistent and predictable results. The evaluators also determined that the developers have used a well defined and documented life cycle model for the TOE. The evaluators also concluded that the development security measures applied by the developers provide sufficient assurance of the confidentiality and integrity of the TOE.

**Vulnerability assessment:** The evaluator's reviewed the developer's vulnerability analysis and performed an independent vulnerability analysis to develop penetration tests for the TOE. Refer to the next section of the report for additional details of the vulnerability testing.

All these evaluation activities resulted in **PASS** verdicts.

# 12 ITS Product Testing

The evaluators reviewed the testing evidence produced by the developers and the independent testing conducted during the previous evaluation of the TOE. In addition, the evaluators carried out independent functional and vulnerability testing of the TOE.

## 12.1 Assessing Developer Tests

The evaluators confirmed that the developer met their testing responsibilities for the TOE by examining the developer test evidence and reviewing the developer test results as well as examining the results of independent testing conducted during a previous evaluation of the TOE.

The evaluators reviewed the developer's analysis of test coverage and depth and found them to be complete and accurate. There is a complete correspondence between the tests identified in the developer's test documentation and the functional specification and high-level design.

## 12.2 Independent Functional Testing

During this evaluation, the evaluators developed functional tests to augment developer testing of select TOE security functions. Additionally, given the change in the evaluated configuration from the original evaluation the evaluators repeated a representative subset of developer test procedures on the Windows 2000 platform. The subset of tests provided coverage of all TOE security functions.

Actual results achieved during the independent functional testing matched the developer's expected results and provided assurance of the correct operation of the TOE on both the Sun Solaris 8 and Windows 2000 platforms.

## 12.3 Independent Vulnerability Testing

After reviewing the developers test and vulnerability analysis evidence, the evaluators employed a flaw hypothesis methodology to develop a list of potentially exploitable vulnerabilities of the TOE in the following areas:

a. Generic vulnerabilities;

b. Bypassing;

c. Tampering;

d. Direct attacks; and

e. Misuse.

Test cases were then developed, documented and executed in an attempt to exploit the postulated vulnerabilities. Extensive use was made of public domain network attack tools in an attempt to compromise the TOE. A public domain search of known vulnerabilities revealed several potential vulnerabilities for the TOE. All of these potential vulnerabilities were first exposed after the original evaluation of the TOE. In each case it was the assessment of the evaluators that a high attack potential was required in order to exploit any of these vulnerabilities. Therefore, while the evaluated configuration of the product does contain residual vulnerabilities, they are not exploitable in the intended environment.

The independent penetration testing did not uncover any new vulnerabilities in the TOE.

### 12.4 Conduct of Testing

The TOE was installed and configured in the IT Security Evaluation and Testing (ITSET) facility at Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario. All penetration and vulnerability testing was conducted at this facility. The CCS Certification Body witnessed a portion of the testing.

### 12.5 Test Results

All independent functional, penetration and vulnerability tests yielded the expected results. No additional exploitable vulnerabilities were uncovered during the testing.

## 13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 4** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the Evaluation Technical Report[2] (ETR).

## 14 Evaluator Comments, Observations and Recommendations

The independent vulnerability analysis conducted during this evaluation revealed a number of vulnerabilities or potential vulnerabilities in several areas of the TOE. All of these vulnerabilities were uncovered after the previous evaluation of the TOE. All of these residual vulnerabilities are assessed as requiring a high attack potential for exploitation. For this reason they are assessed as not exploitable within the intended operating environment of the TOE. More detailed information about the residual vulnerabilities is included in the ETR.

[2] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

# 15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

| Acronym/Abbreviation/Initialization | Description |
|---|---|
| CC | Common Criteria for Information Technology Security Evaluation |
| CCEF | Common Criteria Evaluation Facility |
| CCS | Canadian Common Criteria Evaluation and Certification Scheme |
| CEM | Common Methodology for Information Technology Security Evaluation |
| CR | Certification Report |
| CSE | Communications Security Establishment |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| FP | Feature Pack |
| GUI | Graphical User Interface |
| ISO | International Organisation for Standardisation |
| IT | Information Technology |
| ITSET | Information Technology Security Evaluation and Testing |
| IP | Internet Protocol |
| IPSec | Internet Protocol Security |
| LAN | Local Area Network |
| NG | Next Generation |
| PALCAN | Program for the Accreditation of Laboratories Canada |
| PP | Protection Profile |
| SOF | Strength of Function |
| ST | Security Target |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| VPN | Virtual Private Network |

## 16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-001/002/003, Version 2.2 r256, January 2004.

b) Common Methodology for Information Technology Security Evaluation, CCIMB-2004-01-004, Part 2: Evaluation and Methodology, Version 2.2 r256, January 2004.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) Common Criteria Certification Report No. P172, Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1), running of specified platforms, Issue 2.0, February 2003.

e) Task LFD/T317 (Phase 1) Evaluation Technical Report, Issue 1.0, Doc Ref: P16759/Eval/R-02/01, May 2002.

f) Common Criteria EAL 4 Evaluation, Check Point Software Technologies Inc., VPN-1/FireWall-1 Next Generation (Feature Pack 1), Security Target Issue 1.9.3, 3 June 2005.

g) Evaluation Technical Report (ETR), Check Point VPN-1/FireWall-1, EAL 4 Evaluation, Common Criteria Evaluation Number, 383-4-41, Document No. 1505-000-D002, Version 1.0, 27 June 2005.