National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Check Point VPN-1/Firewall-1 NGX (R60)

Report Number: **CCEVS-VR-06-0033**
Dated: **August 25, 2006**
Version: **1.1**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

Check Point
3A Jabotinsky St., Diamond Tower
Ramat Gan, Israel 52520

Evaluation Personnel:

Science Applications International Corporation CCTL, Columbia, MD
Cynthia Reese (lead evaluator)
Leonard Eaton (evaluator)
Craig Floyd (evaluator)
Michael Boberski (evaluator)
Jean Petty (evaluator)
Michele Rupell (evaluator)

Validation Personnel:

Scott Shorter, Orion Security Solutions
James Donndelinger, Aerospace
John Nilles, Aerospace

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Check Point VPN/FireWall-1 NGX (R60). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of Check Point VPN/FireWall-1 was performed by the Science Applications International Corporation Common Criteria Testing Laboratory in the United States and was completed in August 2006. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Metatron, Ltd. The ETR and test report used in developing this validation report were written by the SAIC CCTL. The evaluation team determined the product to be Part 2 and Part 3 conformant, and concluded that the Common Criteria version 2.2 requirements for Evaluation Assurance Level (EAL) 4 (augmented with Systematic Flaw Remediation) have been met, and furthermore that the ST conforms to the Intrusion Detection System System Protection Profile, Version 1.5, March 9, 2005.

The Check Point VPN/FireWall-1 is a network boundary protection device that provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewall. The TOE provides information flow controls, including traffic filtering, application-level proxies and intrusion detection and prevention capabilities. IPSec VPN functionality encrypts and authenticates network traffic to and from selected peers, in order to protect the traffic from disclosure or modification over untrusted networks. Management can be performed either locally or remotely using the management GUI that is included in the Target of Evaluation (TOE).

Figure 1 illustrates the physical configuration of the TOE and IT Environment (TOE components are shaded in grey).

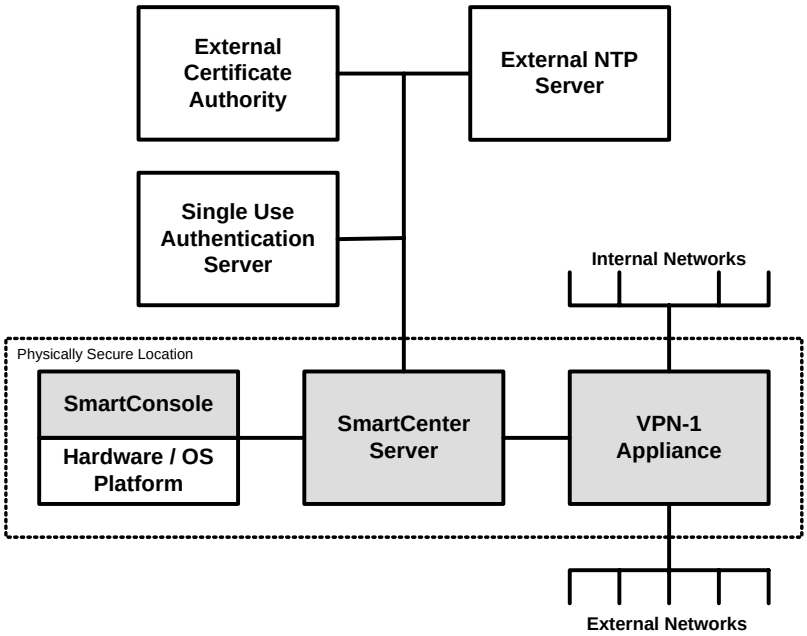

Figure 1 - TOE Hardware Components

In addition to the hardware and software components, the purchase of the Check Point Enterprise Software Subscription plan is required for receiving software upgrades, as part of Check Point's evaluated flaw remediation procedures.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 4 evaluation augmented by Systematic Flaw Remediation. Therefore the validation team concludes that the SAIC CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's listing on the CCEVS Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	The TOE consists of TOE security policy enforcement software running on any of the hardware platforms and operating system combinations listed in Appendix A of the Security Target. The TOE supports the following operating systems: • Check Point SecurePlatform NGX (R60) HFA 03 TOE management software is always installed on a separate platform running the Check Point SecurePlatform operating system, selected from the list given in Section A.1 of the Security Target. TOE software also includes a Management GUI product (SmartConsole) that is installed on a standard PC (outside the

Item	Identifier
	TOE) running a Microsoft Windows operating system.
Security Target	*Check Point VPN-1/FireWall-1 NGX,* ST revision 1.2.2, August 23, 2006
Protection Profiles	*Intrusion Detection System System Protection Profile*, Version 1.5, March 9, 2005
Evaluation Technical Report	*Final Evaluation Technical Report For Check Point Check Point VPN/FireWall-1 NGX*, Version 0.3, August 23, 2006
Conformance Result	CC Part 2 conformant, CC Part 3 conformant, EAL 4 augmented by ALC_FLR.3
Sponsor	Check Point 3A Jabotinsky St., Diamond Tower Ramat Gan, Israel 52520
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
CCEVS Validator(s)	Scott Shorter, Orion Security Solutions James Donndelinger, Aerospace John Nilles, Aerospace

3 Security Policy

The explicit TOE security policy consists of the UNAUTHENTICATED SFP that controls the HTTP and SMTP traffic filter functionality of the firewall, and the AUTHENTICATED SFP that controls FTP and Telnet traffic filter functionality of the firewall, and the TRAFFIC FILTER SFP that is applied to all traffic sent through the TOE.

In addition, the TOE implements the following implied security policies:

- Stateful Inspection
- Security Servers
- Virtual Private Network
- Audit
- Security Management
- Secure Internal Communications
- Identification and Authentication
- TSF Protection

4 Assumptions

The following assumptions about the TOE's operational environment are articulated in the ST:

A.PHYSEC	The TOE is physically secure.
A.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

5 Architectural Information

The high level architecture of the TOE is shown in Figure 2. The Check Point VPN/FireWall-1 Appliance, the rightmost block of the figure, consists of compliance tested hardware, a specially developed Linux operating system with enhanced protections against bypassibility, and the firewall software application.

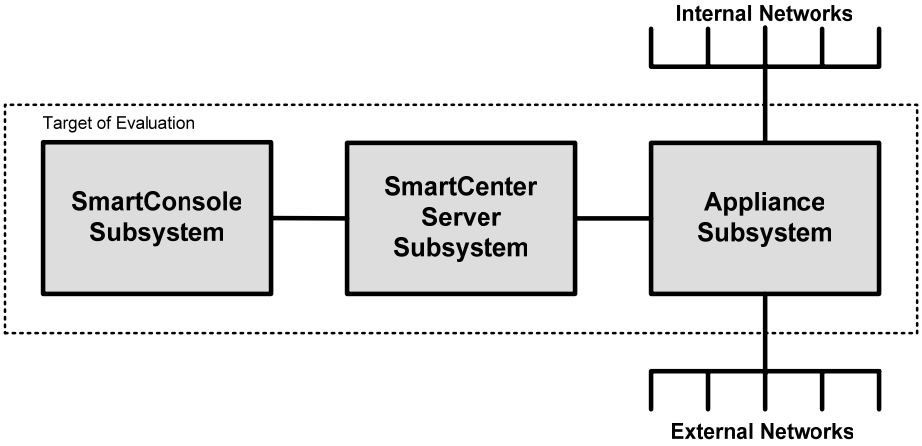

Figure 2 - TOE Architecture

The SmartConsole subsystem is user level software running on a general purpose PC that provides a management GUI that enables authorized administrators to configure the TOE and receive log, alert and system status data. The SmartConsole subsystem consists of the following software applications:

- SmartDashboard: TOE configuration capability
- SmartView Tracker: audit log review capability
- SmartView Monitor: real time TOE status monitoring and alert capability

The SmartCenter Server subsystem is user level software running on a general purpose PC that manages the TOE data, serves as a central point of administration of the TOE, and provides an internal certification authority (ICA) to support Secure Internal Communications (SIC).

The Appliance Subsystem provides all security functionality other than management and audit. In particular, the following security functions are implemented by the Appliance Subsystem:

- Stateful Inspection
- Security Servers

- VPN
- Audit Generation
- User Identification and Authentication
- TSF Protection

6 Documentation

The following documentation is provided with the product:

- CC Evaluated Configuration Installation Guide - NGX (R60), July 2006, Check Point Part No. 701666
- CC Evaluated Configuration Administration Guide - NGX (R60), July 2006, Check Point Part No. 701665
- CC Evaluated Configuration User Guide - NGX (R60), Check Point Part No. 701667, January 2006
- Virtual Private Networks NGX (R60), Check Point Part No. 701308, June 2005
- Firewall and SmartDefense NGX (R60), Check Point Part No. 701318, May 2005
- SmartView Monitor NGX (R60), Check Point Part No. 701311, May 2005
- SmartCenter NGX (R60), Check Point Part No. 701309, June 2005
- Check Point Getting Started Guide NGX (R60), Check Point Part No. 701314, January 2005
- Check Point SecurePlatform/SecurePlatform Pro - NGX (R60), Check Point Part No. 701315, May 2005

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer tested the interfaces identified in the high level design documentation and mapped each test to the security function tested. The scope of the developer tests included all TOE Security Functions. The evaluation team determined that the developer's actual test results matched the expected results and witnessed a subset of the tests. Testing consisted of a suite of automated tests as well as a number of manual tests.

In particular, developer testing contained the following types of tests:

- Stateful Inspection Security Function Tests
    - Anti-spoofing – Demonstrates automatic dropping of packets that do not correspond to the network topology as defined by the administrator
    - Packet Inspection - Demonstrates accept, drop and reject behavior as a function of combination of values of the information flow security attributes
    - Post-Inspect – Demonstrates intrusion detection system analysis and reaction
    - Residual Information Protection – Demonstrates that residual information is not leaked from one packet to another
    - FTP Security Server – Demonstrates the capability to restrict the set of acceptable FTP commands that can traverse the TOE
    - Telnet Security Server – Demonstrates the validation of Telnet option codes
    - HTTP Security Server – Demonstrates the HTTP validation checks performed by the TOE
    - SMTP Security Server – Demonstrates the validation of SMTP traffic and the enforcement of administrator defined restrictions on attachment types and mail size
    - User Authentication – Demonstrates the capability to authenticate FTP and Telnet users via remote authentication server in the IT Environment

- Virtual Private Network Security Function Tests
    - Cryptographic Algorithm – Demonstrates interoperable behavior of the claimed cryptographic algorithms
    - IKE/IPSec – Demonstrates adherence to relevant RFC requirements
    - Audit – Demonstrates the logging of rejected IKE and IPSec packets
- Audit Security Function
    - Traffic Related Audit Generation – Demonstrates selective audit record generation for events and specified logging of security-relevant information
    - Security Server Audit Generation – Demonstrates selective audit record generation for successful and unsuccessful authentication events, protocol validation errors, and HTTP and SMTP connections
    - VPN-related audit generation – Demonstrates that the TOE selectively logs VPN key exchanges and encrypted communications and VPN errors
    - Audit Collection and Recording – Demonstrates monitoring of system resources, audit threshold behavior, and resource exhaustion alerts
    - SmartCenter Server Audit – Demonstrates logging of management operations
    - Audit Review – Demonstrates restriction of audit review to users explicitly granted the right, and search and sort capability
    - Status Monitoring – Demonstrates appliance status monitoring capabilities
    - Alerts – Demonstrates alerts can be generated for auditable events and resource monitoring
- Security Management Security Function
    - Management Functions – Demonstrates TOE management capabilities, including startup and shutdown, multiple authentication mechanisms, audit trail management, backup and restore, control of communication with authorized external IT entities, management of IDS system behavior, VPN rules, information flow control rules, user security attributes, and audit storage thresholds.
    - Administrator Access Control – Demonstrates user management and permission profiles, restriction of management functionality to authorized administrators
- Secure Internal Communications Security Function
    - Internal CA – Demonstrates certificate management capabilities
    - Secure Internal Communications – Demonstrates the proper function of the SIC capability
- Identification and Authentication Security Function
    - Single User Password – Demonstrates the use of Radius or SecureID for FTP or Telnet authentication
    - Administrator Authentication – Demonstrates SIC certificate based administrator authentication
    - User Authentication – Demonstrates IKE authentication, and FTP and Telnet authentication
    - External IT Entity Authentication – Demonstrates IKE authentication of peer IPSec VPN gateways and hosts, and NTP single use authentication
    - User Identification – Demonstrates that administrators are correctly identified in audit trail, identification of IP addresses of communicating entities in logs, and logging of user identities for FTP, Telnet and IKE.
- TSF Protection Security Function
    - Domain Separation – Demonstrate that the TSF maintains a security domain for its own execution, enforces separation between subjects, protection of intra-OTE management communications,
    - Reference Mediation – Demonstrates non-bypassibility of traffic mediation
    - Hardware Clock – Demonstrates correct timestamping of audit records
    - Self Testing – Demonstrates FIPS 140-2 self tests, monitoring of operational status, and watchdog revival of critical processes.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all subsystem interfaces were tested by the developer. The evaluation team performed a sample of the developer's test suite, representative of the TOE Security Functions, and devised an independent set of team tests and penetration tests.

The independent tests run by the evaluation team included the following types of tests:

- Confirming auditing of dropped packets
- Attempting to force residual information from one packet to another by manipulating packet headers
- Testing the audit resource exhaustion
- Confirming that invalid certificates cannot be used for administrator login
- Performing a Nessus vulnerability scan to and through the firewall

8 Evaluated Configuration

The evaluated configuration includes the following components:

- **One or More Enforcement Modules** - Check Point VPN-1/FireWall-1 NGX software installed on an appliance running the Check Point SecurePlatform NGX operating system
- **One SmartCenter Server** - management server software installed on a host running the Check Point SecurePlatform NGX operating system
- **One or More SmartConsoles** – management GUI software installed on a host running a Microsoft Windows operating system. The SmartConsole hardware and operating system are not considered part of the evaluated system – they are installed and configured by the administrator as needed to support the Check Point application.

The evaluated configuration requires configuration of some specific values of features, as outlined below. More details on these security considerations can be found in the product's guidance documentation.

- The prospective customer must define, document, and follow a network security policy that is appropriate for their site. However, the following security considerations must also be implemented to be compliant with the evaluated configuration of TOE:
- All TOE components must be secured so that only authorized personnel have physical access to the TOE.
- The TOE should not be used to provide security in an environment where the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered high.
- Installers should not install general-purpose applications, public data or other capabilities that are outside the evaluated configuration on any firewall or SmartCenter Server host. In particular, they must not install services (e.g. an FTP server) that can be accessed remotely by non-administrative users.
- Only trustworthy administrators should receive authorization to manage the evaluated configuration.
- A configured firewall shall mediate traffic for at least two networks. Installers must ensure that all information paths between mediated networks pass through a firewall in the evaluated configuration.

- VPN-1/FireWall-1 NGX shall be managed from an administrative workstation, running SmartConsole. Use of CLI or Web interfaces is restricted to product installation. Once the product is operational, the only administrator interfaces used by authorized administrators are SmartConsole applications.
- Radius and NTP shared secrets shall be randomly chosen 16-byte values.
- Telnet and FTP users shall be authenticated using single-use password mechanisms.
- Customers must purchase and follow the procedures for Check Point's Enterprise Software Subscription plan in order to be notified of flaw remediation software updates.

9 Flaw Remediation Procedures

Check Point's flaw remediation process provides a mechanism for user-reported flaws to be processed by the developer, and for prompt distribution of software changes in response to discovered flaws in security and other critical product functionality. Note that the flaw remediation process is available for customers that purchase the Enterprise Software Subscription plan – this plan is required to operate in the evaluated configuration. A security reporting procedure is available to all Enterprise Software Subscribers as well as third-party vulnerability researchers. The developer regularly reviews the MITRE Common Vulnerabilities and Exposures (CVE) database for flaw reports that might be relevant to the product. As of August 21, 2006, there are no vulnerabilities in the CVE database that are applicable to the evaluated product or its direct predecessors, and no other reporting mechanisms have identified any critical security flaws.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

Science Applications International Corporation CCTL has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 4 augmented by ALC_FLR.3. A team of validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in August 2006.

11 Validator Comments

In the evaluated configuration the TOE is a useful product – a traffic filter firewall, application proxy firewall, intrusion detection system and VPN gateway – and meets the requirements of the Intrusion Detection System System Protection Profile. A network protection system based on the TOE can be centrally administered using the SmartConsole application; in the evaluated configuration this requires a separate management LAN.

The product contains more functionality than was covered by the evaluation, including web-based, command line and SNMP management, LDAP based user administration, the SmartUpdate online software upgrade process, failover and load balancing capabilities, and some VPN modes, See section 2.4.7 of the Security Target for more detail on functionality that was omitted from the TOE. During the evaluation, no evidence was found that pointed to any specific security vulnerabilities associated with the features that were not evaluated, but since they were not evaluated, and not covered by any claims in the Security Target, no further conclusions can be drawn about their effectiveness.

Users must purchase and follow the procedures for Check Point's Enterprise Software Subscription plan in order to operate in the evaluated configuration and achieve the systematic

flaw remediation requirements cited in the Security Target. This will enable users to download security patches as they become available.

The TOE includes a flexible, intuitive and usable management system, including certificate based administrator authentication, customizable administrator permissions, a graphical user interface, and support for remote management. The product also includes a standards compliant IKE/IPSec implementation that may be used in the evaluated configuration, something that not all firewall TOEs include.

12 Security Target

Check Point VPN-1/FireWall-1 NGX Security Target, Version 1.2.2, August 23, 2006

13 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated January 2004, Version 2.2.

[7] Final Evaluation Technical Report for a Target of Evaluation Check Point Check Point VPN/FireWall-1 NGX, Part I (Non-Proprietary), Version 0.3, August 23, 2006

[8] Final Evaluation Technical Report for a Target of Evaluation Check Point Check Point VPN/FireWall-1 NGX, Part I (Proprietary), Version 0.3, August 23, 2006

[9] Final Evaluation Technical Report for a Target of Evaluation Check Point Check Point VPN/FireWall-1 NGX, Part II (Proprietary), Version 0.3, August 23, 2006

[10] Check Point VPN-1/FireWall-1 NGX Test Documentation, Version 1.0.3, June 13, 2006

[11] Evaluation Team Test Plan For Check Point (SAIC Proprietary and Check Point Proprietary), Version 0.5, 6/21/06

[12] Check Point VPN-1/FireWall-1 NGX Security Target, Version 1.2.2, August 23, 2006

[13] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.