National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Check Point Software Technologies LTD

Check Point VPN-1 Power/UTM NGX R65 with HFA 30

Report Number: **CCEVS-VR-VID10329-2009**
Dated: **March 25, 2009**
Version: **1.5**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Jim Donndelinger
John Nilles
Scott Shorter

Common Criteria Testing Laboratory

Ms. Cynthia Reese
Mrs. Jean Petty
Science Applications International Corporation
Columbia, Maryland

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Check Point Security Target.

Table of Contents

1 EXECUTIVE SUMMARY

This report documents the results of the Validation Panel's oversight of the evaluation of the Check Point VPN-1 Power/UTM NGX R65 product. It presents the evaluation results, 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 was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) and was completed during February 2009. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the Validation Panel. The evaluation determined that the product conforms to the Common Criteria Version 2.2, Part 2 extended and Part 3 conformant and meets the requirements of Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.3 (Systematic Flaw Remediation).

The Check Point VPN-1 Power/UTM NGX R65 is a network perimeter security 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 and SSL 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).

The Validation Team provided oversight on 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 Common Evaluation Methodology (CEM) work units), and reviewed successive versions of the ETR and test report. The Validators' observations support the CCTL's conclusion that the product satisfies the functional and assurance requirements defined in the Security Target (ST). Therefore, the Validation Panel concludes that the findings of the evaluation team 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 Evaluation Assurance Level (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 evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List. **Table 1** provides information needed to completely identify the product.

Table 1 Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Check Point VPN-1 Power/UTM NGX R65 with HFA 30
Protection Profile	Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006
Security Target	Check Point VPN-1 Power/UTM NGX R65 Security Target, Version 1.0; March 4, 2009
Evaluation Technical Report	Final Evaluation Technical Report For Check Point VPN-1 Power/UTM NGX R65 , Part1 (Non Proprietary), Version 0.2, 4 February 2009 Final Evaluation Technical Report For Check Point VPN-1 Power/UTM NGX R65 , Part 1 (Proprietary), Version 0.2, 4 February 2009 Final Evaluation Technical Report For Check Point VPN-1 Power/UTM NGX R65 , Part 2 (Proprietary), Version 0.5, 4 February 2009
CC Version	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, January 2004 Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2 Revision 256, January 2004
Conformance Result	Part 2 extended, Part 3 conformant, EAL4 augmented
Sponsor	Check Point Software Technologies LTD.
Developer	Check Point Software Technologies LTD
Evaluators	SAIC, Columbia, MD
Validators	Jim Donndelinger, The Aerospace Corporation John Nilles, The Aerospace Corporation Scott Shorter, Orion Security Solutions

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 analysis of network traffic at the network layer, and performing information flow control based on any part of the data being mediated, as well as on state information. An IDS/IPS capability is integrated with the product's traffic-filtering functionality, matching traffic with predefined attack signatures, and providing recording, analysis, and reaction capabilities.
- Security Servers: inspection of FTP, telnet, HTTP and/or SMTP traffic to verify protocol conformance
- Virtual Private Network: IPSec and SSL virtual private network gateway
- Audit: generation, storage, analysis and notification of audit events
- Security Management: administrative management and administrator access control functions
- Secure Internal Communications: protection for management traffic using the TLS protocol
- Identification and Authentication: authentication of external IT entities, administrators and users via IKE, TLS, single-use or static passwords.
- TSF Protection: protection mechanisms such as domain separation, packet defragmentation, self testing, reference mediation and a hardware clock.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

The following conditions are assumed to exist in the operational environment:

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 networks1.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

4.1 Operating Environment

Table 2 lists the security functional requirement that must be satisfied by the IT Environment as presented in the ST.

Table 2 IT Environment Security Functional Requirements

Security Functional Class	Security Functional Components
User Data Protection (FDP)	FDP_UCT.1.1 Basic data exchange confidentiality
	FDP_UIT.1 Data exchange integrity

[1] This assumption means that the TOE does not provide remote services to human users, other than use of identification and authentication functions. The objective for the non-IT environment O.NOREMO upholds this assumption. Note however that both PPs allow the TOE to provide a limited number of security functions to remote (identified and authenticated) authorized external IT entities. These are listed in section **Error! Reference source not found.** above.

Security Functional Class	Security Functional Components
Identification and authentication (FIA)	FIA_UAU.5 Multiple authentication mechanisms
Trusted path/channels (FTP)	FTP_ITC.1 Inter-TSF trusted channel

4.2 Clarification of Scope

The Security Target specified the security requirements of the TOE, which determined the scope of the evaluation. The security requirements allocated to the IT environment have not been verified as part of the Check Point evaluation—it is the responsibility of the integrator to ensure the IT environment satisfies those requirements. The IT security services provided by the environment support the User Data Protection (FDP), the Identification and Authentication (FIA), and the Trusted Path/Channel (FTP)

There is functionality included in the product which is excluded from the evaluation and is identified in section 2.4.7 (Functionality Excluded from the TOE Evaluated Configuration) of the Security Target. The following list is condensed from that section.

- ClusterXL
- SmartUpdate
- OPSEC client APIs
- Remote Management via SNMP
- Remote Management via WebUI
- Nokia Network Voyager software management utility
- CLIs and SSH not supported for post-installation administration
- Extended Remote Access VPN Modes (hybrid mode and MS IPSec/L2TP clients)
- LDAP User Management
- Dynamic Routing Protocols
- Transparent Mode
- DShield Storm Center
- Content Inspection

5 ARCHITECTURAL INFORMATION

The high level architecture of the TOE is shown in Figure 2. The Check Point Check Point VPN-1 Power/UTM NGX R65 Appliance, the rightmost block of the figure, consists of compliance tested hardware, a specially developed Linux operating system with enhanced protections against bypassability, and the firewall software application.

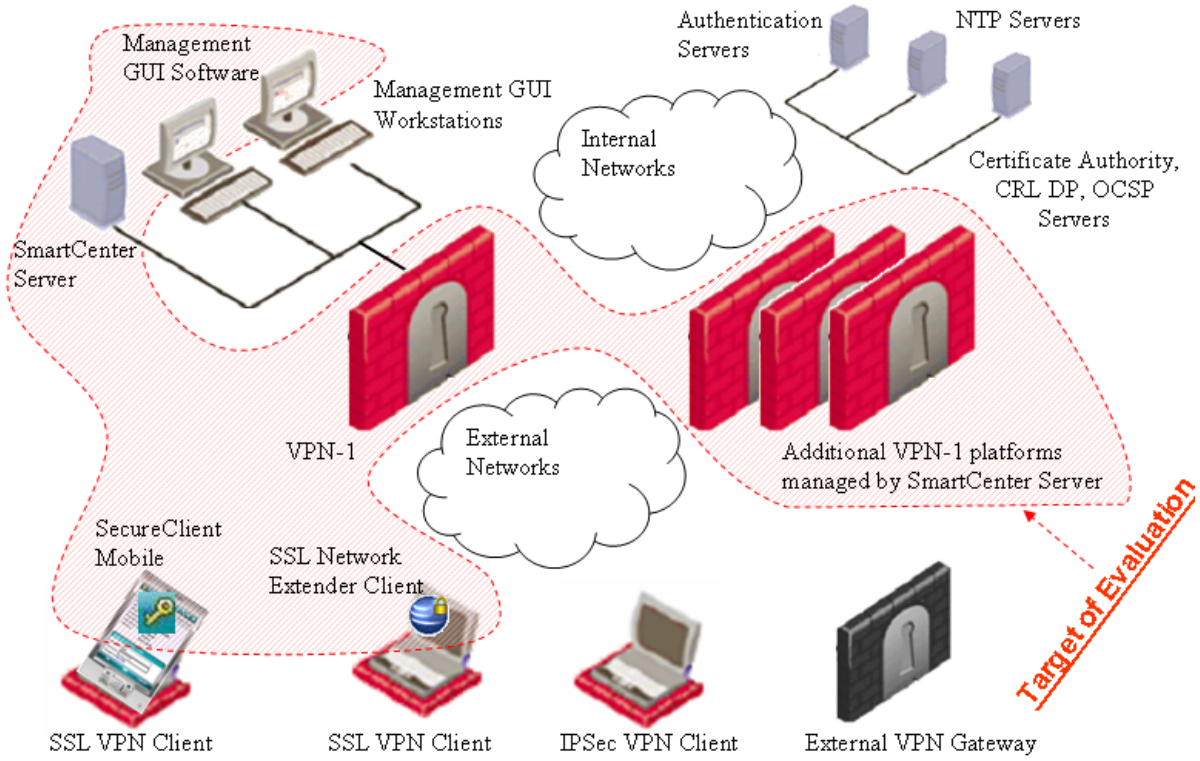

Figure 2 - TOE Architecture

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 was used as evidence for the evaluation of the TOE.

Configuration Item (CI)	CI Unique Identifier	CI Description
Analysis of Correspondence	Check Point VPN-1/FireWall-1 NGX Analysis of Correspondence, Version 0.1, February 21, 2008	Analysis of Correspondence (RCR)
Analysis of Guidance Documentation	Check Point VPN-1/FireWall-1 NGX Analysis of Guidance Documentation, Version 0.2, August 18, 2008	Analysis of Guidance Documentation (MSU)
Configuration Management	Check Point VPN-1/FireWall-1 NGX Configuration Management, Version 4, February 3, 2009	Configuration Management (ACM)
Functional Specification	Check Point VPN-1/FireWall-1 NGX Functional Specification, Version 0.4, August 15, 2008	Functional Specification (FSP)
Guidance Documentation	CC Evaluated Configuration Administration Guide, Check Point Part No.: 702796, August 2008	Administration Guide (ADM)
	CC Evaluated Configuration Installation Guide, Check Point Part No.: 702795, August 2008	Installation Guide (IGS)
	CC Evaluated Configuration User Guide, Check Point Part No.: 702797, August 2008	User Guide (USR)
High-level Design	Check Point VPN-1/FireWall-1 NGX High-level Design, Version 0.3, August 15, 2008	High-level Design (HLD)
Lifecycle Model	Check Point VPN-1/FireWall-1 NGX Life Cycle, Version 0.2, August 18, 2008	Life Cycle (ALC)
Low-level Design	Check Point VPN-1/FireWall-1 NGX Low-level Design, Version 0.2, August 15, 2008	Low-level Design (HLD)
Security Policy Model	Check Point VPN-1/FireWall-1 NGX Security Policy Model, Version 0.1, February 11, 2008	Security Policy Model (SPM)
Security Target	Check Point VPN-1/FireWall-1 NGX Security Target, Version 1.0, March 4, 2009	Security Target (ST)
Test	Check Point VPN-1/FireWall-1	Test Documentation (ATE)

Configuration Item (CI)	CI Unique Identifier	CI Description
Documentation	NGX Test Documentation, Version 0.7, December 31, 2008 Check Point VPN-1/FireWall-1 NGX Actual Test Results, Version 0.5, February 4, 2009	
Vulnerability Assessment	Check Point VPN-1/FireWall-1 NGX Vulnerability Analysis, Version 0.2, August 15, 2008	Vulnerability Analysis (VLA)

7 IT PRODUCT TESTING

7.1 Vendor Testing

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

7.1.1 Testing Approach

The developer testing approach is described in the "Check Point VPN-1/FireWall-1 NGX Test Documentation"

The testing of the security functions was performed by a series of automated tests and manual tests. To ensure test reproducibility, automated tests form the core of the CC tests. Automated tests always restore the test environment to a known configuration as an initial step. This feature was used to ensure that manual tests are also reproducible, by performing each test on an environment that has been generated by running an identified automated test.

The vendor test documentation shows the correspondence between security functions and TSFI. The vendor test suite demonstrates the security-relevant behavior at the interfaces defined in the design documentation. The results of the tests demonstrated that the TOE meets the security functional requirements specified in the Security Target.

The security functions that were tested are the same as those mentioned in the Security Target: Stateful Inspection, Security Servers, VPN, Audit, Security Management, SIC, Identification & Authentication, and Protection of the TSF.

7.1.2 Test Descriptions

The vendor test documentation includes detailed test procedures in section 4 of the test documentation; both automated and manual tests. Each test procedure includes detailed setup instructions, prerequisites, test steps, and expected results in the body of the test procedures.

The actual results are captured in a separate vendor test document.

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
- SSL VPN – demonstrates the SSL VPN functionality
- 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-bypassability 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.

7.1.3 Depth and Coverage

The amount of testing performed as it relates to the required functionality is described in the rationale for ATE_COV work units. The depth of testing performed as it relates to the High Level design is described in the rationale for the ATE_DPT work units in the Evaluation Technical Report.

7.1.4 Test Results

The actual results are captured in a separate vendor test document. For each description included in the "Check Point VPN-1/FireWall-1 NGX Test Documentation", there are actual results included in the "Check Point VPN-1/FireWall-1 NGX Actual Test Results."

7.2 Evaluator 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

Based upon further validation review, the following test cases were added to the vendor test suite:

- demonstration of the blocking of overlapping IP fragments.
- demonstration of the handling of invalid and large Certificate Revocation Lists (CRL)

8 EVALUATED CONFIGURATION

Check Point VPN-1 Power/UTM is a software product produced by Check Point. The product is installed on a hardware platform in combination with an operating system (OS), in accordance with TOE guidance, in a FIPS 140-2 compliant mode.

The consumer installs the software on commodity hardware platforms identified in Appendix A - TOE Hardware Platforms section A.1 section of the ST. Alternatively, the consumer can purchase the software pre-installed on the security appliances identified in sections A.2 and A.3 of the ST.

All platforms identified in Appendix A provide an AMD or Intel-based CPU as well as memory, disk, local console and network interface facilities that are tested by Check Point as providing sufficient service and reliability for the normal operation of the software. A hardware clock/timer with on-board battery backup supports the operating system in maintaining reliable timekeeping.

9 RESULTS OF THE EVALUATION

The evaluation was conducted based upon CC version 2.2 and CEM version 2.2. The evaluation determined the Check Point TOE to be Part 2 extended and Part 3 conformant, and that the TOE meets the Part 3 Evaluation Assurance Level (EAL 4) requirements augmented with ALC_FLR.3

9.1 Evaluation of the Check Point Security Target (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Check Point product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

9.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured

the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

The evaluation team also applied the ALC_FLR.3 related work units from the Flaw Remediation CEM Supplement (Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R). The evaluation team ensured the developer has a process to systematically track flaws, document flaws, address flaws, and provide flaw information to TOE users.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE security functional requirements are enforced by the TOE. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The results of the vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Evaluation of the Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

9.10 Assurance Requirement Results

The assurance requirements for the TOE evaluation are those required by EAL4.

9.10.1 Common Criteria Assurance Components

The CEM work units associated with EAL4 are distributed amongst the ETR sections in chapter

15 of the ETR. Collectively, the ETR sections in chapter 15 encompass all CEM work units for EAL4. Each ETR section includes the CEM work units associated with that ETR section title (e.g. ACM). Within each ETR section, for each CEM work unit the following is provided:

- Verdict
- Verdict Rationale

The rationale justifies the verdict using the CC, the CEM, and any interpretations and the evaluation evidence examined. The rationale demonstrates how the evaluation evidence meets each aspect of the criteria.

The work performed contains a description of the action performed or the method used to apply the work unit.

9.10.2 Testing and Vulnerability Assessment

In addition to ETR sections the evaluators developed a Test Plan/Report Part to capture the detail beyond the CEM work unit information. This detail is described within the CEM guidance for the testing and vulnerability assessment work units. Primarily, the additional detail is focused on team test procedures, penetration test procedures, results from running the vendor's sample, and the justification of running the vendor's sample.

The evaluation team prepared a Draft of the Test Plan/Report prior to testing that addressed the selection of vendor tests to run, the team test procedures, and the penetration test procedures. After performing the test, the Test Report Part was updated to include the actual results from the vendor sample run and the team test. The Test Report is included in the "Check Point VPN-1 Power/UTM Part 2 Final ETR Proprietary" ETR document, chapter "Test Report".

9.11 Conclusions

The conclusions for the ST evaluations and the TOE evaluations are addressed below.

9.11.1 ST Evaluation

Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the Check Point VPN-1 Power/UTM NGX R65 Security Target is a CC compliant ST.

9.11.2 TOE Evaluation

The verdicts for each CEM work unit in the ETR sections included in chapter 15 are each "PASS". Therefore, the TOE (see below product identification) satisfies the Check Point VPN-1 Power/UTM NGX R65 Security Target, when configured according to the following guidance documentation:

- NGX R65 CC Evaluated Configuration Installation Guide, Part No. 702795, October 2008

9.12 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test further demonstrated the claims in the ST.

10 VALIDATOR COMMENTS AND RECOMMENDATIONS

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.

The validation team was impressed with the quality of the functional specification for the TOE, it provided a very thorough and well organized presentation of the required information.

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. The IKE/IPSec implementation was tested by ICSA Labs for the correctness of the protocol implementation and for interoperability with other VPN products.

This evaluation used evidence and analysis from the prior evaluation (VID 10091) of Check Point VPN-1/Firewall-1 NGX R60, with the changes to the TOE between R60 and R65 receiving the greatest amount of scrutiny and analysis. The validators worked with the evaluation team to ensure that the analysis and testing performed for the R65 features was commensurate with EAL4 requirements and the prior R60 evaluation and that analysis and testing of the R60 features was updated as necessary to reflect the new product's security functionality. The changes from R60 to R65 include the addition of the SSL VPN security function (including the inclusion of new TOE components and interfaces) as well as some updates to the R60 interfaces, including support of Office Mode for IKE and Topology Updates for remote access IPSec VPN.

11 SECURITY TARGET

The *Check Point VPN-1/FireWall-1 NGX Security Target*, Version 1.0, March 4, 2009 is included here by reference.

GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
DAC	Discretionary Access Control
DDL	Data Definition Language
DML	Data Manipulation Language
DRDA	Distributed Relational Database Architecture
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
LBAC	Label Based Access Control
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PP	Protection Profile
RDBMS	Relational Database Management System
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

12 BIBLIOGRAPHY

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

[2] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2 Revision 256, January 2004

[3] COMMON CRITERIA PROJECT SPONSORING ORGANIZATIONS. *Common Evaluation Methodology for Information Technology Security: Evaluation Methodology,* January 2004, Version 2.2, CCMB-2004-01-004.

[4] COMMON CRITERIA PROJECT SPONSORING ORGANIZATIONS. *Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation*, Version 1.1, February 2002, CEM-2001/0015R

[5] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, *Evaluation Technical Report for* Check Point VPN-1 Power/UTM NGX R65 *Part 1 (Non-Proprietary)*, Revision 0.2, 4 February 2009.

[6] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, *Evaluation Technical Report for* Check Point VPN-1 Power/UTM NGX R65 *Part 1 (Proprietary)*, Revision 0.2, 4 February 2009.

[7] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, *Evaluation Technical Report for* Check Point VPN-1 Power/UTM NGX R65 *Part 2 (Proprietary)*, Revision 0.5, 4 February 2009.

[8] Check Point VPN-1 Power/UTM NGX R65 *Security Target*, Version 1.0, 4 March 2009.

[9] COMMON CRITERIA EVALUATION AND VALIDATION SCHEME. *NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories*, Version 1.0, March 20, 2001, Scheme Publication #4.