National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Check Point Software Blades R77

Report Number: CCEVS-VR-VID10388-2013
Dated: December 30, 2013
Version: 1.0

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 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

List of Tables

1 Executive Summary

The evaluation of **Check Point Software Blades R77** was performed by Leidos, in the United States and was completed in December 2013. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The criteria against which the Check Point Software Blades R77 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 4. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation versions 3.1, revision 4. The Target of Evaluation (TOE) claims demonstrable compliance to *U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments*, Version 1.1, July 25, 2007 (TFF PP), *U.S. Government Protection Profile for Application Level Firewall in Basic Robustness Environments*, Version 1.1, July 25, 2007 (APP PP), and the *U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments*, Version 1.7, July 25, 2007 (IDS System PP).

The TOE is a network perimeter security gateway that provides controlled connectivity between two or more network environments. The TOE implements a broad set of information flow controls including traffic filtering, application-level proxies, network address translation (NAT), and intrusion detection and prevention. IKE/IPSEC and SSL virtual private networking (VPN) functionality encrypts and authenticates network traffic.

Leidos determined that the product satisfies evaluation assurance level (EAL) 4 augmented with ALC_FLR.3 as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the *Check Point Software Blades R77 Security Target*, version 1.3, September 24, 2013. This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is Check Point Software Blades R77 running on Check Point specific appliances and Open Server hardware platforms running the Check Point Gaia operating system. This Validation Report is not an endorsement of Check Point Software Blades R77 by any agency of the US Government and no warranty of the product is either expressed or implied.

The technical information included in this report was obtained from the Final Evaluation Technical Report for Check Point Software Blades R77 ETR parts 1 and 2 and the associated test report produced by Leidos.

2 Identification

Evaluated Product:	Check Point Software Blades R77
Sponsor & Developer:	Check Point Software Technologies LTD. 5 Ha'Solelim St Tel Aviv, Israel 67897
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	December 2013
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Protection Profiles:	U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments, Version 1.1, July 25, 2007 U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments, Version 1.1, July 25, 2007 U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environment, Version 1.7, July 25, 2007
Evaluation Class:	Evaluation Assurance Level (EAL) 4 Augmented with ALC_FLR.3
Description	The TOE is the Check Point Software Blades R77, comprised of Security Gateway Version R77: Firewall, IPSEC VPN, IPS Acceleration and Cluster; and Security Management Version R77: Network Policy Management, Logging & Status Monitoring. The TOE is a network perimeter security gateway that provides controlled connectivity between two or more network environments.

Disclaimer	The information contained in this Validation Report is not an endorsement of the Check Point Software Blades R77 by any agency of the U.S. Government and no warranty of Check Point Software Blades R77 is either expressed or implied.
Evaluation Personnel:	Tony Apted Kevin R. Micciche Gary Grainger Amit Sharma Dragua Zenelaj
Validation Scheme:	NIAP Common Criteria Evaluation and Validation Scheme

2.1 Evaluation Details

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. Note that assurance requirements outside the scope of EAL 1 through EAL 4 are addressed at the discretion of the CCEVS.

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.

The following table serves to identify the evaluated Security Target and TOE.

Table 1 ST and TOE identification

ST Title:	Check Point Software Blades R77 Security Target, Version 1.4, November 18, 2013
TOE Identification:	TOE Software Identification: Check Point Software Blades R77, comprised of the following Check Point software blades[1]: • Security Gateway Version R77: Firewall, IPSEC VPN, IPS, Acceleration and Clustering • Security Management Version R77: Network Policy Management, Logging & Status, Monitoring
Operating Platform:	The TOE includes the following hardware platforms for the R77 Gateway Software o Supported Check Point Security Appliances o Power-1 507* o Power-1 907* o Power-1 1106*, 1107*, 1108* o UTM-1 27*, 57* o UTM-1 107*, 207*, 307* o Check Point 22** Appliances o Check Point 42**, 44**, 46**, 48**

[1] Software Blades are security modules purchased by customers independently or in pre-defined bundles, for installation on a Check Point Security Gateway or Security Management server.

	Appliances o Check Point 122**, 124**, 126**, 135** Appliances o Check Point 214**, 216**, 217** Appliances o VSX-1 3070 Appliances o VSX-1 9070 Appliances o VSX-1 9090 Appliances o VSX-1 11000 series Appliances o VSX-1 11200 series (VSLS) Appliances o Check Point 12200 VSX Appliances o Check Point 12400 VSX Appliances o Check Point 12600 VSX Appliances o Check Point 21400 VSX Appliances Supported Hardware running the SecurePlatform Gaia R77 operating System Check Point — IAS Server L2, L6, L8, M2, M6, M8, D1, R2, R6, R8, U1 Dell — PowerEdge 620, 720 Fujitsu — Primergy RX100 S6, S7; Primergy RX200 S6, S7; Primergy RX300 S6, S7 HP — ProLiant DL120 G7; ProLiant DL320e G8; ProLiant DL360 G7, 360p G8; ProLiant DL380 G7, 380p G8 IBM — System X x3550 M3, M4; System X x3650 M3, M4 Supported Check Point IP Appliances o IP295 o IP395 o IP565 o IP695 o IP1285 o IP2455 Supported Check Point Security Management Appliances o Smart-1 5 o Smart-1 25 o Smart-1 50 o Smart-1 150

3 Security Policy

3.1 Summary

Check Point Software Blades R77 mediates information flows between clients and servers located on internal and external networks governed by the firewall. Proxy servers on the firewall, for the services FTP and Telnet, require authentication by client users before requests for such services can be authorized.

User authentication may be achieved by a remote access client authenticating using IKE or TLS, against authentication credentials held by the user. Administrators also need to authenticate to the TOE before they can use the Management GUIs to access Security Management. The TOE can be optionally configured to perform user authentication with the support of external authentication servers in the IT environment.

Proxies are also provided for the services SMTP and HTTP that can optionally, as determined by the authorized administrator, require the client user to authenticate.

The product additionally imposes traffic-filtering controls on mediated information flows between clients and servers according to the site's security policy rules. By default, these security policy rules deny all inbound and outbound information flows through the TOE. Only an authorized administrator has the authority to change the security policy rules.

Once an authorized administrator describes the network topology in terms of networks and IP addresses, anti-spoofing controls prevent information flows that contain invalid source addresses, i.e. source addresses that should not be received by the TOE interface on which the information flow has arrived.

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.

IPSec VPN and SSL VPN capabilities are provided to encrypt network traffic to and from selected peers, in order to protect traffic from disclosure or modification over untrusted networks. External IT entities establishing VPN tunnels with the TOE can be VPN gateways such as the TOE (site to site VPN), or may be single-user client workstations (remote access VPN). The VPN identifies and authenticates the peer entity as part of the process of establishing the VPN tunnel, via the IKE or TLS protocols, respectively. HTTPS has also been provided to perform IDS analysis on encrypted streams.

Administrators can perform both local and remote management of the TOE. Administrator sessions are protected via a trusted path between the Management GUI and the Security Management server. Internal TOE communications between the Security Management

server and Security Gateway appliances is also protected from disclosure and undetected modification.

Audit trail and IDS System data is stored in log databases, stamped with a dependable date and time when recorded. Auditable events include modifications to the group of users associated with the authorized administrator role, all use of the identification and authentication mechanisms (including any attempted reuse of authentication data), all information flow control decisions made by the TOE according to the security policy rules, and the use of all security functions. If log storage is exhausted, then the only recordable events that may be performed are those performed by the authorized administrator. The TOE includes tools to perform searching and sorting on the collected audit trail and IDS System data according to attributes of the data recorded and ranges of some of those attributes.

The Check Point Software Blades R77 Security Gateway appliance protects itself and the Security Management server and Management GUIs against network-level attacks by unauthorized users. Domain separation is provided between TOE interfaces. Self-tests are run during initial start-up and periodically during normal operation to ensure correct operation. A hardware clock provides reliable timestamps.

Fault-tolerance is ensured by supporting multiple Security Gateway appliances and Security Management hosts that synchronize databases and state tables among redundant instances. Critical hardware, software, and networking components are constantly monitored, allowing the TOE to reconfigure itself to bypass faulty components.

3.2 TOE Threats

3.2.1. Firewall-related Threats

The following threats are identified in [TFF-PP]

T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person on an external network may attempt to bypass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorized person may send impermissible information

	through the TOE which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.AUMACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
T.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

3.2.2. IDS-related Threats

The following threats are identified in [IDSSPP]

T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities

	or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.2.1 Virtualization-related Threats

The following threats are countered by the TOE's virtualization functionality.

T.ACCESS	An unauthorized person or external IT entity may be able to access data flowing through or stored within the TOE in violation of Virtual System domain separation policy.

3.2.3. VPN-related Threats

The following threats are countered by the TOE's VPN functionality.

T.NACCESS	An unauthorized person or external IT entity may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.
T.NMODIFY	An unauthorized person or external IT entity may modify data that is transmitted between the TOE and a remote authorized external IT entity.

3.2.4. Fault-related Threats

The following threat is countered by the TOE's fault tolerance functionality.

T.FAULT	A failure in a critical hardware or software entity may disrupt TOE security functions.

3.3 Assumptions and Organizational Security Policies

The following assumptions and Organizational Security Policies (OSP) are identified in the Security Target:

3.3.1. Physical Assumptions

The following conditions are assumed to exist in the operational environment. Each of these assumptions is consistent with the explicit or implicit assumptions made in each of the PPs for which conformance is claimed: [TFF-PP] and[IDSSPP].

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NOEVIL	Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. However, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

3.3.2. Firewall PP OSPs

The [APP-PP] defines the following OSP:
Federal agencies are required to protect sensitive but unclassified information with cryptography. Products and systems compliant with this Protection Profile are expected to utilize cryptographic modules for remote administration compliant with FIPS PUB 140-1 (level 1).

P.CRYPTO	AES (Advanced Encryption Standard as specified in FIPS 197) encryption must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-2 (level 1).

3.3.3. IDS System PP OSPs

The following OSPs are defined in [IDSSPP]. [IDSSPP] does not identify which organization and which organizational security policy any of these OSPs are drawn from.

P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about

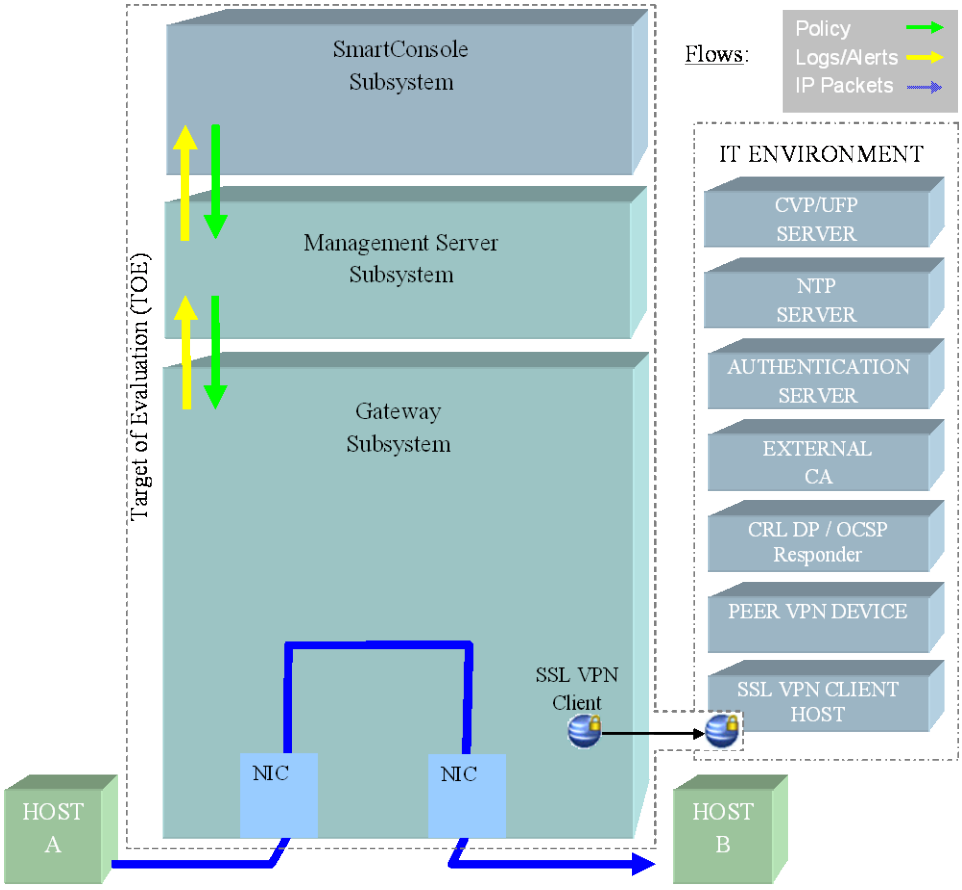
	intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4 Architectural Information

Check Point Software Blades R77 is a network perimeter security gateway that provides controlled connectivity between two or more network environments.

Check Point Software Blades R77 is a TOE in parts composed of three types of machines: SmartConsole hosts, Management Server hosts, and Gateways. Each physically independent machine is defined as a separate subsystem. Inter-subsystem interfaces are manifested as network connections, which are protected by the SIC SF.

Subsystem Decomposition



Smart Console Subsystem
The SmartConsole machine is a general purpose PC running SmartConsole, the Check Point Management GUI. SmartConsole applications include Security Management, SmartDashboard, SmartView Tracker, and SmartView Monitor. Each of these is modeled in this document as a security-enforcing module. The SmartConsole subsystem interacts with the Management Server subsystem over the CPMI inter-subsystem interface, enabling an administrator to manage the TOE and to receive log, alert and system status data.

Management Server Subsystem
The Management Server subsystem serves as an intermediate between the SmartConsole and Gateway subsystems in the TOE. In addition, the Management Server application provides for a Public Key Infrastructure (PKI) for the TOE (ICA), to support the Secure Internal Communications (SIC) capability.

The Management Server subsystem handles policy, log, alert and system status data flows. In handling the policy data flow, it receives policy data entered by the TOE administrator via SmartConsole, and processes (compiles), stores and distributes it to one or more Gateways. In handling the log and alert data flow, it receives data from Gateways, and processes, stores and conveys it to SmartConsoles for viewing by the TOE administrator. In

handling the system status data flow, it passes queries from the SmartConsole to the Gateway and query results from the Gateway to the SmartConsole.

The Management Server subsystem supplies a Public Key Infrastructure for the TOE – the Internal Certificate Authority (ICA). The ICA issues, renews and revokes certificates for administrators and Gateways. SIC keys and certificates are pushed by the Security Management subsystem to the various SIC entities within the TOE, and Certificate Revocation Lists (CRLs) are distributed to SIC entities.

The Management Server machine operating system is Check Point Gaia R77. The machine hardware is any of the hardware platforms identified in the ST as suitable for Security Management.

Gateway Subsystem
The Gateway subsystem is the policy enforcement point for traffic flowing through the TOE. Traffic filtering is performed by kernel-level code to ensure maximum performance. User-level modules perform tasks which the kernel cannot: write-to-file duties, log handling, inter-host communication (e.g. IKE/IPsec SA establishment) and management.

The Gateway Platform operating system is Gaia R77. Gaia is a Check Point proprietary operating system that is a stripped-down version of the Red Hat Enterprise Linux (RHEL) Version 5.2 distribution (2.6.18 kernel). All changes done by Check Point to the Red Hat RPMs are under the Open-GPL Open Source license.

4.1 Physical Boundaries

The Target of Evaluation (TOE) includes the following components:

- Check Point Security Gateway Appliances, including Security Gateway software, Gaia operating system, and appliance hardware; and
- Security Management servers, including Security Management software, Gaia R77 OS, and hardware platform; and
- SmartConsole Management GUI software; and
- SSL Network Extender (SSL VPN) client software; and
- TOE guidance.

5 Documentation

Check Point offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The documentation for the TOE is:

- Check Point Software Blades R77 CC Evaluated Configuration Installation Guide, April 2013
- Check Point Software Blades R77 CC Evaluated Configuration Administration Guide, April 2013

The following documents are available for additional guidance, but it is the CC Specific document above that serves to guide the user to operate the TOE in its evaluated configuration.

- Security Management Server R77 Administration Guide, August 27, 2013
- SmartView Monitor R77 Administration Guide, August 20, 2013
- Check Point IPS R77 Administration Guide, August 15, 2013
- Firewall Administration Guide Version R77, August 27, 2013
- Virtual Private Networks Administration Guide Version R76, February 17, 2013
- Security Gateway Technical Administration Guide Version R77, August 29, 2013
- Gaia Administration Guide Version R77, August 29, 2013
- Check Point VSX Administration Guide Version R77, August 26, 2013

6 IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL4 evaluation.

6.1 Developer Testing

The developer created test procedures specifically to fulfill the test requirements for an EAL4 evaluation. The tests were developed to provide good coverage of the security functions related to each of the security requirements in the Security Target. The developer has documented their tests in a test plan where the results of the tests are presented as prose conclusions, notes, screen shots, and summaries for each of the applicable test platforms.

6.2 Independent Testing

Independent testing took place at the developer's location in in October 2013 and in Israel in November 2013.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE (in three distinct but representative configurations) in accordance with the provided guidance, and exercised a representative subset of the developers test plan on equipment configured in the testing laboratory.

This effort involved installing and configuring the Check Point Software Blades R77 components in their respective tiers on a representative subset of the supported operating systems. Subsequently, the evaluators exercised a subset of the available developer's test procedures for the Check Point Software Blades R77 TOE. The subset of tests was selected in order to ensure that each of the claimed security functions was meaningfully sampled.

Also, the evaluators devised independent tests to ensure that start-up and shutdown operations were audited, to verify the claimed methods of audit storage, to verify use of management of audit and audit of use of the TSF data consistency, to verify audit of cryptographic activity, to verify claimed client-visible error codes, to verify correct cipher suite and key sizes, to verify filtering based on connection-oriented protocols, to verify that users cannot re-use single-use authenticator for user authentication, to verify management restrictions at the SmartConsole interfaces, and to verify management of default security attributes.

In addition to the use of developer provided and independently devised security functional tests, the evaluators also explored the possibility to penetrate or bypass the security mechanisms. Much of this work was based on analysis of the design, source code, and actual configuration information derived from the installed and configured products. However, the evaluators also devised some tests including scans of the installed products (for open ports) attempts at account harvesting, and also examination of actual network traffic between the client and server products

Given the complete set of test results from test procedures exercised by the developer and the sample of tests directly exercised by the evaluators, the testing requirements for EAL4 are fulfilled.

7 Evaluated Configuration

The TOE is Check Point Software Blades R77 installed according to the Check Point Software Blades R77 CC Evaluated Configuration Installation Guide.

8 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, and the CCEVS. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing notes, comments, or vendor actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by Leidos.

Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 4 augmented with ALC_FLR.3. The following components are taken from CC part 3:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_IMP.1 Implementation representation of the TSF
- ADV_TDS.3 Basic modular design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.4 Production support, acceptance procedures and automation
- ALC_CMS.4 Problem tracking CM coverage
- ALC_DEL.1 Delivery procedures
- ALC_DVS.1 Identification of security measures
- ALC_FLR.3 Systematic flaw remediation
- ALC_LCD.1 Developer defined life-cycle model
- ALC_TAT.1 Well-defined development tools
- ASE_CCL.1 Conformance claims

- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.2 Security objectives
- ASE_REQ.2 Derived security requirements
- ASE_SPD.1 Security problem definition
- ASE_TSS.1 TOE summary specification
- ATE_COV.2 Analysis of coverage
- ATE_DPT.1 Testing: basic design
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing – sample
- AVA_VAN.3 Focused vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached Pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.

The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

9 Validator Comments/Recommendations

The validators have no comments or specific recommendations.

10 Annexes

Not applicable.

11 Security Target

Check Point Software Blades R77 Security Target, Version 1.4, November 18, 2013

12 Acronym List

CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CM	Configuration Management
CMP	Configuration Management Plan
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versioning System
DoD	Department of Defense
EAL	Evaluation Assurance Level
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High-level Design
ID	Identity/Identification
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

13 **Bibliography**

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

[5] Check Point Software Blades R77 Security Target, Version 1.3, September 24, 2013.

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report For Check Point Software Blades R77, parts 1 and 2 (and associated test report), version 1.0, December 4, 2013.