

**National Information Assurance Partnership**  
**Common Criteria Evaluation and Validation Scheme**



**Validation Report**

**Check Point Software Blades R7x**

**Report Number:** CCEVS-VR-10387-2012  
**Dated:** November 26, 2012  
**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

1	Executive Summary .....	1
1.1	Evaluation Details .....	2
2	Identification .....	<b>Error! Bookmark not defined.</b>
3	Security Policy .....	6
3.1	Summary .....	6
3.2	TOE Threats .....	7
4	Assumptions and Organizational Security Policies .....	11
4.1	Physical Assumptions .....	<b>Error! Bookmark not defined.</b>
4.2	Virtualization OSPs .....	<b>Error! Bookmark not defined.</b>
4.3	IDS System PP OSPs .....	<b>Error! Bookmark not defined.</b>
5	Architectural Information .....	12
5.1	Physical Boundaries .....	14
6	Documentation .....	15
7	IT Product Testing .....	16
7.1	Developer Testing .....	16
7.2	Independent Testing .....	16
8	Evaluated Configuration .....	17
9	Results of the Evaluation .....	17
10	Validator Comments/Recommendations .....	18
11	Annexes .....	18
12	Security Target .....	18
13	Acronym List .....	19
14	Bibliography .....	20

## List of Tables

Table 1 ST and TOE identification..... 4

VALIDATION REPORT  
Check Point Software Blades R7x

## 1 Executive Summary

The evaluation of **Check Point Software Blades R7x** was performed by SAIC, in the United States and was completed in November 2012. 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](http://www.niap-ccevs.org). The criteria against which the Check Point Software Blades R7x TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3. 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 3. 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.

Science Applications International Corporation (SAIC) 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 R7x Security Target*, version 1.2, November 8, 2012. This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is Check Point Software Blades R7x running on Check Point specific appliances and Open Server hardware platforms running the Check Point SecurePlatform operating system. This Validation Report is not an endorsement of Check Point Software Blades R7x 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 R7x ETR parts 1 and 2 and the associated test report produced by SAIC.

VALIDATION REPORT  
Check Point Software Blades R7x

## 2 Identification

<b>Evaluated Product:</b>	Check Point Software Blades R7x
<b>Sponsor &amp; Developer:</b>	Check Point Software Technologies LTD. 5 Ha'Solelim St Tel Aviv, Israel 67897
<b>CCTL:</b>	Science Applications International Corporation Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
<b>Completion Date:</b>	November 2012
<b>CC:</b>	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, September 2009
<b>Interpretations:</b>	There were no applicable interpretations used for this evaluation.
<b>CEM:</b>	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 3, September 2009
<b>PP:</b>	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
<b>Evaluation Class:</b>	Evaluation Assurance Level (EAL) 4 Augmented with ALC_FLR.3
<b>Description</b>	The TOE is the Check Point Software Blades R7x, comprised of Security Gateway Version R70.1 with R7x hotfix: Firewall, IPSEC VPN, IPS Acceleration and Cluster; and Security Management Version R71.10 with R7x hotfix: Network Policy Management, Logging & Status Monitoring. The TOE is a

VALIDATION REPORT  
Check Point Software Blades R7x

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 R7x by any agency of the U.S. Government and no warranty of Check Point Software Blades R7x is either expressed or implied.

**Evaluation Personnel:**

M. Evencie Pierre  
Gary Grainger  
Tammy Compton

**Validation Scheme:**

NIAP Common Criteria Evaluation and Validation Scheme

VALIDATION REPORT  
Check Point Software Blades R7x

## 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**

<b>ST Title:</b>	Check Point Software Blades R7x Security Target, Version 1.2, November 8, 2012
<b>TOE Identification:</b>	<p>TOE Software Identification: Check Point Software Blades R7x, comprised of the following Check Point software blades<sup>1</sup>:</p> <ul style="list-style-type: none"> <li>• Security Gateway Version R70.1 with R7x hotfix: Firewall, IPSEC VPN, IPS, Acceleration and Clustering</li> <li>• Security Management Version R71.10 with R7x hotfix: Network Policy Management, Logging &amp; Status, Monitoring</li> </ul>
<b>Operating Platform:</b>	<p>The TOE includes the following hardware platforms for the R7x Gateway Software</p> <ul style="list-style-type: none"> <li>• Supported Check Point Security Appliances <ul style="list-style-type: none"> <li>○ Power-1 507*</li> <li>○ Power-1 907*</li> <li>○ Power-1 1106*, 1107*, 1108*</li> <li>○ UTM-1 27*, 57*</li> <li>○ UTM-1 107*, 207*, 307*</li> <li>○ Check Point 22** Appliances</li> </ul> </li> </ul>

<sup>1</sup> 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.

VALIDATION REPORT  
Check Point Software Blades R7x

	<ul style="list-style-type: none"><li>○ Check Point 42**, 46**, 48** Appliances</li><li>○ Check Point 122**, 124**, 126** Appliances</li><li>○ Check Point 214**, 216** Appliances</li> <li>● Supported Hardware running the SecurePlatform R7x operating System<ul style="list-style-type: none"><li>○ Check Point IAS Server L2, L6, L8, M2, M6, M8, D1, R2, R6, R8, U1</li><li>○ Dell PowerEdge 620, 720</li><li>○ Fujitsu Primergy RX100 S6, S7 Primergy RX200 S6, S7 Primergy RX300 S6, S7</li><li>○ HP ProLiant DL120 G7 ProLiant DL320e G8 ProLiant DL360 G7, G8 ProLiant DL380 G7, G8</li><li>○ IBM System X x3550 M3, M4 System X x3650 M3, M4</li></ul></li> <li>● Supported Check Point Security Management Appliances<ul style="list-style-type: none"><li>○ Smart-1 5</li><li>○ Smart-1 25</li><li>○ Smart-1 50</li><li>○ Smart-1 150</li></ul></li></ul>
--	--



## 3 Security Policy

### 3.1 Summary

Check Point Software Blades R7x 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.

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.

VALIDATION REPORT  
Check Point Software Blades R7x

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 R7x 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.

VALIDATION REPORT  
Check Point Software Blades R7x

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.

VALIDATION REPORT  
Check Point Software Blades R7x

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.

### 3.2.3. 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.
---------	---

VALIDATION REPORT  
Check Point Software Blades R7x

### 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

VALIDATION REPORT  
Check Point Software Blades R7x

	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.

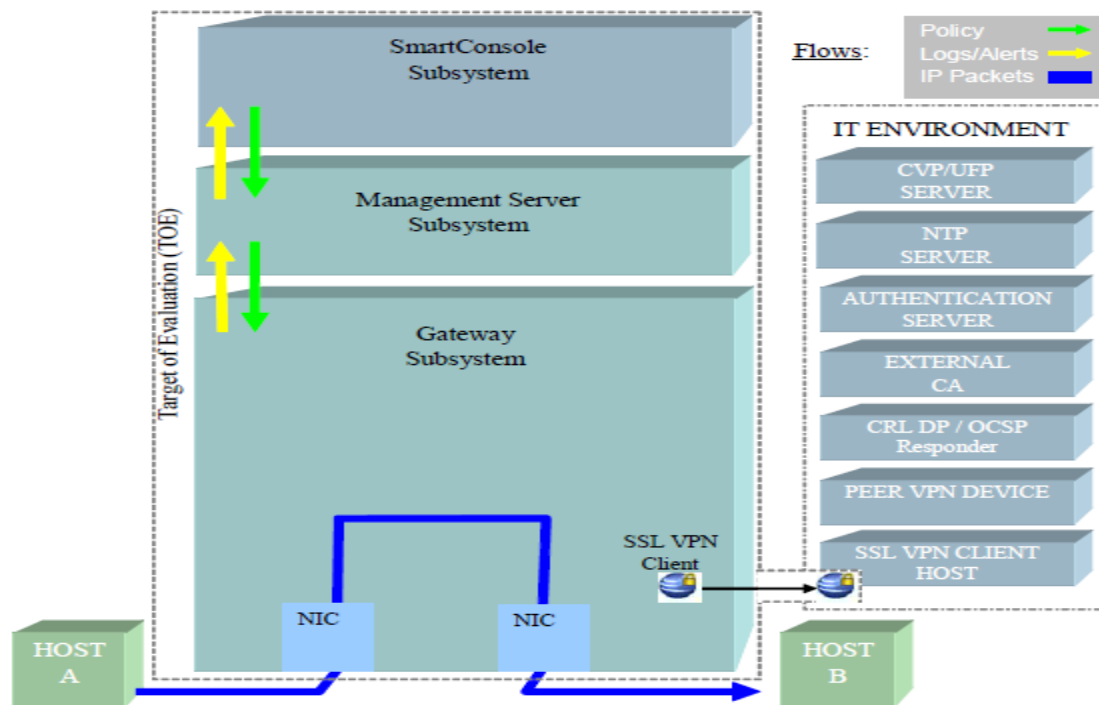
## 4 Architectural Information

Check Point Software Blades R7x is a network perimeter security gateway that provides controlled connectivity between two or more network environments.

Check Point Software Blades R7x 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

VALIDATION REPORT  
Check Point Software Blades R7x



### Smart Console Subsystem

The SmartConsole Subsystem is the Administrator's point of access for performing administration of the TOE, monitoring and viewing audit data of the TOE. It includes three applications: SmartDashboard, which is the primary management GUI and provides all configuration capabilities (i.e. user management, policy management, etc.); SmartView Tracker, provides the ability to view the different audit logs; and SmartView Monitor provides the means for monitoring the TOE status in real-time and receiving alerts.

### Management Server Subsystem

The Management Server subsystem is responsible for:

- Administrator authentication and authorization
- Providing remote administrators with an encrypted trusted path
- Audit/log collection and log database management
- Management of security policy, functions and configuration settings
- Distribution of SIC and VPN public key credentials to TOE entities
- Management high-availability
- TOE component status collection

The Management Server subsystem is responsible for managing the TOE databases, objects, users, and policies. It communicates with the SmartConsole subsystem for audit management, audit review, and monitoring of TOE status and alerts. It provides the interfaces for managing the gateways, transfers security policy configuration information to the gateways, collect information managed by the gateways and exports audit and IDS



VALIDATION REPORT  
Check Point Software Blades R7x

information to the OPSEC clients. It provides a cryptographically protected trusted for all security management server interfaces with other TOE subsystems and with OPSEC clients.

A Management Server host runs Management Server software on the underlying platform, which is comprised of a standard hardware platform and the SecurePlatform operating system.

### **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.

The Gateway subsystem is responsible for:

- Traffic filtering
- NAT
- Site-to-Site and remote access VPN
- IDS/IPS
- Non-administrative I&A
- Fault Tolerance (ClusterXL)

The Gateway subsystem receives security policy and other configuration information from the security management subsystem. It applies the security policy to information sent by users through the gateway subsystem, and sends log records and status information to the security management subsystem. All external information flows into and through the gateway subsystem are mediated by its stateful inspection capabilities. Security policy rules protect the gateway and the other TOE subsystems from external unauthorized access. The Gateway platform operating system is Check Point SecurePlatform R70.1 with R7x hotfix.

## **4.1 Physical Boundaries**

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

- Check Point Software Blades R7x Security Gateway software;
- Check Point Software Blades R7x Security Management software;
- Hardware Platforms and operating systems on which TOE Security Gateway and Security Management software is installed;
- Smart Console R7x Management GUI software;
- SSL Network Extender and SecureClient Mobile (SSL VPN) client software; and
- TOE Guidance

VALIDATION REPORT  
Check Point Software Blades R7x

## 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 R7x CC Evaluated Configuration Installation Guide, March 2012
- Check Point Software Blades R7x CC Evaluated Configuration Administration Guide, August 2012

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.

- SecurePlatform R71 Administration Guide, April 13, 2010
- Security Management Server R71 Administration Guide, April 22, 2010
- SmartView Monitor R71 Administration Guide, April 6, 2010
- Check Point IPS R71 Administration Guide, April 6, 2010
- Firewall Administration Guide Version R70, March 5, 2009
- Virtual Private Networks Administration Guide Version R70, April 23, 2009
- ClusterXL R70.1 Administration Guide, June 23, 2009
- VPN-1 FIPS 140-2 Non-Proprietary Security Policy, Version 2.9, October 2009

## 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 Rockville, Maryland from July 9 through July 19, 2012.

The evaluators received the TOE in the form that normal 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 R7x 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 R7x 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 R7x installed according to the Check Point Software Blades R7x 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 SAIC.

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

VALIDATION REPORT  
Check Point Software Blades R7x

- 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 R7x Security Target, Version 1.2, November 8, 2012

## 12 Acronym List

<b>CC</b>	Common Criteria
<b>CCTL</b>	CC Testing Laboratory
<b>CI</b>	Configuration Item
<b>CM</b>	Configuration Management
<b>CMP</b>	Configuration Management Plan
<b>CVE</b>	Common Vulnerabilities and Exposures
<b>CVS</b>	Concurrent Versioning System
<b>DoD</b>	Department of Defense
<b>EAL</b>	Evaluation Assurance Level
<b>FSP</b>	Functional Specification
<b>GUI</b>	Graphical User Interface
<b>HLD</b>	High-level Design
<b>ID</b>	Identity/Identification
<b>IP</b>	Internet Protocol
<b>IT</b>	Information Technology
<b>NIAP</b>	National Information Assurance Partnership
<b>NIST</b>	National Institute of Standards and Technology
<b>NSA</b>	National Security Agency
<b>OS</b>	Operating System
<b>PP</b>	Protection Profile
<b>SAIC</b>	Science Applications International Corporation
<b>SAR</b>	Security Assurance Requirement
<b>SFR</b>	Security Functional Requirement
<b>ST</b>	Security Target
<b>TOE</b>	Target of Evaluation
<b>TSF</b>	TOE Security Functions
<b>TSS</b>	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 R7x Security Target, Version 1.2, November 8, 2012.
- [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 R7x, parts 1 and 2 (and associated test report), version 1.0, October 15, 2012.