# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme

# Validation Report

# Check Point VSX

**Report Number:** **CCEVS-VR-10375-2012**
**Dated:** **11 June 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

# List of Tables

# 1 Executive Summary

The evaluation of **Check Point VSX** was performed by SAIC, in the United States and was completed in May 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. The criteria against which the Check Point VSX 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) 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 provides a virtualization environment for the implementation of network traffic information flow controls, providing controlled connectivity between two or more network environments. Information flow control functionality is implemented by one or more *Virtual Systems*, each logically equivalent to a Check Point Security Gateway appliance. Each Virtual System is associated with two or more logical interfaces. Check Point VSX maintains a separate domain of execution for each Virtual System, with separate security policies, state tables, configuration parameters, and audit logs. Routing tables are also virtualized, supporting the allocation of overlapping network address ranges for different Virtual Systems. Information flows between Virtual Systems are allowed or denied by an authorized administrator using a Mandatory access control policy.

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 VSX Security Target*, version 1.1, May 20, 2012. This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is Check Point VSX R67.10 in Combination with Provider-1 R71 with R7x hotfix software running on Check Point VSX appliances and Open Server hardware platforms running the Check Point SecurePlatform operating system. This Validation Report is not an endorsement of Check Point VSX 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 VSX ETR parts 1 and 2 and the associated test report produced by SAIC.

# 2 Identification

**Evaluated Product:**

Check Point VSX R67.10 in Combination with Provider-1 R71 with R7x hotfix

**Sponsor & Developer:**

Check Point Software Technologies LTD.
5 Ha'Solelim St
Tel Aviv, Israel 67897

**CCTL:**

Science Applications International Corporation
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

**Completion Date:**

May 2012

**CC:**

Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, September 2009

**Interpretations:**

There were no applicable interpretations used for this evaluation.

**CEM:**

Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 3, September 2009

**PP:**

U.S. Government Protection Profile for Traffic Filter 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 VSX R67.10 in combination with Provider-1 R71 with R7x hotfix which provides a virtualization environment for the implementation of network traffic information flow controls, providing controlled connectivity between two or more network environments.

**Disclaimer**

The information contained in this Validation Report is not an endorsement of the Check Point VSX by any agency of the U.S. Government and no warranty of Check Point VSX is either expressed or implied.

**Evaluation Personnel:** M. Evencie Pierre
Gary Grainger
Tammy Compton

**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 VSX Security Target, Version 1.1, May 20, 2012 |
| **TOE Identification:** | TOE Software Identification:<br>Check Point VSX R67.10.20[1] in combination with<br>Check Point Provider-1 R71 with R7x hotfix<br>(*TOE software also includes SmartConsole management GUI products that are installed on a standard PC (outside the TOE) running a Microsoft Windows operating system. The evaluated version for SmartConsole is: R71 with R7x hotfix.*)<br><br>TOE Hardware Identification:<br>The TOE consists of Check Point VSX software on an appliance platform running the Check Point SecurePlatform VSX operating system. The TOE includes the<br>following classes of appliances:<br>• Open Server hardware platforms (listed in section<br>• Check Point VSX-1 security appliances<br><br>Check Point Provider-1 software is always installed on a separate platform running the Check Point SecurePlatform operating system. These Provider-1 hardware platform includes<br>• Check Point Smart-1 50<br>• Check Point Smart-1 150 |

| | |
|---|---|
| | TOE Support Program Identification: Enterprise Software Subscription |
| **Operating Platform:** | Check Point VSX Appliances<br>• Check Point Appliances running the appliance specific build of the Check Point SecurePlatform VSX R67.10.20<br>• Non Check Point appliances<br>o VSX-1 3070<br>o VSX-1 9070<br>o VSX-1 9090<br>o VSX-1 11000 series<br>o VSX-1 11200 series (VSLS)<br>o Check Point 12200 VSX<br>o Check Point 12400 VSX<br>o Check Point 12600 VSX<br>o Check Point 21400 VSX<br>• Non Check Point appliances<br>o Check Point IAS Server M2, M6, M8, D1, D2, D6, D8, R2, R6, R8<br>o Dell PowerEdge 610, 710<br>o Fujitsu Primergy RX200 S6<br>o Fujitsu Primergy RX300 S6<br>o HP ProLiant DL360 G7<br>o HP ProLiant DL380 G7<br>o IBM System X x3550 M3<br>o IBM System X x3650 M3<br>Check Point Provider-1 Appliances<br>o Check Point Smart-1 50 Security appliance<br>• Check Point Smart-1 150 Security appliance |

# 3 Security Policy

## 3.1 Summary

Check Point VSX is a virtualization environment for the implementation of network traffic information flow controls, providing controlled connectivity between two or more network environments. VSX gateway network interfaces are associated with Virtual Systems. Virtual Systems run information flow control programs coded in Check Point's patented INSPECT language. Each Virtual System runs in a separate execution domain, and can read and write packets only from its associated interfaces. Administrator-defined conditional access controls constrain inter-System traffic.

The product 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 administrators have the authority to change the security policy rules.

Once an 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. User authentication may be achieved by a remote access client authenticating using IKE or TLS, against public key credentials held by the user. Administrators also need to authenticate to the TOE before they can use the Management GUIs to access Provider-1. The TOE can be optionally configured to perform user authentication with the support of external authentication servers in the IT environment.

TOE administration is also virtualized. A single Check Point Provider-1 installation can support many Customer management domains. A separate management database is maintained for each Customer, providing separation of security management data and audit logs between domains.

Administrators can perform both local and remote management of the TOE. AES encryption is used to protect remote management sessions. Administrator sessions are protected via a trusted path between the management GUI and Provider-1. Internal TOE communications between Check Point Provider-1 hosts and Check Point VSX gateways is also protected from disclosure and undetected modification.

Audit trail data and IDS System 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 an 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 an 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 VSX gateway protects itself and the Check Point Provider-1 installation 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 VSX gateways and Provider-1 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

**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. |

### 3.1.2. 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. |

### 3.1.3. 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 Customer data flowing through or stored within the TOE. |

### 3.1.4. 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. |

### 3.1.5. 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. |

# 4 Assumptions and Organizational Security Policies

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

## 4.1 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.<br>However, they are capable of error. |
| A.SINGEN | Information can not flow among the internal and external networks unless it passes through the TOE. |

## 4.2 Virtualization OSPs

The following OSP is defined in the ST to require compartmentalization of Customer data within the TOE.

| | |
|---|---|
| P.CUST | The TOE shall enforce separation between Customer networks and data and allow controlled sharing of information. |

## 4.3 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. |

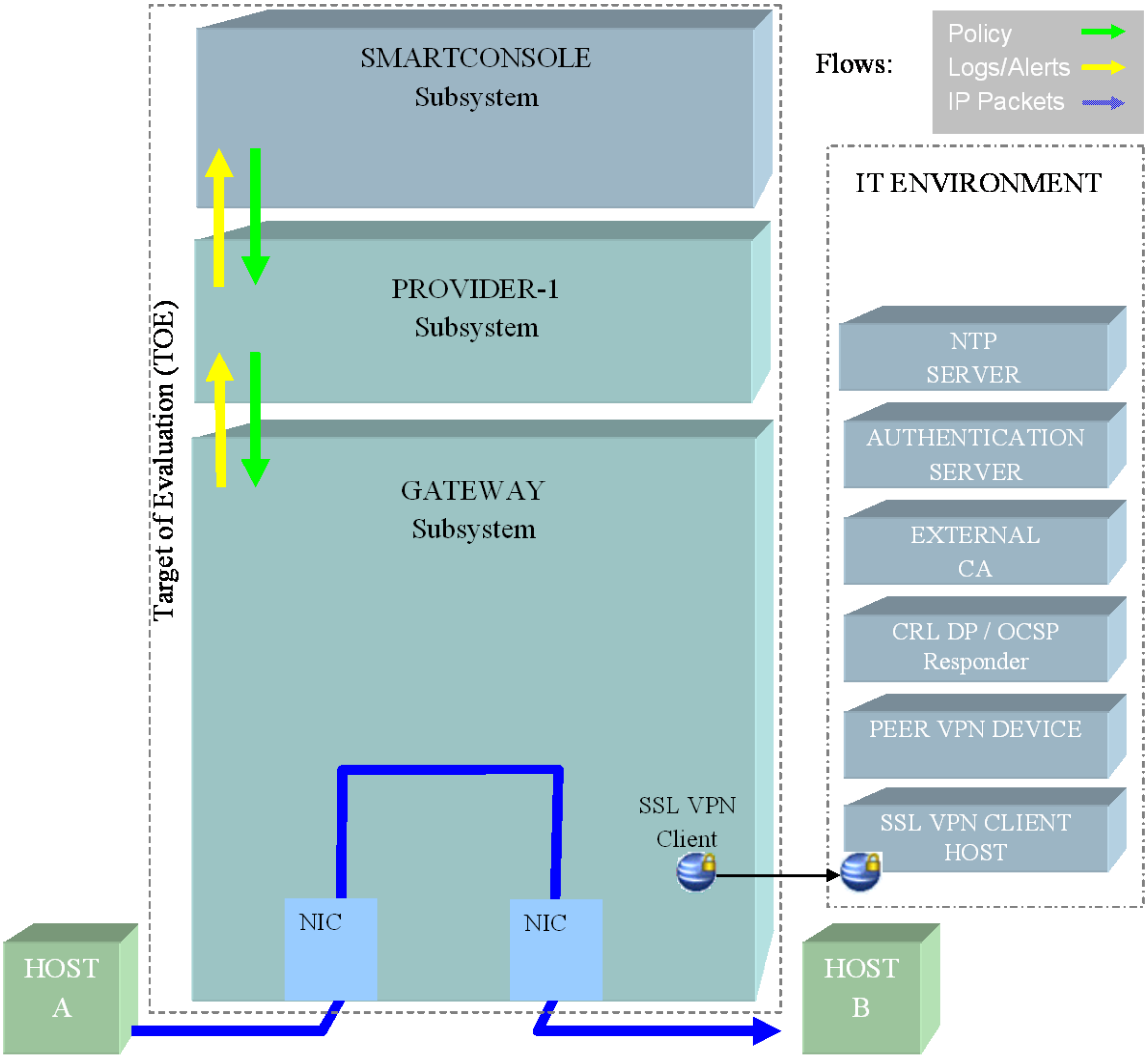
| | |
|---|---|
| P.MANAGE | The TOE shall only be managed by authorized users. |
| P.ACCESS | All data collected and produced by the TOE shall only be used for authorized purposes. |
| P.ACCACT | Users of the TOE shall be accountable for their actions within the IDS. |
| P.INTGTY | Data collected and 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. |
| | |

# 5 Architectural Information

Check Point VSX is a virtualization environment for the implementation of network traffic information flow controls, providing controlled connectivity between two or more network environments.

Check Point VSX is a TOE in parts, composed of three types of machines: SmartConsole hosts, Provider-1 hosts, and VSX 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.

**Top-Level TOE Subsystem Decomposition**



- SmartConsole 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 represents a set of management GUIs that includes four WIN32 applications running on a Windows operating system. The applications and their main roles are:
  - SmartDashboard – allows the administrator to manage CMA-specific and MDS-level (Global SmartDashboard) objects and security policy.
  - SmartView Tracker - provides the administrator the ability to review audit logs collected by CMAs and MDSs.
  - SmartView Monitor - provides the administrator with a means of monitoring TOE status in real time and receiving alerts.
  - Provider-1 MDG – allows an administrator to connect to the MDS for managing the Provider-1 installation, including definition and monitoring of Provider-1 hosts, high-availability, Customers, management GUI hosts, and administrator accounts.

The Provider-1 Subsystem executes the SmartConsole Subsystem's requests. All configuration data is stored on the Provider-1. Each application, when started, retrieves its data from the Provider-1.
The SmartConsole applications are launched by a common Launcher application that authenticates the administrator to Provider-1, and then hands off the user session to the appropriate application.

- Provider-1 Subsystem

The Provider-1 subsystem serves as an intermediate between the SmartConsole and Gateway subsystems in the TOE. In addition, the Provider-1 application provides for a Public Key Infrastructure (PKI) for the TOE (ICA), to support the Secure Internal Communications (SIC) capability.

The Provider-1 subsystem contains one Multi-Domain Server (MDS) per Provider-1 host, each hosting one or more Customer Management Add-ons (CMAs). Gateways and Virtual Systems are grouped in relation to Customers: each Gateway or Virtual System is managed by its assigned Customer's Provider-1 CMA.

Each CMA 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 MDS uses the same design as the CMA, but instead of managing Gateways and Virtual Systems, it manages CMAs. Global policy data entered by the TOE administrator via Global SmartDashboard is distributed to the CMAs. Log records and status information generated by the MDS can be accessed from SmartConsole.

The Provider-1 Subsystem supplies a Public Key Infrastructure for the TOE – the Internal Certificate Authority (ICA). The MDS ICA issues, renews and revokes certificates for administrators and for CMAs. The CMA ICAs issue, renew and revoke certificates for managed Gateways and Virtual Systems. SIC keys and certificates are pushed by the Provider-1 Subsystem to the various SIC entities within the TOE, and Certificate Revocation Lists (CRLs) are distributed to SIC entities.

The Provider-1 machine operating system is Check Point SecurePlatform R71 with R7x hotfix. The machine hardware is any of the hardware platforms identified in the ST as suitable for Provider-1.

- Provider-1 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.

Information flow control functionality is implemented by one or more *Virtual Systems*, each logically equivalent to a Check Point Security Gateway appliance. Each Virtual System is associated with two or more logical interfaces. Check Point VSX maintains a separate domain of execution for each Virtual System, with separate security policies, state tables, configuration parameters, and audit logs. Routing tables are also virtualized, supporting the allocation of overlapping network address ranges for different Virtual Systems. Information flows between Virtual Systems can be configured by defining Virtual Router and Virtual Switch entities that connect to multiple Virtual Systems.

The Gateway Platform operating system is Check Point SecurePlatform VSX R67.10. SecurePlatform 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.

## 5.1 Physical Boundaries

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

- Check Point VSX software, OS, and Hardware platform(s) on which the software is installed
- Check Point Provider-1 (Management) server software, OS and hardware
- Management GUI software
- TOE Guidance

# 6 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 VSX CC Evaluated Configuration Installation Guide, February 2012
- Check Point VSX CC Evaluated Configuration Administration Guide, May 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.

- Provider-1 R71 Admin Guide
- Security Management Server R71 Admin Guide
- Check Point IPS R71 Admin Guide
- SmartView Monitor R71Admin Guide
- SecurePlatform R71 Admin Guide
- Firewall R71 Admin Guide
- VPN R71 Admin Guide
- ClusterXL R71 Admin Guide

# 7 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.

## 7.1 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.

## 7.2 Independent Testing

Independent testing took place at the developer's location in Rockville, Maryland from January 3rd through January 11, 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 VSX 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 VSX 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 support for Nat-T with pre-shared secret, to verify frame tagged with unknown vlan, to verify handling of request containing routing information, to verify that users cannot re-use single-use authenticator for user authentication, to verify management restrictions at the SmartConsole interfaces, to verify management of default security attributes, to verify revocation of user security attributes, and to verify use of the CLI and DBeit tools restrictions.

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.

# 8 Evaluated Configuration

The TOE is Check Point VSX R67.10 installed according to the Check Point VSX CC Evaluated Configuration Installation Guide.

# 9 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

| | |
|---|---|
| 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.

# 10 Validator Comments/Recommendations

The validators have no comments or specific recommendations.

# 11 Annexes

Not applicable.

# 12 Security Target

Check Point VSX Security Target, Version 1.1, May 20, 2012

# 13 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 |
| **SAIC** | Science Applications International Corporation |
| **SAR** | Security Assurance Requirement |
| **SFR** | Security Functional Requirement |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functions |
| **TSS** | TOE Summary Specification |

# 14 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 VSX Security Target, Version 1.1, May 20, 2012.