National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Check Point Software Technologies Ltd.

5 Ha'Solelim Street

Tel Aviv 67897, Israel

Check Point Software Technologies Ltd. Security Gateway Appliances R77.30

Report Number: CCEVS-VR-10652-2015
Dated: December 31, 2015
Version: 0.2

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

ACKNOWLEDGEMENTS

Validation Team

Tony Chew
Rob Heald
Meredith Hennan
Jerome Myers
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Cornelius Haley
Ed Morris
Khai Van
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Check Point Software Technologies Ltd. Security Gateway Appliances R77.30. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in January 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant.

The Target of Evaluation (TOE) is Security Gateway Appliances R77.30. The product is a VPN Gateway and packet filtering firewall appliance. The product provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewalls.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Check Point Software Technologies Ltd. Security Gateway Appliances R77.30 (NDPP11e3/VPN/FW) Security Target, Version 0.91, 12/29/15 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Check Point Software Technologies Ltd. Security Gateway Appliances R77.30
	(Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012 with the following two extended packages:
	Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011
	Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, 15 April 2013
ST:	Check Point Software Technologies Ltd. Security Gateway Appliances R77.30 (NDPP11e3/VPN/FW) Security Target, Version 0.91, 12/29/2015, 2015
Evaluation Technical Report	Evaluation Technical Report for Check Point Software Technologies Ltd. Security Gateway Appliances R77.30 (NDPP11e3/VPN/FW), Version 0.2, 12/29/2015, 2015.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Check Point Software Technologies Ltd.
Developer	Check Point Software Technologies Ltd.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Tony Chew
	Rob Heald
	Meredith Hennan
	Jerome Myers
	Aerospace Corporation

3 Architectural Information

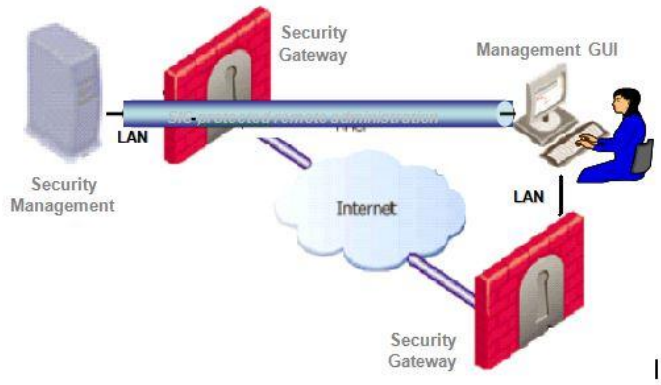
Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is Security Gateway Appliances R77.30. The product is a VPN Gateway and packet filtering firewall appliance. The product provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewalls.

3.1 TOE Architecture

The TOE is a network device with firewall capabilities for filtering traffic based on packet rules. It is a distributed system with support for a security management server, allowing remote administration over a protected IPsec connection. The 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, Security Gateway software, and hardware platform; and
- SmartConsole Management GUI software



Check Point Security Gateway R77.30 Security Gateway software is installed on a hardware platform in combination with an operating system (OS), in accordance with TOE guidance, in a FIPS 140-2 compliant mode. The OS supports the TOE by providing storage for audit trail, an IP stack for in-TOE routing, NIC drivers and an execution environment for daemons and security servers.

Check Point Security Gateway Appliances mediate information flows between clients and servers located on internal and external networks governed by the firewall. Proxy servers on the firewall, for the FTP service, requires 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, against either a pre-shared key or certificate. 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.

Check Point's virtual machine engine supports the definition of separate execution domains for Virtual Systems. Incoming IP packets bind to an appropriate VS corresponding to the logical interface (i.e. physical or virtual LAN interface) on which they are received, and the VS that is defined to receive the packet from that interface. The packets are labeled with the VSID, and are handled in the context of that VS's execution domain, until they are dropped, forwarded out of the gateway, or handed to another VS according to administrator-defined rules. While the packet filtering based upon VSIDs is included in the scope of the evaluation, the architectural aspects of domain separation is not covered.

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.

Security Management is performed using the SmartConsole Management GUI software. The Security Management software, OS and hardware platform are collectively identified as the 'Security Management server'.

One or more Security Gateway appliances are managed by a Security Management server installation that maintains security policy information for the gateways, and collects audit records from the gateways for review by TOE administrators. The audit records may also be sent to an external audit server.

The evaluated configuration supports both local and remote administration. Local administration is via a directly connected console. Remote administration is via an IPsec protected connection between the Security Management Server and the Gateway Appliance or via a remote CLI protected via an IPsec connection.

3.2 Physical Boundaries

There are three different hardware platforms for the Check Point Security Gateway Appliances and Security Management Appliances including Check Point IAS appliances integrated with HP and Fujitsu. All platforms use the same image. The difference is mainly in hardware makeup and physical ports. All platforms are x86 based hardware.

The SmartConsole Management GUI software is installed on a Windows workstation (Windows 8, Windows 7). Authorized administrators use the GUI software or CLI to remotely manage the TOE.

The TOE may be configured to interact with external servers:

- External Certificate Authority (CA).
- External certificate validation server (HTTP or LDAP CRLDP, OCSP).
- External NTP time-synchronization server
- External audit server (OPSEC)

3.3 TOE Evaluated Configuration

Below is a list of hardware platforms included in the evaluation. All platforms are x86 based hardware.

Note: The models identified using the '**' convention use a zero-justified numbering system for the licensed software blades, e.g. the 'Check Point 21412 Appliance' would support up to 12 software blade licenses, whereas the 'Check Point 21407' Appliance' would be the same hardware model supporting up to 7 blades

- Check Point 22** Appliances
- Check Point 42**, 44**, 46**, 48** Appliances
- Check Point 122**, 124**, 126**, 135**, 138** Appliances
- Check Point 214**, 216**, 217**, 218** Appliances

The following commodity hardware platforms are included in the evaluated configuration for Security Gateway and Security Management software, running the GAiA R77.30 operating system.

Check Point IAS appliances	D1, D2, D6, D8, R2, R6, R8
Fujitsu	Primergy RX100 S6, S7
	Primergy RX200 S6, S7
	Primergy RX300 S6, S7
HP	ProLiant DL120 G7
	ProLiant DL320e G8
	ProLiant DL360 G7
	ProLiant DL380 G7
	ProLiant DL360p G8
	ProLiant DL380p G8

The following Check Point security appliance models are included in the evaluated configuration for the Security Management software, running the GAiA R77.30 operating system:

- Smart-1 5
- Smart-1 25
- Smart-1 50
- Smart-1 150
- Smart-1 205
- Smart-1 210
- Smart-1 225
- Smart-1 3050
- Smart-1 3150

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security Audit
2. Cryptographic support
3. User data protection
4. Stateful Traffic Filtering Firewall/VPN Packet Filtering
5. Identification and authentication
6. Security Management
7. Protection of the TSF
8. TOE Access
9. Trusted path/channels

4.1 Security Audit

The Gateway Appliances can be configured to store logs locally, forward logs to the Security Management Server, or both. If configured to send logs to the Security Management Server, in the event of a loss of network connectivity to the Security Management Server, then the Gateway Appliance will store locally until the connection is restored. The TOE can be configured to send audit logs to a syslog server as well. The connection between the TOE and remote server is protected with IPsec. Finally, note that the Gateway Appliances can be configured such that if they run out of disk space for local logs, they can block all connections.

4.2 Cryptographic support

The TOE uses a Check Point cryptographic module that has received Cryptographic Algorithm Validation Program (CAVP) certificates for all cryptographic functions claimed in this ST. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

4.3 User data protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

4.4 Stateful Traffic Filtering Firewall/VPN Packet Filtering

The TOE supports many protocols for packet filtering including icmpv4, icmpv6, ipv4, ipv6, tcp and udp. The firewall rules implement the SPD rules (permit, deny, bypass). Each rule can be configured to log status of packets pertaining to the rule. All codes under each protocol are implemented. The TOE supports FTP for stateful filtering.

The TOE mediates the information flows according to an administrator-defined policy. Some of the traffic may be either silently dropped or rejected (with notification to the presumed source).

The TOE's firewall and VPN capabilities are controlled by defining an ordered set of rules in the Security Rule Base. The Rule Base specifies what communication will be allowed to pass and what will be blocked. It specifies the source and destination of the communication, what services can be used, at what times, whether to log the connection and the logging level.

4.5 Identification and authentication

The TOE implements a password based authentication mechanism that identifies operators via usernames. Passwords are stored obfuscated, and passwords for local login are stored Unix hashed. The TOE supports passwords with lengths 15 or greater characters and all special characters as required by the Protection Profiles.

4.6 Security management

The TOE allows both local and remote administration for management of the TOE's security functions. The TOE creates and maintains profiles for configured administrators. An administrator can log in locally to the TOE using a serial connection. The administrator is greeted with a console environment, where configuration is mainly done through command-line syntax. The local login operates in a Unix shell. There are two remote administration interfaces. The first remote administration interface is executed through a Graphical User Interface using TLS over IPsec. Though the connections from a browser to the TOE are TLS connections, the TOE requires an IPSec connection to wrap the TLS connection. The second remote administration interface is a command line interface (CLI) using SSH over IPsec.

4.7 Protection of the TSF

The TOE includes capabilities to protect itself from unwanted modification as well as protecting its persistent data.

The TOE does not store passwords in plaintext. They are obfuscated, and UNIX shell login passwords are stored as a UNIX hash. The TOE does not support any command line capability to view any cryptographic keys generated or used by the TOE.

The TOE only allows updates after their signature is successfully verified. The TOE update mechanism uses ECDSA with SHA-512 and P-521 to verify the signature of the update package.

The TOE's FIPS executables are signed using ECDSA with SHA-512 and P-521. For other executables a hash is computed during system installation and configuration and during updates.

During power-up the integrity of all executables is verified. If an integrity test fails in the cryptographic module, the system will enter a kernel panic and will fail to boot up. If an integrity test fails due to a non-matching hash, a log is written. Also during power-up, algorithms are tested in the kernel and user-space. If any of these test fail, the TOE is not operational for users.

The TOE is able to terminate interactive sessions if the session is inactive for a set period of time. The time can be configured via the TOE configuration. Also, the TOE can lock a user out based on the number of failed logins. This can also be configured via the TOE configuration.

4.8 TOE Access

Access to the TOE is mainly through a Security Management Server. The connection between the Security Management Server and the TOE is secured via IPsec. The second remote administration interface is CLI and is also protected with IPsec. The TOE also provides a local login console, which is a Unix shell environment.

4.9 Trusted path/channels

The TOE protects all communications with outside entities using IPsec communications only. This is mainly to fulfill a Commercial Solutions for Classified (CSfC) requirement for communications. Any other protocol (such as SSH or TLS) is wrapped in an IPsec tunnel.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012 (NDPP11e3)
- Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011 (STFFEP10)
- Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, 15 April 2013(VPNGEP11)

That information has not been reproduced here and the referenced Protection Profiles should be consulted if there is interest in that material.

6 Documentation

The following documents were available with the TOE for evaluation:

- Check Point Software Technologies LTD. Security Gateway Appliances R77.30 Common Criteria Supplement, Version 0.2, December 29, 2015
- Check Point Software Technologies LTD. R77.30 Installation Guide, Version1.0, December 9, 2015

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report (NDPP11e3/STFFEP10/VPNGEP11) for Check Point Software Technologies Ltd. Security Gateway Appliances, Version 0.3, 12/29/2015, and summarized in the Assurance Activities Report (NDPP11E3/VPNGEP11/STFFEP10) for Security Gateway Appliances R77.30 (TSS Activities), Version 0.4, 12/29/2015, which is publically available.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDPP11e3/STFFEP10/VPNGEP11including the tests associated with optional and selection-based requirements.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL1 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

8.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Security Gateway Appliances R77.30 appliance that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDPP11e3/STFFEP10/VPNGEP11 related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDPP11e3/STFFEP10/VPNGEP11 and recorded the results in a Test Report, summarized in the Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE. The evaluator also performed fuzz testing as required by the VPNGEP11.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

8.8 Clarifications of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the NDPP11e3/STFFEP10/VPNGEP11. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
5. This evaluation covers packet filtering based upon Virtual System IDs, however the architectural aspects of execution domains and domain separation are not covered.

9 Validator Comments/Recommendations

The validator comments are covered under the Clarifications of Scope section.

10 Annex

Not applicable.

11 Security Target

The Security Target is identified as: Check Point Software Technologies Ltd. Security Gateway Appliances R77.30 (NDPP11e3/VPN/FW) Security Target, Version 0.91, 12/29/2015, 2015.

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012

[5] Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011

[6] Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, 15 April 2013

[7] Check Point Software Technologies Ltd. Security Gateway Appliances R77.30 (NDPP11e3/VPN/FW) Security Target, Version 0.91, 12/29/2015, 2015 (ST)