National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

collaborative Protection Profile for Stateful Traffic Filter Firewalls

Version 2.0 + Errata 20180314

14 March 2018

Report Number: CCEVS-VR-PP-0051
Dated: 05 September 2019
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

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
Gossamer Security Solutions
Catonsville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0 + Errata 20180314 (cPP_FW_V2.0E). It presents a summary of the cPP_FW_V2.0E and the evaluation results.

Gossamer Security Solutions, located in Catonsville, Maryland, performed the evaluation of cPP_FW_V2.0E concurrent with the first product evaluation against the PP's requirements. The evaluated product was Cisco Next-Generation Firewalls (NGFW) running ASA version 9.8 and FX-OS version 2.2 on the 2k family.

This evaluation addressed the base requirements of cPP_FW_V2.0E and several of the additional requirements contained in Appendices A and B.

The Validation Report (VR) author independently performed an additional review of the PP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements.

The evaluation determined that cPP_FW_V2.0E is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this VR has been evaluated at NIAP approved CCTLs 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). The Security Target (ST) includes material from both cPP_FW_V2.0E and the VPN Gateway Extended Package; completion of the ASE work units satisfied the APE work units for cPP_FW_V2.0E, but only for those parts of the Security Target that were relevant to this PP.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against PPs that contain Evaluation Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of cPP_FW_V2.0E was performed concurrent with the first product evaluation against the PP's requirements. In this case, the Target of Evaluation (TOE) was Cisco Next-Generation Firewalls (NGFW) running ASA version 9.8 and FX-OS version 2.2 on the 2k family, evaluated by Gossamer Security Solutions in Catonsville, Maryland, United States of America

These evaluations addressed the base requirements of cPP_FW_V2.0E, and several of the additional requirements contained in Appendices A and B.

cPP_FW_V2.0E contains a set of "base" requirements that all conformant STs must include, and additionally contains "Optional" and "Selection-based" requirements. Optional

requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE.

A specific ST may not include all non-base requirements, so the initial use of the PP addresses (in terms of the PP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ workunits performed against cPP_FW_V2.0E. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of cPP_FW_V2.0E were evaluated.

The following identifies the PP subject of the evaluation/validation, as well as the supporting information from the evaluation performed against this PP and any subsequent evaluations that address additional optional and/or selection-based requirements in the cPP_FW_V2.0E.

Protection Profile	collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0 + Errata 20180314, 14 March 2018
ST (Base)	Cisco Adaptive Security Appliances on FP2100 Security Target, Version 0.27, 9 July 2018
Assurance Activity Report (Base)	Assurance Activity Report (FWcPP20E/VPNGWEP21) for Cisco Adaptive Security Appliances on FP2100, Version 0.5, 09 July 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTLs	Gossamer Security Solutions, Catonsville, Maryland

3 cPP_FW_V2.0E Description

The cPP_FW_V2.0E specifies information security requirements for firewalls, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

This collaborative Protection Profile (cPP) defines requirements for the evaluation of Stateful Traffic Filter Firewalls. Such products are generally boundary protection devices, such as dedicated firewalls, routers, or perhaps even switches designed to control the flow of information between attached networks. While in some cases, firewalls implementing security features serve to segregate two distinct networks – a trusted or protected enclave and an untrusted internal or external network such as the Internet – that is only one of many possible applications. It is common for firewalls to have multiple physical network connections enabling a wide range of possible configurations and network information flow policies.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.PHYSICAL_PROTECTION	The firewall device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the firewall's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the firewall and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the firewall that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the firewall.
A.LIMITED_FUNCTIONALITY	The firewall device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the firewall device should not provide a computing platform for general purpose applications (unrelated to networking/filtering functionality).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the firewall device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the firewall. The firewall device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The firewall device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the firewall device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING[1]	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate

[1] Note that A.COMPONENTS_RUNNING only applies to a TOE whose security functionality is implemented across multiple distributed components.

	that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on firewall equipment when the equipment is discarded or removed from its operational environment.

4.2 Threats

The following table contains applicable threats.

Table 2: Threats

Threat Name	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the firewall by nefarious means such as masquerading as an administrator to the firewall, masquerading as the firewall to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between the firewall and a network device. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the firewall and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target firewalls that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the firewall itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The

	result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the firewall itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the firewall without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and firewall data enabling continued access to the firewall and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or firewall credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the firewall. Having privileged access to the firewall provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.NETWORK_DISCLOSURE	An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.
T.NETWORK_ACCESS	With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.

T.NETWORK_MISUSE	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others.
T.MALICIOUS_TRAFFIC	An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.

4.3 Organizational Security Policies

The following table contains applicable organizational security policies.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
There are no security objectives defined for the TOE.	

The following table contains security objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	Environmental Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING[2]	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or

[2] Note that OE.COMPONENTS_RUNNING only applies to a TOE whose security functionality is implemented across multiple distributed components.

	failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5 Requirements

As indicated above, requirements in the cPP_FW_V2.0E are comprised of the "base" requirements and additional requirements that are optional or selection-based, or objective. The following table contains the "base" requirements that were validated as part of the Cisco evaluation activities referenced above.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Cisco NGFW
	FAU_GEN.2: User Identity Association	Cisco NGFW
	FAU_STG_EXT.1: Protected Audit Event Storage	Cisco NGFW
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Cisco NGFW
	FCS_CKM.2: Cryptographic Key Establishment	Cisco NGFW
	FCS_CKM.4: Cryptographic Key Destruction	Cisco NGFW
	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)	Cisco NGFW
	FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)	Cisco NGFW
	FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)	Cisco NGFW
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)	Cisco NGFW
	FCS_RBG_EXT.1: Random Bit Generation	Cisco NGFW
FDP: User Data Protection	FDP_RIP.2: Full Residual Information Protection	Cisco NGFW
FFW: Firewall	FFW_RUL_EXT.1: Stateful Traffic Filtering	Cisco NGFW
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Management	Cisco NGFW
	FIA_PMG_EXT.1: Password Management	Cisco NGFW
	FIA_UIA_EXT.1: User Identification and Authentication	Cisco NGFW
	FIA_UAU_EXT.2: Password-based Authentication Mechanism	Cisco NGFW
	FIA_UAU.7: Protected Authentication Feedback	Cisco NGFW
FMT: Security Management	FMT_MOF.1/ManualUpdate: Management of Security Functions Behavior	Cisco NGFW

	FMT_MTD.1/CoreData: Management of TSF Data	Cisco NGFW
	FMT_SMF.1: Specification of Management Functions	Cisco NGFW
	FMT_SMR.2: Restrictions on Security Roles	Cisco NGFW
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Administrator Passwords	Cisco NGFW
	FPT_SKP_EXT.1: Protection of TSF Data (For Reading of all Pre-Shared, Symmetric and Private Keys)	Cisco NGFW
	FPT_STM_EXT.1: Reliable Time Stamps	Cisco NGFW
	FPT_TST_EXT.1: TSF Testing	Cisco NGFW
	FPT_TUD_EXT.1: Trusted Update	Cisco NGFW
FTA: TOE Access	FTA_SSL_EXT.1: TSF-initiated Session Locking	Cisco NGFW
	FTA_SSL.3: TSF-initiated Termination	Cisco NGFW
	FTA_SSL.4: User-initiated Termination	Cisco NGFW
	FTA_TAB.1: Default TOE Access Banners	Cisco NGFW
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	Cisco NGFW
	FTP_TRP.1/Admin: Trusted Path	Cisco NGFW

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG.1: Protected Audit Trail Storage	PP Evaluation
	FAU_STG_EXT.2/LocSpace: Counting Lost Audit Data	PP Evaluation
	FAU_STG.3/LocSpace Action in Case of Possible Audit Data Loss	PP Evaluation
FCO: Communication	FCO_CPC_EXT.1: Component Registration Channel Definition	PP Evaluation
FFW: Firewall	FFW_RUL_EXT.2: Stateful Filtering of Dynamic Protocols	Cisco NGFW
FIA: Identification and Authentication	FIA_X509_EXT.1/ITT: X.509 Certificate Validation	PP Evaluation
FMT: Security Management	FMT_MOF.1/Services: Management of Security Functions Behaviour	Cisco NGFW
	FMT_MTD.1/CryptoKeys: Management of TSF Data	PP Evaluation
FPT: Protection of the TSF	FPT_ITT.1: Basic Internal TSF Data Transfer Protection	PP Evaluation
FTP: Trusted Path/Channels	FTP_TRP.1/Join: Trusted Path	PP Evaluation

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_DTLSC_EXT.1: DTLS Client Protocol	PP Evaluation
	FCS_DTLSC_EXT.2: DTLS Client Protocol – with Authentication	PP Evaluation
	FCS_DTLSS_EXT.1: DTLS Server Protocol	PP Evaluation
	FCS_DTLSS_EXT.2: DTLS Server Protocol with Mutual Authentication	PP Evaluation
	FCS_HTTPS_EXT.1: HTTPS Protocol	Cisco NGFW
	FCS_IPSEC_EXT.1: IPsec Protocol	Cisco NGFW
	FCS_SSHC_EXT.1: SSH Client Protocol	PP Evaluation
	FCS_SSHS_EXT.1: SSH Server Protocol	Cisco NGFW
	FCS_TLSC_EXT.1: TLS Client Protocol	PP Evaluation
	FCS_TLSC_EXT.2: TLS Client Protocol with Authentication	Cisco NGFW
	FCS_TLSS_EXT.1: TLS Server Protocol	Cisco NGFW
	FCS_TLSS_EXT.2: TLS Server Protocol with Mutual Authentication	PP Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.1/Rev: X.509 Certificate Validation	Cisco NGFW
	FIA_X509_EXT.2: X.509 Certificate Authentication	Cisco NGFW
	FIA_X509_EXT.3: X.509 Certificate Requests	Cisco NGFW
FMT: Security Management	FMT_MOF.1/AutoUpdate: Management of Security Functions Behaviour	PP Evaluation
	FMT_MOF.1/Functions: Management of Security Functions Behaviour	PP Evaluation
FPT: Protection of the TSF	FPT_TST_EXT.2: Self-Tests Based on Certificates	PP Evaluation
	FPT_TUD_EXT.2: Trusted Update Based on Certificates	PP Evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the cPP_FW_V2.0E.

Table 9: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Cisco NGFW
	ASE_ECD.1: Extended Components Definition	Cisco NGFW

	ASE_INT.1: ST Introduction	Cisco NGFW
	ASE_OBJ.1: Security Objectives for the Operational Environment	Cisco NGFW
	ASE_REQ.1: Stated Security Requirements	Cisco NGFW
	ASE_SPD.1: Security Problem Definition	Cisco NGFW
	ASE_TSS.1: TOE Summary Specification	Cisco NGFW
ADV: Development	ADV_FSP.1 Basic Functional Specification	Cisco NGFW
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Cisco NGFW
	AGD_PRE.1: Preparative Procedures	Cisco NGFW
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Cisco NGFW
	ALC_CMS.1: TOE CM Coverage	Cisco NGFW
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Cisco NGFW
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Cisco NGFW

7 Results of the Evaluation

Note that for APE elements and work units that are identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 10: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Cisco NGFW; PP Evaluation
APE_ECD.1	Pass	Cisco NGFW; PP Evaluation
APE_INT.1	Pass	Cisco NGFW; PP Evaluation
APE_OBJ.1	Pass	Cisco NGFW; PP Evaluation
APE_REQ.1	Pass	Cisco NGFW; PP Evaluation
APE_SPD.1	Pass	Cisco NGFW; PP Evaluation

8 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 as interpreted by the supplemental guidance in the cPP_FW_V2.0E Evaluation Activities to determine whether or not the claims made are justified.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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.

9 Bibliography

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

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

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 4, dated: September 2012.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0 + Errata 20180314, 14 March 2018.

[7] Cisco Adaptive Security Appliances on FP2100 Security Target, Version 0.27, 9 July 2018.

[8] Assurance Activity Report (FWcPP20E/VPNGWEP21) for Cisco Adaptive Security Appliances on FP2100, Version 0.5, 09 July 2018.