National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0, February 27, 2015

Report Number: CCEVS-VR-PP-0034
Dated: April 20, 2017
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, 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 the collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0 (cPPFW10). It presents a summary of the cPPFW10 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the cPPFW10 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Cisco's Adaptive Security Appliances and ASA Virtual Version 9.6 (Version Code 2). The evaluation was performed by Gossamer Security Solutions Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, in the United States and was completed in April 2017. This evaluation addressed the base requirements of the cPPFW10, as well as a few of the optional and selection-based requirements contained in the Appendices.

The information in this report is largely derived from the Assurance Activity Report (AAR), written by Gossamer Security Solutions.

The evaluation determined that the cPPFW10 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP 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). Because the ST contains only material drawn directly from the cPPFW10, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

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

The validation team found that the evaluation showed that the cPPFW10 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

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 Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles and Extended Packages containing Assurance 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 the cPPFW10 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Cisco Adaptive Security Appliances and ASA Virtual Version 9.6 (Version Code 2), provided by Gossamer Security Solutions Common Criteria Testing Laboratory (CCTL) in Catonsville, MD in the United States and was completed in April 2017.

The cPPFW10 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are either optional or selection-based depending on the requirement in question. The vendor may choose to include such requirements in the ST and still claim conformance to this PP. If the vendor's TOE performs capabilities that are governed by any additional requirements, that vendor is expected to claim all of the additional requirements that relate to these capabilities.

Because these additional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements that are incorporated into that initial ST.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional requirements in the cPPFW10.

Protection Profile	*collaborative Protection Profile for collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0, February 27, 2015*
ST (Base)	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
Assurance Activity Report (Base)	Assurance Activity Report Cisco Adaptive Security Appliances and ASA Virtual Version 9.6 (Version Code 2) Version 1.0, March 27, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL (base and additional)	Gossamer Security Solutions, 1352 N Rolling Rd Catonsville, MD USA
CCEVS Validators (base)	Marybeth Panock, Aerospace Corporation Kenneth Stutterheim, Aerospace Corporation
CCEVS Validators (Additional)	

3 cPPFW Description

The requirements in the cPPFW10 apply to a stateful traffic filter firewall network traffic is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats. It has the ability to match packets to a known active (and allowed) connection to permit them and drop others. The firewall often serves as a boundary device between two separate network security domains, and, as such, must provide a minimal set of common security functionality. These functional requirements define authorized communication with the firewall, audit capabilities, user access, update processes, and self-test procedures for critical components.

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 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.

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The firewall 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 pqhysical 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 is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the firewall should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
A.TRUSTED_ADMINSTRATOR	The authorized administrator(s) for the firewall 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 is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the firewall.

Table 1: Assumptions

4.2 Threats

Threat	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

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_COMMUNICATIONS_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., 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
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 include 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	A component of the firewall may fail during start-up or during operations causing a compromise or failure in the security functionality of the firewall, leaving the firewall susceptible to

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.

Table 2: Threats

4.3 Organizational Security Policies

Organizational Security Policy	Organizational Security Policy 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.

Table 3: Organizational Security Policies

4.4 Security Objectives

The following table contains objectives for the Operational Environment.

TOE Security Obj.	TOE 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	TOE 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.

Table 4: Security Objectives for the Operational Environment

5 Requirements

As indicated above, requirements in the cPPFW10 are comprised of the "base" requirements. The following are table contains the "base" requirements that were validated as part of the evaluation activity referenced above.

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FAU_GEN.2: User Identity Association	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FAU_STG_EXT.1: Protected Audit Event Storage	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FCS: Cryptographic Support	FCS_CKM.1 Cryptographic Key Generation	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_CKM.2 Cryptographic Key Establishment	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_CKM_EXT.4: Cryptographic Key Destruction	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_COP.1(1) Cryptographic Operation- AES Data Encryption/Decryption	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_COP.1(2): Cryptographic Operation- Signature Generation and Verification	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_COP.1(3) Cryptographic Operation- Hash Algorithm	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_COP.1(4) Cryptographic Operation- Keyed Hash Algorithm	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_RBG_EXT.1 Random Bit Generation Services	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FDP: User Data Protection	FDP_RIP.2: Full Residual Information Protection	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FIA: Identification and Authentication	FIA_PMG_EXT.1: Password Management	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FIA_UIA_EXT.1: User Identification and Authentication	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

	FIA_UAU_EXT.2: Password-based Authentication Mechanism	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FIA_UAU.7: Protected Authentication Feedback	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FIA_X509_EXT.1: Certificate Validation	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FIA_X509_EXT.2: Certificate Authentication	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FIA_X509_EXT.3: Certificate Requests	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FMT: Security Management	FMT_MOF.1(1)/TrustedUpdate: Management of Security Functions Behavior	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FMT_MTD.1: Management of TSF Data	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FMT_SMF.1: Specification of Management Functions	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FMT_SMR.2: Restriction on Security Roles	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FPT: Protection of the TSF	FPT_SKP_EXT.1: Protection of TSF Data (Symmetric Keys)	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FPT_APW_EXT.1: Protection of Administrator Passwords	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FPT_STM.1: Reliable Time Stamps	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FPT_TST_EXT.1: TSF Testing	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FPT_TUD_EXT.1: Integrity for Installation and Update	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FTA: TOE Access	FTA_SSL_EXT.1: TSF-initiated Session Locking	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FTA_SSL.3: TSF-initiated Termination	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FTA_SSL.4: User-initiated Termination	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

	FTA_TAB.1 Default TOE Access Banners	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FTP_TRP.1 Trusted Path	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FFW: Stateful Traffic Filtering	FFW_RUL_EXT.1: Stateful Traffic Filtering	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

Table 5: Base Requirements

The following table contains the additional optional requirements contained in Appendix A, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG.1: Protected Audit Trail Storage	PP Evaluation
	FAU_STG_EXT.2: Counting Lost Audit Data	PP Evaluation
	FAU_STG_EXT.3: Display Warning for Local Storage Space	PP Evaluation
FMT: Security Management	FMT_MOF.1(1)/TrustedUpdate: Management of Security Functions Behavior	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FMT_MOF.1(1)/Audit: Management of Security Functions Behavior	PP Evaluation
	FMT_MOF.1(2)/Audit: Management of Security Functions Behavior	PP Evaluation
	FMT_MOF.1(1)/AdminAct: Management of Security Functions Behavior	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FMT_MOF.1(2)/AdminAct: Management of Security Functions Behavior	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FMT_MOF.1(1)/LocSpace: Management of Security Functions Behavior	PP Evaluation
	FMT_MTD.1/AdminAct: Management of TSF Data	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FPT: Protection of the TSF	FPT_FLS.1/LocSpace: Failure with Preservation of Secure State	PP Evaluation

Requirement Class	Requirement Component	Verified By
FFW: Firewall	FFW_RUL_EXT.2: Stateful Traffic Filtering of Dynamic Protocols	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

Table 6: Optional Requirements

The following table contains the additional 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). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
Cryptographic Support	FCS_HTTPS_EXT.1 HTTPS Protocol	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_IPSEC_EXT.1 IPsec Protocol	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_SSHC_EXT.1 SSH Client Protocol	PP Evaluation
	FCS_SSHS_EXT.1 SSH Server Protocol	PP Evaluation
	FCS_TLSC_EXT.1: TLS Client Protocol	PP Evaluation
	FCS_TLSC_EXT.2 TLS Client Protocol with Authentication	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_TLSS_EXT.1 TLS Server Protocol	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FCS_TLSS_EXT.2 TLS Server Protocol with Mutual Authentication	PP Evaluation
FPT: Protection of the TSF	FPT_TST_EXT.2: Self tests based on certificates	PP Evaluation
	FPT_TUD_EXT.2:Trusted Updates based on certificates	PP Evaluation
FMT: Security Management	FMT_MOF.1(2)/TrustedUpdate: Management of Security Functions Behavior	PP Evaluation

Table 7: Selection-Based Requirements

6 Assurance Requirements

The following are the assurance requirements contained in the cPPFW10:

Requirement Class	Requirement Component	Verified By
ADV: Development	ADV_FSP.1 Basic Functional Specification	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

AGD: Guidance documents	AGD_OPE.1: Operational User Guidance	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	AGD_PRE.1: Preparative Procedures	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	ALC_CMS.1: TOE CM Coverage	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	ALC_TSU_EXT.1: Timely Security Updates	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

Table 8: Assumptions

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
APE_ECD.1	Pass	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
APE_INT.1	Pass	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
APE_OBJ.2	Pass	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
APE_REQ.1	Pass	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

Table 9: Evaluation Results

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 cPPFW10 Assurance 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.
- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Cisco Systems, Cisco Adaptive Security Appliances and ASA Virtual Version 9.6 *Security Target* Version 1.0, January 20, 2017

[7] Cisco Systems, Cisco Adaptive Security Appliances and ASA Virtual Version 9.6*Assurance Activity Report* Version 1.0, February 1, 2017

[8] collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0, Version 1.2, February 27, 2015