National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway

Version 2.0, December 1, 2015

Report Number: CCEVS-VR-PP-0033
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 Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, Version 2.0 (VPNGWEP20). It presents a summary of the VPNGWEP20 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the VPNGWEP20 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 VPNGWEP20, 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 VPNGWEP20 is both Common Criteria Part 2 Extended and Part 3 Conformant. The EP 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 VPNGWEP20, 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 VPNGWEP20 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 EP.

In order to promote thoroughness and efficiency, the evaluation of the VPNGWEP20 was performed concurrent with the first product evaluation against the EP. 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 VPNGWEP20 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 EP. 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 EP will address (in terms of the EP evaluation) the base requirements that are incorporated into that initial ST.

The following identifies the EP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this EP, as well as subsequent evaluations that address additional requirements in the VPNGWEP20.

Protection Profile	*collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, Version 2.0, December 1, 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 Conformant
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 VPNGWEP20 Description

The VPNGWEP20 specifies information security requirements for VPN gateways that go above and beyond the security requirements that are considered to be universal for generic network devices. Since the EP builds on the NDcPP, conformant TOEs are obligated to implement the functionality required in the NDcPP along with the additional functionality defined in this EP.

In particular, a VPN Gateway establishes a secure tunnel that provides an authenticated and encrypted path to another site(s) and thereby decreases the risk of exposure of information transiting an untrusted network. The baseline requirements of this EP are those determined necessary for a multi-site VPN Gateway device.

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.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be e

Table 1: Assumptions

4.2 Threats

Threat	Threat Definition
T.NETWORK_DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a *phishing* episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information.
T. NETWORK_ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network.
T.NETWORK_MISUSE	Devices located outside the protected network, while permitted to access particular *public* services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network.
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.

T.REPLAY_ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a "replay" attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: • Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome.

Table 2: Threats

4.3 Organizational Security Policies

The VPNGWEP20 does not define organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

TOE Security Objectives	TOE Security Objective Definition
O.CRYPTOGRAPHIC_FUNCTIONS	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement a cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.
O.AUTHENTICATION	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (IPSec) will allow a VPN peer to establish VPN connectivity with another VPN peer. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.
O.ADDRESS_FILTERING	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, compliant TOE's will implement Packet Filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) and/or receiving (destination) applicable network traffic as well as on established connection information.
O.FAIL_SECURE	There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism and provide signature-based validation of updates to the TSF.
O.PORT_FILTERING	To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or

	receiving (destination) port (or service) identified in the network traffic as well as on established connection information.

Table 3: Security Objectives for the TOE

The following table contains objectives for the Operational Environment.

TOE Security Objectives	TOE Security Objective Definition
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

Table 4: Security Objectives for the Operational Environment

5 Requirements

As indicated above, requirements in the VPNGWEP20 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
FCS: Cryptographic Support	FSC_CKM.1/IKE: Cryptographic Key Generation (for IKE Peer Authentication)	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FIA_X509_EXT.4: X.509 Certificate Identity	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
FPF: Packet Filtering	FPF_RUL_EXT.1: Packet Filtering	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/SelfTest: Fail Secure	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

Table 5: Base Requirements

The following table contains the additional optional 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
FTA: TOE Access	FTA_SSL.3: TSF-initiated Termination	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

Requirement Class	Requirement Component	Verified By
	FTA_TSE.1: TOE Session Establishment	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017
	FTA_VCM_EXT.1: VPN Client Management	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 C, 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
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, Security Target Version 1.0, March 27, 2017

Table 7: Selection-Based Requirements

Note that the EP provides guidance to ST authors for how to claim certain requirements from the base PP in order to be consistent with the requirements defined in the EP. These SFRs are considered to be part of the base PP and were determined to be appropriately applied in the CCTL's evaluation of the ST. Therefore, they were not assessed separately as part of this VR.

6 Assurance Requirements

The following are the assurance requirements contained in the VPNGWEP20:

Requirement Class	Requirement Component	Verified By
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: Assurance Requirements

Note that this is not a new SAR; instead, this provides additional guidance for an SAR in the base PP for TOEs that claim conformance to this EP.

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.1	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 VPNGWEP20 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] Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, Version 2.0 December 1, 2015