National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, April 12th, 2013

Report Number: CCEVS-VR-PP-0007
Dated: 15 April 2015
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
Leidos, Inc.
Columbia, 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 Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1 (VPNGWEP11). It presents a summary of the VPNGWEP11 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the VPNGWEP11 was performed concurrent with the first product evaluation against the EP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Cisco Integrated Service Routers Generation 2 (ISR G2). The evaluation was performed by the Leidos Inc. Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in March 2014. This evaluation addressed the base and additional requirements of the VPNGWEP11. Since the VPNGWEP is an extended package of the Network Device Protection Profile (NDPP), this evaluation also included requirements from this PP, although this is outside the scope of this VR.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the Leidos CCTL. Similarly, for materials covered by the Fortress evaluation that were out of scope of the Aruba Networks evaluation, the ETR produced by Leidos was referenced. Additional review of the PP to confirm that it meets the claimed APE assurance requirements was performed independently by the VR author as part of the completion of this VR.

The evaluation determined that the VPNGWEP11 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 material drawn directly from the VPNGWEP11, 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. Note that the ST also contains materials from the base NDPP that the VPNGWEP11 is an extension of. Items in the ST that were taken from the base NDPP and do not relate to the VPNGWEP11 were not examined for this VR.

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 VPNGWEP11 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the evaluation technical 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 Profile 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 VPNGWEP11 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Cisco Integrated Service Routers Generation 2, provided by Cisco Systems. The evaluation was performed by the Leidos Inc. Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in March 2014.

The VPNGWEP11 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are conditionally expected to be included if conformant TOEs provide that capability. The vendor may choose to include such requirements in the ST and still claim conformance to this EP. Since the VPNGWEP11 is an extended package of the NDPP, the ST and TOE must also claim conformance to the "base" NDPP, which includes any applicable optional requirements from that PP.

The EP's optional requirements may not be included in a particular ST; however, the initial evaluation that was performed (and subsequently used as a basis for this VR) included the optional requirements; therefore, the VR has been written with respect to both the base and additional requirements of the EP.

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 optional requirements in the VPNGWEP11.

Protection Profile	*Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, April 12, 2013.*
ST (Base)	Cisco Integrated Service Routers Generation 2 (ISR G2) Security Target, Version 1.1, March 2014
Evaluation Technical Report (Base)	Evaluation Technical Report For Cisco Integrated Service Routers Generation 2, Version 5.0, February 19, 2014
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)	Leidos (formerly SAIC) Inc., Columbia, MD USA
CCEVS Validators (base)	Daniel Faigin and Jerome Myers, The Aerospace Corporation

3 VPNGWEP Description

The VPNGWEP11 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 NDPP, conformant TOEs are obligated to implement the functionality required in the NDPP 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. However, a compliant TOE may also contain the ability to act as a headend for remote clients. Because this capability is optional, the remote client based requirements have been included within Appendix D of the EP.

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: TOE Assumptions

Assumption Name	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 enforced on all applicable network traffic flowing among the attached networks.

4.2 Threats

The following table describes the threats that are defined for this EP in the event that only the "base" requirements are applicable.

Table 2: Threats

Threat Name	Threat Definition
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T.NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.TSF_FAILURE	Security mechanisms of the TOE mail fail, leading to a compromise of the TSF.
T.REPLAY_ATTACK	If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.
T.DATA_INTEGRITY	A malicious party attempts to change the data being sent – resulting in loss of integrity.

The following table describes additional threats that are defined for the EP when the headend configuration is anticipated to be the operational environment for a TOE claiming conformance to the EP.

Table 3: Threats

Threat Name	Threat Definition
T.UNAUTHORIZED_CONNECTION	While a VPN client may have the necessary credentials (e.g., certificate, pre-shared key) to connect to a VPN gateway, there may be instances where the remote client, or the machine the client is operating on, has been compromised and attempts to make unauthorized connections,
T.HIJACKED_SESSION	There may be an instance where a remote client's session is hijacked due to session activity. This could be accomplished because a user has walked away from the machine that was used to establish the session.
T.UNPROTECTED_TRAFFIC	A remote machine's network traffic may be exposed to a hostile network. A user may be required to use a hostile (or unknown) network to send network traffic without being able to route the traffic appropriately.

4.3 Organizational Security Policies

There are no organizational security policies defined by the EP.

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
O.ADDRESS_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination addresses.
O.AUTHENTICATION	The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE will provide means to encrypt and decrypt data as a means to maintain confidentiality and allow for detection and modification of TSF data that is transmitted outside of the TOE.
O.FAIL_SECURE	Upon a self-test failure, the TOE will shutdown to ensure data cannot be passed while not adhering to the security policies configured by the administrator.
O.PORT_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination transport layer ports.

The following table describes additional threats that are defined for the EP when the headend configuration is anticipated to be the operational environment for a TOE claiming conformance to the EP.

Table 5: Threats

Threat Name	Threat Definition

Threat Name	Threat Definition
O.CLIENT_ESTABLISHMENT_CONSTRAINTS	To address the concern that a remote client may be compromised and attempt to establish connections with the headend VPN gateway outside of "normal" operations, this objective specifies conditions under which a remote client may establish connections. The administrator may configure the headend VPN gateway to accept a 7 client's request for a connection based on attributes the administrator feels are appropriate.
O.REMOTE_SESSION_TERMINATION	A remote client's session can become vulnerability when there is a lack of activity. This is primarily due to a user walking away from a device that has a remote connection established. While some devices have a "lock screen" or logout capability, they cannot always assumed to be configured or available. To address this concern, a session termination capability is necessary during an administrator specified time period.
O.ASSIGNED_PRIVATE_ADDRESS	There are instances where a remote client desires secure communication with a gateway that is trusted. While a user may be connected via an untrusted network, it should still be possible to ensure that it can communicate with a known entity that controls the routing of the client's network packets. This can be accomplished by the VPN headend assigning an IP address that the gateway controls, as well as providing a routing point for the client's network traffic.

The following table contains objectives for the Operational Environment.

Table 6: Security Objectives for the Operational Environment

Environmental Security Obj.	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.

5 Requirements

As indicated above, requirements in the VPNGWEP11 are comprised of the "base" requirements and additional requirements that are conditionally optional. The following are table contains the "base" requirements that were validated as part of the Cisco evaluation activity referenced above. Within the table, SFRs that are formatted in **bold** refer to SFRs that were defined in the NDPP but were augmented or modified for the VPNGWEP. SFRs with no formatting refer to SFRs that did not exist at all in the NDPP or were significantly redefined.

Requirement Class	Requirement Component
FAU: Security Audit	**FAU_GEN.1: Audit Data Generation**
FCS: Cryptographic Support	**FCS_CKM.1(1): Cryptographic Key Generation (for asymmetric keys)**
	FCS_CKM.1(2): Cryptographic Key Generation (for asymmetric keys)
	FCS_COP.1(1): Cryptographic Operation (for data

Requirement Class	Requirement Component
	encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_IPSEC_EXT.1: Internet Protocol Security (IPsec) Communications
	FCS_RBG_EXT.1: Cryptographic Operation: Random Bit Generation
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling
	FIA_X509_EXT.1: X509 Certificates
FMT: Security Management	FMT_MOF.1: Management of Functions Behavior
	FMT_SMF.1: Specification of Management Functions
FPF: Packet Filtering	FPF_RUL_EXT.1: Packet Filtering
FPT: Protection of the TSF	FPT_FLS.1: Fail Secure
	FPF_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Trusted Update
FTP: Trusted Path/Channels	**FTP_ITC.1: Inter-TSF Trusted Channel**

The following table contains the optional requirements contained in Appendices C and D, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). As stated previously, all optional requirements were assessed as part of the initial evaluation that was conducted alongside the review of this EP.

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	Cisco Integrated Services Routers Generation 2, March 2014
FTA: TOE Access	FTA_SSL.3: TSF-initiated Termination	Cisco Integrated Services Routers Generation 2, March 2014
	FTA_TSE.1: TOE Session Establishment	Cisco Integrated Services Routers Generation 2, March 2014
	FTA_VCM_EXT.1: VPN Client Management	Cisco Integrated Services Routers Generation 2, March 2014

6 Assurance Requirements

The following are the assurance requirements contained in the VPNGWEP11. Note that since the VPNGWEP11 is an extension of the NDPP, the evaluation laboratory also performed the assurance activities for the NDPP in the course of this evaluation. Additionally, the AVA_VAN.1 prescribed by the VPNGWEP11 is intended to supplement what is required by the NDPP and not replace it.

Requirement Class	Requirement Component
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

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
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Pass

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 VPNGWEP 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 Organisations. *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 Organisations. *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 Organisations. *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 Organisations. *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] Leidos, Inc. *Evaluation Technical Report For Cisco Integrated Service Routers Generation 2*, Version 5.0, February 19, 2014.

[7] Cisco Systems, Inc. *Cisco Integrated Services Routers Generation 2 (ISR G2) Security Target*, Version 1.1. March 2014.

[8] Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, April 12, 2013.