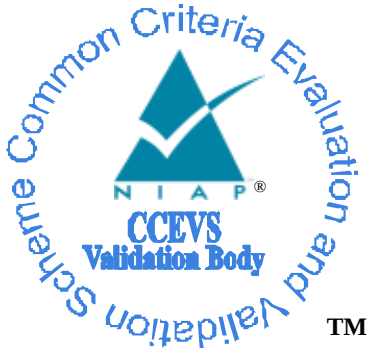
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

Extended Package for VPN Gateway, Version 2.1, March 8, 2017

Report Number: CCEVS-VR-PP-0040
Dated: October 3, 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

Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

Table of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Security Requirements for VPN Gateway (Version 2.1) Extended Package (EPVPNGW21). It presents a summary of the EPVPNGW21 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the EPVPNGW21 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 Firepower 4100 and 9300 Security Appliances. The evaluation was performed by the Gossamer Security Solutions, Inc. Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in September 2017.

Additional review of the EP 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 EPVPNGW21 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 material drawn directly from the EPVPNGW21, performance of the majority of the ASE work units serves to satisfy the APE work units as well.

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 EPVPNGW21 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 Profile 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 EPVPNGW21 was performed concurrent with the first product evaluation against the EP. In this case the TOE for this first product was Cisco System's Firepower 4100 and 9300 Security Appliances. The evaluation was performed by Gossamer Security Solutions, Inc. Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in September 2017.

The EPVPNGW21 contains a set of "base" requirements that all conformant STs must include, and in addition, contains "Optional" and "Selection-Based" requirements. Optional requirements are those that that specify security functionality that is desirable but is not explicitly required by the EP. The vendor may choose to include such requirements in the ST and still claim conformance to this EP.

Selection-Based requirements are those that must be claimed only in certain situations, depending on the selections made in the base requirements. Selection-Based requirements are those that must be claimed only in certain situations, depending on the selections made in the base requirements.

Because these discretionary 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 as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the EPVPNGW21 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

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 optional requirements in the EPVPNGW21.

Protection Profile	*Extended Package for VPN Gateway, Version 2.1, 8 March 2017*
ST (Base)	*Security Target for Cisco Firepower 4100 and 9300 Security Appliances Security Target, Version 1.0, September 11, 2017*
Assurance Activity Report (Base)	*Assurance Activity Report (FWCPP10/VPNGWCEP21) for Cisco Firepower 4100 and 9300 Security Appliances, Version 0.5, September 11, 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	Gossamer Security Solutions, Catonsville, MD
CCEVS Validators	Jean Petty, MITRE Corporation
	Chris Thorpe, MITRE Corporation

3 EPVPNGW21 Description

The EPVPNGW21 describes security requirements for VPN Gateways. Products evaluated against this EP are defined as devices at the edge of a private network that terminates an IPsec tunnel, which provides device authentication, confidentiality, and integrity of information traversing a public or untrusted network. The EP is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats to VPN Gateway technology. However, this EP is not complete in itself, but rather extends the collaborative Protection Profiles for Stateful Traffic Filter Firewalls (FWcPP) and Network Devices (NDcPP). This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the FWcPP and NDcPP.

4 Security Problem Description and Objectives

4.1 Assumptions

The following assumptions that are defined in this EP extend the threats that are defined by the claimed base PP(s).

Table 1: 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 threats that are defined in this EP extend the threats that are defined by the claimed base PP(s).

Table 2: Threats

Threat Name	Threat Definition
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.HIJACKED_SESSION (only applicable when the TOE is functioning as a VPN headend device and the optional SFRs in Appendix A.1 are claimed)	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.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. From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network. From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled

Threat Name	Threat Definition
	e-mail servers, or, that access to the mail server must be done over an encrypted link.
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. From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.
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. From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected

Threat Name	Threat Definition
	network thereby further limiting the potential disclosure of information. From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses and/or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.
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. • No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these modifications.
T.UNAUTHORIZED_CONNECTION (only applicable when the TOE is functioning as a VPN headend device and the optional SFRs in Appendix A.1 are claimed)	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.UNPROTECTED_TRAFFIC (only applicable when the TOE is functioning as a VPN headend device and the optional SFRs in Appendix A.1 are claimed)	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

No organizational policies have been identified that are specific to this EP.

4.4 Security Objectives

There are currently no security objectives for the operational environment defined in this EP. The table below contains objectives for the TOE.

Table 3: Security Objectives for the TOE

Environmental Security Obj.	Environmental Security Objective Definition
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.ASSIGNED_PRIVATE_ADDRESS (only applicable when optional SFR FTA_VCM_EXT.1 is claimed)	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.
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.CLIENT_ESTABLISHMENT_CONSTRAINTS (only applicable when optional SFR FTA_TSE.1 is claimed)	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 client's request for a connection based on attributes the administrator feels are appropriate.
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.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

Environmental Security Obj.	Environmental Security Objective Definition
	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.
O.REMOTE_SESSION_TERMINATION (only applicable when optional SFR FTA_SSL.3 is claimed)	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.SYSTEM_MONITORING	To address the issues of administrators being able to monitor the operations of the VPN gateway, it is necessary to provide a capability to monitor system activity. Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure packet filtering rules to 'log' when network traffic is found to match the configured rule. As a result, matching a rule configured to 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security associations (SAs) is auditable, not only between peer VPN gateways, but also with certification authorities (CAs).
O.TOE_ADMINISTRATION	Compliant TOEs will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE.

5 Requirements

As indicated above, requirements in the EPVPNGW21 are comprised of the "base" requirements, in addition to "selection-based" and "optional requirements." The following table contains the "base" requirements that were validated as part of the evaluation. SFRs listed in **bold** are those where the EP requires a modification of an SFR already defined in the base PP, rather than defining an entirely new SFR.

Table 4: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	**FCS_COP.1(1): Data Encryption/Decryption**	Cisco Firepower 4100 and 9300 Security Appliances Security Target

Requirement Class	Requirement Component	Verified By
	FCS_IPSEC_EXT.1: IPSec	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	FCS_CKM.1/IKE: Cryptographic Key Generation (IKE Peer Authentication)	Cisco Firepower 4100 and 9300 Security Appliances Security Target
FIA: Identification and Authorization	FIA_AFL.1.: Authentication Failure Handling	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	FIA_X509_EXT.4: Certificate Identity	Cisco Firepower 4100 and 9300 Security Appliances Security Target
FMT: Security Management	FMT_MTD.1/AdminAct: Management of TSF Data	Cisco Firepower 4100 and 9300 Security Appliances Security Target
FPF: Packet Filtering	FPF_RUL_EXT.1: Rules for Packet Filtering	Cisco Firepower 4100 and 9300 Security Appliances Security Target
FPT: Protection of the TSF	FPT_FLS.1/SelfTest: Self-Test Failures	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	FPT_TST_EXT.2: TSF Testing	Cisco Firepower 4100 and 9300 Security Appliances Security Target
FTP: Trusted Paths/Channels	**FTP_ITC_EXT.1: Inter-TSF Trusted Channel**	Cisco Firepower 4100 and 9300 Security Appliances Security Target

The table below lists the "**Optional**" requirements.

Table 5: Optional Requirements

Requirement Class	Requirement Component	Verified By
FTA: TOE Access	FTA_SSL.3/VPN: TSF-Initiated Termination	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	FTA_TSE.1: TOE Session Establishment	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	FTA_VCM_EXT.1: VPN Client Management	Cisco Firepower 4100 and 9300 Security Appliances Security Target

The table below lists the "**Selection-Based**" requirements.

Table 6: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authorization	FIA_PSK_EXT.1: Pre-Shared Key Composition	Cisco Firepower 4100 and 9300 Security Appliances Security Target

6 Assurance Requirements

The VPNGWEP21 does not define any new assurance requirements beyond those defined in the base PPs that it extends. It does modify the assurance activities used to evaluate AVA_VAN.1 but does not define any additional SARs. Listed below are the SARs that are tested for ST/TOEs that include this EP in their conformance claims:

Table 7: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	ASE_ECD.1: Extended Components Definition	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	ASE_INT.1: ST Introduction	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	ASE_OBJ.1: Security Objectives for the Operational Environment	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	ASE_REQ.1: Stated Security Requirements	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	ASE_SPD.1: Security Problem Definition	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	ASE_TSS.1: TOE Summary Specification	Cisco Firepower 4100 and 9300 Security Appliances Security Target
ADV: Development	ADV_FSP.1 Basic Functional Specification	Cisco Firepower 4100 and 9300 Security Appliances Security Target
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	AGD_PRE.1: Preparative Procedures	Cisco Firepower 4100 and 9300 Security Appliances Security Target
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE	Cisco Firepower 4100 and 9300 Security Appliances Security Target
	ALC_CMS.1: TOE CM Coverage	Cisco Firepower 4100 and 9300 Security Appliances Security Target
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Cisco Firepower 4100 and 9300 Security Appliances Security Target
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Cisco Firepower 4100 and 9300 Security Appliances Security Target

7 Results of the Evaluation

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.

Table 8: Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Cisco Firepower 4100 and 9300 Security Appliances Security Target
APE_ECD.1	Pass	Cisco Firepower 4100 and 9300 Security Appliances Security Target
APE_INT.1	Pass	Cisco Firepower 4100 and 9300 Security Appliances Security Target
APE_OBJ.1	Pass	Cisco Firepower 4100 and 9300 Security Appliances Security Target
APE_REQ.1	Pass	Cisco Firepower 4100 and 9300 Security Appliances Security Target

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 EPVPNGW21 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 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* – Part 2: Evaluation Methodology, Version 3.1, Revision 4, dated: September 2012.

[5] Gossamer Security Solutions, Inc., *Assurance Activity Report (FWcPP10/VPNGWcEP21) for Cisco Firepower 4100 and 9300 Security Appliances*, Version 0.5, 11 September 2017.

[6] Gossamer Security Solutions, Inc., *Security Target for Systems Cisco Firepower 4100 and 9300 Security Appliances*, Version 1.0, 11 September 2017.

[7] *Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package*, Version 2.1, 8 March 2017

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

[9] *collaborative Protection Profile for Network Devices*, Version 1.0, 27 February 2015