National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways

Version 1.0

22 November 2019

Report Number: CCEVS-VR-PP-0060
Dated: 02 October 2020
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 Requirements
Gossamer Security Solutions
Catonsville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, Version 1.0 (CFG_NDcPP-VPNGW_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the collaborative Protection Profile for Network Devices (CPP_ND_V2.1) Base-PP and the PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0 (MOD_VPNGW_V1.0). It presents a summary of the CFG_NDcPP-VPNGW_V1.0 and the evaluation results.

Gossamer Security Solutions, located in Catonsville, Maryland, performed the evaluation of the CFG_NDcPP-VPNGW_V1.0 and MOD_VPNGW_V1.0 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa.

This evaluation addressed the base security functional requirements of MOD_VPNGW_V1.0 as part of CFG_NDcPP-VPNGW_V1.0. The Module defines additional requirements, some of which the NetIron evaluation claimed.

The Validation Report (VR) author independently performed an additional review of the PP-Configuration and Module as part of the completion of this VR, to confirm they meet the claimed ACE requirements.

The evaluation determined the CFG_NDcPP-VPNGW_V1.0 is both Common Criteria Part 2 Extended and Part 3 Conformant. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the PP-Configuration and Module identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from both CPP_ND_V2.1 and MOD_VPNGW_V1.0; completion of the ASE work units satisfied the ACE work units for this Module, but only for the materials defined in this Module, and only when the Module is in the defined PP-Configuration.

The initial results by the validation team found that the evaluation showed that the MOD_VPNGW_V1.0 did not meet the requirements of the ACE components. These findings were confirmed by the VR author and NIAP. While the Assumption and the Organization Security Policy was mentioned in Section 3.2 and 3.2, they were not explicitly stated in Section 6.1.2 of the Consistency of Security Problem Definition. As a result, MOD_VPNGW_V1.0 was updated through the issuance of a NIAP Technical Decision (TD). The validation team found that MOD_VPNGW_V1.0 meets the requirements of the ACE components. NIAP determined the impact of the changes were limited to the consistency rationale in the PP-Module and did not alter the outcome of the evaluation.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 workunits specific to the technology described by the PP or Module. Products may only be evaluated against Modules when a PP-Configuration is defined to include the Module with at least one corresponding Base-PP.

In order to promote thoroughness and efficiency, the evaluation of the CFG_NDCPP-VPNGW_V1.0 and MOD_VPNGW_V1.0 was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa, performed by Gossamer Security Solutions in Catonsville, Maryland, United States.

This evaluation addressed the base security functional requirements of MOD_VPNGW_V1.0 as part of CFG_NDCPP-VPNGW_V1.0. The Module defines additional requirements, some of which the NetIron evaluation claimed.

MOD_VPNGW_V1.0 contains a set of base requirements that all conformant STs must include, and additionally contains optional and selection-based requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ work units performed against the Module. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the CFG_NDCPP-VPNGW_V1.0 were evaluated.

The following identifies the Module in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this Module.

PP-Configuration	PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, Version 1.0, 22 November 2019
Module(s) in PP-Configuration	PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 17 September 2019
ST (Base)	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa Security Target, Version 0.4, 27 May 2020
Assurance Activity Report (Base)	Assurance Activity Report (NDcPP21/VPNGW10) for Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa, Version 0.2, 27 May 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	Gossamer Security Solutions Catonsville, Maryland 21228

3 CFG_NDCPP-VPNGW_V1.0 Description

CFG_NDCPP-VPNGW_V1.0 is a PP-Configuration that combines the following:

- collaborative Protection Profile for Network Devices, Version 2.1 (CPP_ND_V2.1)
- Protection Profile Module for Virtual Private Network (VPN) Gateways, Version 1.0 (MOD_VPNGW_V1.0)

The PP-Configuration defines a baseline set of security functional requirements (SFRs) for VPN Gateway applications (defined in CPP_ND_V2.1) that are bundled with agent applications to enforce configured policies on VPN Gateways (defined in MOD_VPNGW_V1.0).

A VPN Gateway is a device composed of hardware and software that is connected to two or more distinct networks and has an infrastructure role in the overall enterprise network. 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.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_NDCPP-VPNGW_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From CPP_ND_V2.1	
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of network devices (e.g., firewall).
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to

Assumption Name	Assumption Definition
	ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
From MOD_VPNGW_V1.0	
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

Table 2 shows the threats defined in the individual components of CFG_NDCPP-VPNGW_V1.0.

Table 2: Threats

Threat Name	Threat Definition
From CPP_ND_V2.1	
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device 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_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device 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 network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and

Threat Name	Threat Definition
	the Administrator would have no knowledge that the device has been compromised.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices 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 network device itself.
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.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
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.
From MOD_VPNGW_V1.0	
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 communicate with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
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.

Threat Name	Threat Definition
	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 e-mail servers, or, that access to the mail server must be done over an encrypted link.
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 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.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

Threat Name	Threat Definition
	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.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.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_NDCPP-VPNGW_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From CPP_ND_V2.1	
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.
From MOD_VPNGW_V1.0	
No OSPs defined in MOD_VPNGW_V1.0.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_NDCPP-VPNGW_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From CPP_ND_V2.1	
No security objectives defined in CPP_ND_V2.1.	
From MOD_VPNGW_V1.0	
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)

TOE Security Objective	TOE Security Objective Definition
	applicable network traffic as well as on established connection information.
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 and ensure that any such connection attempt is both authenticated and authorized. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.
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 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.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	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.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_NDCPP-VPNGW_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From CPP_ND_V2.1	

OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.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.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
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.
From MOD_VPNGW_V1.0	
OE.CONNECTIONS	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.

5 Functional Requirements

As indicated above, CFG_NDCPP-VPNGW_V1.0 includes both CPP_ND_V2.1 and MOD_VPNGW_V1.0. The functional requirements from CPP_ND_V2.1 were evaluated separately so this section applies only to requirements of MOD_VPNGW_V1.0.

As indicated above, requirements in the MOD_VPNGW_V1.0 are comprised of the "base" requirements and additional requirements that are objective. The following table contains the "base" requirements that were validated as part of the Gossamer Security Solutions evaluation activities referenced above.

Table 6: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM.1/IKE: Cryptographic Key Generation (for IKE Peer Authentication)	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa
FPF: Packet Filtering	FPF_RUL_EXT.1: Rules for Packet Filtering	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa
FPT: Protection of the TSF	FPT_FLS.1/SelfTest: Fail Secure (Self-Test Failures)	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa
	FPT_TST_EXT.3: TSF Self-Test with Defined Methods	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa
FTP: Trusted Path/Channels	FTP_ITC.1/VPN: Inter-TSF Trusted Channel (VPN Communications)	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa

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

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FTA: TOE Access	FTA_SSL.3/VPN; TSF-Initiated Termination (VPN Headend)	Module Evaluation
	FTA_TSE.1: TOE Session Establishment	Module Evaluation
	FTA_VCM_EXT.1: VPN Client Management	Module Evaluation

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

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa

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

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
The MOD_VPNGW_V1.0 does not define any additional objective requirements.		

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by CPP_ND_V2.1. The SARs defined in that PP are applicable to MOD_VPNGW_V1.0 as well as CFG_NDCPP-VPNGW_V1.0 as a whole.

7 Results of the Evaluation

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

Table 10: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module evaluation
ACE_CCL.1	Pass	Module evaluation
ACE_SPD.1	Pass	Module evaluation
ACE_OBJ.1	Pass	Module evaluation
ACE_ECD.1	Pass	Module evaluation
ACE_REQ.1	Pass	Module evaluation
ACE_MCO.1	Pass	Module evaluation
ACE_CCO.1	Pass	Module evaluation

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_VPNGW_V1.0 Evaluation Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process the CCEVS Validation Body uses that leads to the issuance of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

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

[6] PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 17 September 2019.

[7] collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018.

[8] PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, Version 1.0, 22 November 2019.

[9] Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa Security Target, Version 0.4, 27 May 2020

[10] Assurance Activity Report (NDcPP21/VPNGW10) for Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa, Version 0.2, 27 May 2020