National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Viasat Secure VPN v1.1.7

Report Number: CCEVS-VR-VID11405-2023
Dated: December 21, 2023
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
ATTN:NIAP, SUITE:6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

<u>Validation Panel</u>

Daniel Fagin

Meredith Martinez

Seada Mohammed

Mike Quintos

The Aerospace Corporation

<u>Common Criteria Testing Laboratory</u>

Oleg Andrianov, Dylan Lyman, Brad Mitchell

UL Verification Services Inc.

Table of Contents

1 Executive Summary 5

2 Identification 5

3 Security Policy 6

3.1 Audit 6

3.2 Cryptographic Operations 6

3.3 Identification and Authentication 7

3.4 Security Management 8

3.5 Protection of the TSF 8

3.6 Packet Filtering 8

3.7 TOE Access 9

3.8 Trusted Path/Channels 9

4 Assumptions and Clarification of Scope 9

4.1 Clarification of Scope 9

5 Architectural Information 9

6 Documentation 10

7 IT Product Testing 11

7.1 Developer Testing 11

7.2 Evaluation Team Independent Testing 11

8 Evaluated Configuration 11

9 Results of the Evaluation 12

9.1 Security Target Evaluation (ASE) 12

9.2 TOE Development (ADV) 12

9.3 Guidance Documents (AGD) 12

9.4 TOE Life Cycle Support (ALC) 13

9.5 TOE Tests (ATE) 13

9.6 Vulnerability Assessment (AVA) 13

9.7 Summary of Evaluation Results 14

10 Validator Comments/Recommendations 14

11 Security Target 15

12 Terms 15

12.1 Acronyms 15

13 Bibliography 15

1 Executive Summary

This report provides an overview of the security information relevant to the Common Criteria evaluation and provides practical information about the Target of Evaluation (TOE). It is intended to assist the end-user of this product in determining the suitability of the product for their use. Potential end-users should review the Security Target (ST) for the functional requirements as well as the assumptions and threats mitigated. The Assurance Activity Report (AAR) should be consulted for detailed information about the activities performed by the Common Criteria Testing Laboratory (CCTL) which provide assurance of the TOE meeting the specified requirements.

The evaluation was performed by UL Verification Services Inc., a Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, CA, USA and assigned Validation ID (VID) 11405 by the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). Further information can be found on their web site (www.niap-ccevs.org).

2 Identification

The TOE is the Viasat Secure VPN v1.1.7.

Viasat's Secure VPN is a VPN Gateway Virtual Network Device that provides a bump-in-the-wire IPsec encryption to virtual or physical systems. The device supports Gateway (GW) to GW IPsec encryption. The sources and destinations that send data over the IPsec tunnel provided by the device and its remote peer are not aware of their existence. The TOE is a Virtualized Network Device executing on Windows Hyper-V virtual machine manager running on the Windows 10 Pro 22H2 Operating System.

Table 1 provides information needed to completely identify the product and security evaluation.

Evaluation Scheme	United States NIAP Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Viasat Secure VPN v1.1.7
Protection Profile	• Collaborative Protection Profile for Network Devices (NDcPP) v2.2e • PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.2
PP Configuration	PP-configuration for Network devices and VPN Gateways, version 1.2
Security Target	Viasat Secure VPN v1.1.7 Security Target, Version 2.6, 1438289, December 13, 2023
Dates of Evaluation	March 2022 – December 2023
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Common Criteria Version	Common Criteria v3.1 Revision 5
Common Evaluation Methodology (CEM) Version	CEM v3.1 Revision 5
Evaluation Technical Report (ETR)	Common criteria Evaluation Technical Report for VID11405, UL1341589-ETR Rev1.2, December 19, 2023

Sponsor/Developer	Viasat, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Oleg Andrianov, Brad Mitchell, Dylan Lyman
CCEVS Validators	Daniel Fagin, Meredith Martinez, Seada Mohammed, Mike Quintos

Table 1: Product Identification

The secure use of the TOE was evaluated in conjunction with the environmental assumptions contained in Section 0. Additionally, the following components must be present in the Operational Environment to support the operation of the TOE.

Component	Description
Hypervisor	Microsoft (MS) Hyper-V Type 1 hypervisor Virtual Machine Manager (VMM) on Windows 10 Pro 22H2 Operating System

Table 2: Operational Environment Components

3 Security Policy

This section contains the product security features and services and contains the policies or rules that the TOE must comply with and/or enforce.

3.1 Audit

- The TOE will audit all events and information defined in Table 3: Auditable Events in the Security Target.
- The TOE will also include the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event.
- The TOE protects storage of audit information from unauthorized deletion.
- The TOE prevents unauthorized modifications to the stored audit records.
- The TOE can transmit audit data to/receive data from an external IT entity using the TLS protocol.
- The TOE performs audit log rotation when the local storage of audit records is full.
- The TOE counts the number of audit records that are overwritten when the local storage space for audit records is full.

3.2 Cryptographic Operations

The TSF performs the following cryptographic operations:

- For TLS as a client and server, supporting the following cryptographic algorithms:
- Supports the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite consisting of the following cryptographic services:
    - ECDSA digital signature generation/verification

- AES-256 in GCM mode for bulk data ciphering
- ECDHE key exchange utilizing the secp384r1 elliptic curve.
- SHA-384 hashing primitive
- HMAC-SHA2-384 for keyed hashing
- The TLS client TSF supports mutual authentication utilizing x.509v3 PKI.
- For IPsec, the TSF supports the following:
- ECDSA digital signature generation/verification for IKEv2 supporting NIST P-256 and P-384 curves.
- AES-GCM-256 algorithm for encryption and message authentication for the IPsec ESP protocol
- AES-GCM-256 or AES-CBC-256 to protect the IKEv2 payload.
- HMAC-SHA-384 to authenticate the IKEv2 payload.
- Diffie-Hellman groups 19 and 20 for use in IKEv2
- IPv4 only; IPv6 is not supported for IPsec.

The TSF utilizes a CTR_DRBG using AES-256, as its source for secure random bit generation.

The Trusted Update TSF utilizes ECDSA digital signatures associated with x.509v3 certificates using P-384 curve.

The TSF zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

3.3 Identification and Authentication

- The TSF supports passwords consisting of alphanumeric and special characters.
- The TSF also allows the Security Administrator (SA) to set a minimum password length.
- The TSF will lock out offending accounts that fail to successfully authenticate after an administratively defined number failed authentication attempts that the remote management interface. The offending account will be unlocked after an administratively configurable amount of time elapses.
- The TSF provides a local console management interface that is accessible via username and password authentication.
- The TSF does not echo back characters input for the password at the local console.
- The TSF utilizes x.509v3 certificates to identify itself to remote management users via the trusted path (HTTPS Server).
- The TSF utilizes x.509v3 certificate-based authentication to support a mutually authenticated trusted channel to a remote audit logging server (TLS client with mutual authentication).
- The TSF utilizes x.509v3 certificates for authentication of system software updates.
- The TSF supports the generation of Certificate Signing Requests.

- The TSF requires all administrative users to authenticate before allowing the user to perform any actions other than:
    - Viewing the warning banner
    - Automated generation of cryptographic keys
    - ICMP echo reply (when configured in packet filtering table by the SA)
    - Responding to ARP requests with ARP replies
    - Packet forwarding through the IPsec tunnel (when configured by the SA)
    - Packet forwarding through BYPASS packet filtering table (when configured by the SA)

3.4 Security Management

The TSF stores and protects the following data:

- Local audit records, user account data, and local authentication data (such as administrator passwords).
- Cryptographic keys including symmetric keys, and private keys.

There is one class of user on the TOE:

- Security Admin user

Management of the TSF:

- The administrator can perform manual updates, modify the behavior of the TSF, enable or disable services offered by the TOE, manage TSF data, modify, delete, generate, or import cryptographic keys, configure the access banner, manage packet filtering, and configure the session inactivity timeout period.
- The administrator may perform these functions locally or remotely via the CLI or RMI.

3.5 Protection of the TSF

- The TSF prevents the reading of secret and private keys.
- The TOE provides reliable time stamps for itself.
- The TOE runs a suite of self-tests during the initial start-up (upon power on) to demonstrate the correct operation of the TSF.
- The TOE provides a means to verify firmware/software updates to the TOE using a digital signature mechanism prior to installing those updates.

3.6 Packet Filtering

- The TSF can be configured to filter network packets based on IPv4, IPv6, TCP and UDP protocols.
    - The TOE can only DROP and LOG IPv6 packets.
- The TSF can be configured to log network packets that match a packet filter rule.
- The TSF processes packet filter rules in an administratively defined order.
- Packet filtering can be applied to any network interface of the TOE.
- The TSF has a final ‘drop’ rule if no rule matches the packet being processed.

3.7 TOE Access

- The TOE, for local interactive sessions, terminates active session after an Authorized Administrator-specified period of session inactivity.
- The TOE terminates a remote interactive session after an Authorized Administrator-configurable period of session inactivity.
- The TOE allows Administrator-initiated termination of the Administrator's own interactive session.
- Before establishing an administrative user session, the TOE is capable of displaying an Authorized Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

3.8 Trusted Path/Channels

- The TOE uses IPsec, and TLS to provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
- The TOE permits the TSF, or the authorized IT entities to initiate communication via the trusted channel.
- The TOE permits remote administrators to initiate communication via the trusted path.
- The TOE requires the use of the trusted path for initial administrator authentication and all remote administration actions.

4 Assumptions and Clarification of Scope

The assumptions, threats and organizational security policies can be found in the NDcPP v2.2e Section 4 and VPNGW PP-Module Section 3.

4.1 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the ST and the associated PP-Configuration.

Any additional functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the device needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. It is likely that any assumptions not upheld by the TOE environment will create new unmitigated threats. This evaluation provides no assurance that the TOE counters any threats which are not identified above.

5 Architectural Information

This section is not applicable as the evaluation did not include ADV_TDS.

The TOE is a Virtualized Network Device executing on Windows Hyper-V virtual machine manager running on the Windows 10 Pro 22H2 Operating System. The TOE is a VPN Gateway, providing an external (black network) interface facing the WAN.

Figure 1 below is a block diagram of the major security functionality and interfaces of the TOE. This figure depicts the following information:

- The TOE is demarked by the red dashed line.
- Logical and physical interfaces are identified.
- Components of the OE are identified.
- Local ("CLI") and Remote Management Interface ("RMI").
- RMI is the Trusted Path TLS/HTTPS protected interface.
- Remote syslog server.
- Remote IPsec Gateway Peer.
- Data flows from Red Network to/from Black Network.

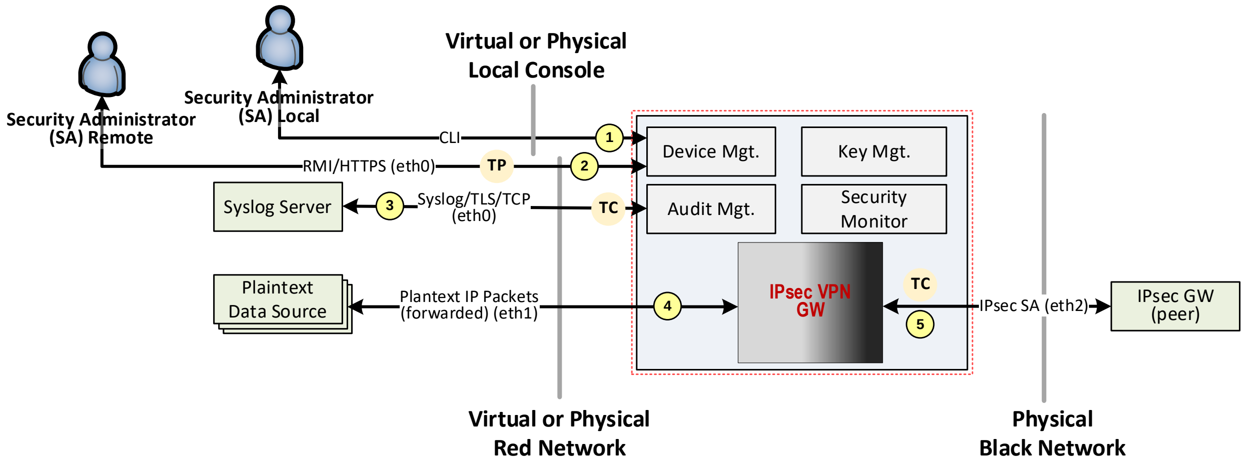

Figure 1 TSF Block Diagram

6 Documentation

The following documents are provided with the product by the developer to the consumer and were evaluated along with the TOE:

- Viasat Secure VPN User Guide, Rev. 008, December 15, 2023
- Viasat Secure VPN, version 1.1.7, REST API Reference, Rev. 005, 6 September 2023

Any additional documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated. To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the documentation from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

The evaluation team configured the TOE according to the vendor-provided guidance documentation and performed the tests specified in the Protection Profile and PP-Module. These results are summarized in the evaluation Assurance Activity Report with the approach summarized here.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities of this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.2.

The test environment used by the CCTL during the course of testing is briefly summarized below and conforms to the expected use-case of the TOE (Network Device, VPN Gateway).

The evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the ST for a product claiming conformance to PP. The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in PP. The Test Plan described how each test activity was to be performed. The evaluation team executed the tests specified in the Test Plan and documented the results in the Evaluation Technical Report. The evaluation team consisted of Oleg Andrianov, Dylan Lyman, and Brad Mitchell from the CCTL.

The test laboratory was configured by UL and physically located at the UL San Luis Obispo facility in an access-controlled environment. Testing was conducted between March 24, 2022 and September 22, 2023.

The ST defines only one TOE model, "Viasat Secure VPN v1.1.7". This is the model that was tested.

The TOE was tested on the platform that is describe in the ST:

- Hardware Platform
  - Dell XPS 8940 Server Hardware
    - Processor: 11th Gen Intel Core i5-1140 @ 2.6Ghz
    - RAM: 16Gb Memory
    - Hard drive: 1TB mechanical (spinning) SATA drive
- Software Platform
  - Windows 10 Pro 22H2
  - Microsoft (MS) Hyper-V Type 1 hypervisor Virtual Machine Manager (VMM)

The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here. The AAR, in section 1.1-1.6 consists of test layout for general testing, a list of tested devices and testing tools, and has diagrams of the test environment.

8 Evaluated Configuration

This evaluation covers the TOE only in its evaluated configuration. To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation identified above in Section 6. The evaluated configuration consists of the Hardware Platform and Software Platform listed in Security Target Section 1.3.4 and the TOE software as described in Security Target Section 1.4.1, in conjunction with the administrative configuration as described in the Guidance Documentation.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation was successful and provides a level of assurance that the TOE meets the Security Functional Requirements identified in the Security Target. This assurance comes from the performance of the work units associated with the Security Assurance Requirements. A detailed description of those Assurance Requirements as well as the details of how the product meets each of them can be found in the Security Target. A more detailed account of the evaluation assurance activities and the results obtained can be found in the Assurance Activity Report.

9.1 Security Target Evaluation (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] and PP-Module for VPN Gateways, Version 1.2.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 TOE Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] and PP-Module for VPN Gateways, Version 1.2.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] and PP-Module for VPN Gateways, Version 1.2.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 TOE Life Cycle Support (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 TOE Tests (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified in the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] and PP-Module for VPN Gateways, Version 1.2.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment (AVA)

The evaluation team applied each AVA CEM work unit as modified by the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] and PP-Module for VPN Gateways, Version 1.2.

The evaluators searched for publicly known vulnerabilities applicable to the TOE on the following dates:

- 08/01/2023
- 10/11/2023
- 10/23/2023
- 11/22/2023

The list of search terms was generated by https://www.cvedetails.com/vulnerability-search.php and cross referencing with https://web.nvd.nist.gov/view/vuln/search for software packages included in the TOE and CPU used by the TOE.

The search terms are:

ACL	libffi	Pyca/cryptography

acvp-parser	libgdbm	pydantic
aiofiles	liblzma-staticdev	PyJWT
argp-standalone	libmnl	Python programming language
Berkeley DB	liboping	python3-setuptools
Busybox	libpcap	python3-six
Bzip2	libpcre	python3-zipp
curl	libubox	python-cffi
django/asgiref	libxml2	python-h11
e2fsprogs	Linux Extended Attributes	python-multipart
elfutils	Linux Kernel	python-pam
Fastapi	Linux-Pam	pyuci
gettext	logrotate	Readline
gkernel: rng-tools / ethtool	lua	Starlette
GLib	more-itertools	strongSwan
GNU Core Utilities	musl	syslog-ng
grub2	ncurses	terminfo
importlib-metadata	OpenSSL	trace-cmd
iproute2	OpenWrt	typing-extensions
IPTables	OpenWrt jsonfilter	uClibc++
json-c	openwrt odhcp6c	util-linux
libcap	opkg	uvicorn
libdbi	Perl	XZ Utils
libestr	Ply	zlib
libfastjson	popt	CPU

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.2, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST. The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] and PP-Module for VPN Gateways, Version 1.2, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documents listed in Section 6. No versions of the TOE and software, either earlier or later, were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Security Target

Viasat Secure VPN v1.1.7 Security Target, version 2.6, December 13, 2023

12 Terms

12.1 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

[5] collaborative Protection Profile for Network Devices, March 23, 2020, Version 2.2e

[6] PP-Module for VPN Gateways, March 31, 2022, Version 1.2