National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

for the

ID Technologies GoSilent Cube + GoSilent Server v25.01

Report Number: CCEVS-VR-11310-2022

Dated: December 22, 2022

Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson

Randy Heimann

Lisa Mitchell

Linda Morrison

Lori Sarem

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

Furukh Siddique

Kevin Steiner

Lightship Security, USA

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of ID Technologies GoSilent Cube + GoSilent Server v25.01 solution provided by ID Technologies, A CACI Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in December 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (CFG_NDcPP-FW-VPNGW_V1.2) which includes the following components:

- collaborative Protection Profile for Network Devices, v2.2e, 23 March 2020 (CPP_ND_V2.2E)
- PP-Module for Stateful Traffic Filter Firewalls, v1.4e, 25 June 2020 (MOD_CPP_FW_v1.4e)
- PP-Module for VPN Gateways, v1.2, 31 March 2022 (MOD_VPNGW_V1.2)

The TOE is the ID Technologies GoSilent Cube + GoSilent Server v25.01. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. 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 ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *ID Technologies GoSilent Cube + GoSilent Server v25.01 Security Target*, Version 1.18, December 2022 and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	ID Technologies GoSilent Cube + GoSilent Server v25.01
Sponsor and Developer	ID Technologies, A CACI Company 19980 Highland Vista Drive, Suite 175 Ashburn, VA 20147
CCTL	Lightship Security USA 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

Item	Identifier
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.
Protection Profile	PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (CFG_NDcPP-FW-VPNGW_V1.2) which includes the following components: • collaborative Protection Profile for Network Devices, v2.2e, 23 March 2020 • PP-Module for Stateful Traffic Filter Firewalls, v1.4e, 25 June 2020 • PP-Module for VPN Gateways, v1.2, 31 March 2022
ST	ID Technologies GoSilent Cube + GoSilent Server v25.01 Security Target, Version 1.18, December 2022
Evaluation Technical Report	ID Technologies GoSilent Cube + GoSilent Server v25.01 Evaluation Technical Report, Version 0.7, December 2022
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Lightship USA: Furukh Siddique, Kevin Steiner
CCEVS Validators	MITRE: Jenn Dotson, Randy Heimann, Lisa Mitchell, Linda Morrison, Lori Sarem, Chris Thorpe

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is a distributed TOE which consists of the ID Technologies GoSilent Cube + GoSilent Server v25.01 operating together as a single solution to provide firewall and VPN capabilities for remote network devices to secure their communications. The GoSilent Cube is a hardware user device and the GoSilent Server is a virtualized appliance.

3.1. TOE Evaluated Configuration

The TOE evaluated configuration includes the ID Technologies GoSilent Cube + GoSilent Server running system software version: 25.01.4 (GoSilent Server) and 25.01.3 (GoSilent Cube).

Type	Model	CPU	Memory	Storage
GoSilent Server	Virtual Appliance	Intel Xeon E3-1270 v5 (Skylake) w/ ESXi 6.5	16 GB UDIMM	8 GB SD Card (hypervisor)
				1 TB SATA HDD
GoSilent Cube	GSC-100	AllWinner H5/ Cortex A-53 (ARM v8-A)	1 GB DRAM	8 GB eMMC
	GSC-120		512 MB DRAM	

3.2. Physical Boundary

The GoSilent Server is a virtualized appliance that runs on ESXi 6.5 with an Intel Xeon E3-1270 v5 (Skylake) CPU. The GoSilent Cube is available in two hardware models, the GSC-100 and GSC-120. These models both use the AllWinner H5/Cortex A-53 (ARM v8-A) CPU and only differ in the amount of memory (1 GB for GSC-100 and 512 MB for GSC-120).

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- Audit Server. The TOE makes use of a syslog server for remote logging.
- OCSP Server/CDP. The TOE communicates with an external OCSP Server and CDP for the purposes of certificate checking.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates logs for auditable events. These logs are stored locally in protected storage and are also forwarded via a TLS connection to an external audit server in real-time. When the maximum storage utilization has been reached, the oldest audit records are discarded so that the new records can be saved. Only authorized administrators may view audit records and no capability to modify the audit records is provided.

4.2. Communication

The TOE provides mechanisms for configuring, registering, and enabling components in order to establish secure communications with each other.

4.3. Cryptographic Support

The TOE implements key generation and other cryptographic services to protect TOE communications including data in transit and at rest. The TOE provides the following CAVP-certified cryptographic services: asymmetric cryptographic key pair generation; key establishment; symmetric data encryption and decryption; digital signature generation and verification; cryptographic hashing; keyed-hash message authentication; and random bit generation.

4.4. User Data Protection

The TOE provides mechanisms to protect user data and prevent its persistence by overwriting storage space with zeros when memory is deallocated.

4.5. Firewall & Packet Filtering

The TOE provides firewall functionality for all traffic passed through the TOE by enforcing stateful network traffic filtering based on examination of network packets and the application of information flow rules.

4.6. Identification and Authentication

The TOE implements mechanisms to identify and authenticate all administrators to ensure only authorized access to TOE functionality or TSF data is granted. Identification and authentication are required for both local and remote administrator access

Authentication of an administrator is through use of a username/password. The minimum password may be configured from 8 to 40 characters, that incorporate a combination of lowercase letters, uppercase letters, numbers, and special characters (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”). The TOE obscures feedback to the administrator when the password is entered. If an authentication attempt fails, (either the username is not recognized, or the password is incorrect) an error message is presented.

The TOE tracks the number of sequential failed authentication attempts for each user account. Upon meeting the configured limit for failed authentication attempts, the TOE locks the account in question for an administrator configured time period. During this time, entering the correct password for the locked account will still result in an authentication failure. Any successful authentication resets the counter to zero.

4.7. Security Management

The TOE provides a suite of management functionality for each TOE component, which is only configurable and accessible by authorized administrators. The TOE supports the role of Security Administrator and can be administered both locally and remotely. Management of the TOE is primarily performed through GoSilent Server. However, initial management of GoSilent Cube, providing enough configuration information for it to connect to GoSilent Server, is required.

4.8. Protection of the TSF

The TOE implements a variety of protection mechanisms including authentication, self-tests, and trusted update functions to ensure the integrity of the TOE and that its TSF data is protected from unauthorized access.

The TOE protects inter-TOE communication between the GoSilent Server and Cube from disclosure and modification using IPSec.

The TOE protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator.

The TOE provides reliable time stamps for its own use. The GoSilent Server obtains time from the virtualization server. Alternatively, the GoSilent Server time can also be set by an administrator. The GoSilent Cube time is set by an administrator.

The TOE provides administrators with the ability to query the current running version of its software and manually update the TOE. Updates are signed with an ID Technologies Security key. Once the image has been downloaded, the TOE checks the signature of the image (against the ID Technologies Security public key) before the image is applied.

At power-on tests are performed on each component to confirm the integrity of the firmware and a statistical assessment of the entropy source to include noise source health test and DRBG randomness.

4.9. TOE Access

The TOE provides session monitoring and management functions for local and remote administrative sessions. The TOE will terminate inactive local and remote interactive sessions after a configurable amount of time. Administrative users may terminate their own sessions.

4.10. Trusted Path/Channels

The TOE provides secure TLS channels between itself and local/remote administrators, including protected logging channels to ensure data in transit is protected.

5. Assumptions

The Security Problem Definition, including the assumptions, can be found in the following documents:

- *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020
- PP-Module for Stateful Traffic Filter Firewalls, v1.4e, 25 June 2020
- PP-Module for VPN Gateways, v1.2, 31 March 2022

That information has not been reproduced here and CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_V1.2 should be consulted if there is interest in that material.

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_V1.2 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices 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 clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the assurance activities specified in the CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_V1.2 and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_V1.2 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *ID Technologies GoSilent Cube + GoSilent Server 25.01 Common Criteria Guide*, Version 1.8, December 2022

All documentation delivered with the product is relevant to and within the scope of the TOE.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *ID Technologies GoSilent Cube + GoSilent Server v25.01 Detailed Test Report*, which is not publicly available. The *ID Technologies GoSilent Cube + GoSilent Server v25.01 Assurance Activities Report*, Version 0.5, December 2022 provides an overview of testing and the prescribed assurance activities.

8.1. Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA lab in Baltimore, MD from August 29, 2022, until December 20, 2022. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

8.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 1 and Table 2 below.

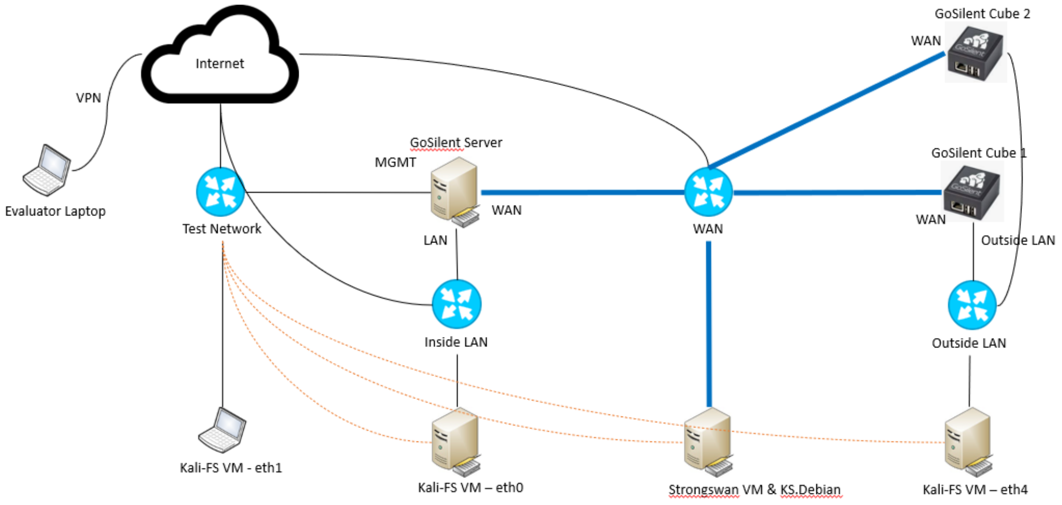

Figure 1: Devices in the Testing Environment

Table 2: Tools Used for Testing

Tool name	**Version**	**Description**
Lightship Greenlight	3.0.34	Tool used for TLS/X509 certificate modification as well as handshake modification
Lightship Strongswan	5.7.1	Tool used for IPsec modification for X.509 Certificates
Scapy	2.4.4	Packet generation tool
Packeth	1.6	Packet generation tool
Openssl	1.1.1k	Openssl was used for simple TLS server or TLS client connections and as an OCSP responder
StrongSwan	Linux StrongSwan U5.7.2/K4.19.0-22-amd64	Used for IPsec peer connections and algorithm testing
Wireshark	3.4.4 (Linux) & 3.6.5 (Windows)	Used for packet capture and analysis
Tcpdump	4.9.3	Used for packet capture and analysis
Apache	2.4.46	Web server hosting CRLs
Hping3	3.0.0	Firewall testing
Google Chrome	108.0.5359.125	Access to the TOE GUI

9. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined the ID Technologies GoSilent Cube + GoSilent Server v25.01 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_V1.2.

9.1. Evaluation of Security Target (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 ID Technologies GoSilent Cube + GoSilent Server v25.01 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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. Evaluation of Development Documentation (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 ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_V1.2 related to the examination of the information contained in the TSS.

The Validation 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. Evaluation of 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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team 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. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team 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. Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_V1.2 and recorded the results in a Test Report, summarized in the AAR.

The Validation team 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 Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *ID Technologies GoSilent Cube + GoSilent Server v25.01 Vulnerability Assessment,* Version 0.5, December 2022, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on December 2, 2022, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: https://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

The Evaluation team performed a search using the following keywords:

- Openssl
- Strongswan
- Syslog-ng
- GoSilent
- GoSilent Cube
- GoSilent Server
- IPSec
- TLS
- Linux kernel
- Intel Xeon E3-1270 v5
- AllWinner H5
- ARM v8
- Cortex-A53
- GSC-100
- GSC-120

The Validation team 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.

9.7. 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 followed the procedures defined in the CEM and performed the Assurance Activities in the CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_V1.2, and correctly verified that the product meets the claims in the ST.

10. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer 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.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11. Annexes

Not applicable.

12. Security Target

ID Technologies GoSilent Cube + GoSilent Server v25.01 Security Target, Version 1.18, December 2022.

13. GLOSSARY

- **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 to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001,* Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002,* Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003,* Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices*, Version 2.2e, March 23, 2020
6. *PP-Module for Stateful Traffic Filter Firewalls*, v1.4e, 25 June 2020
7. *PP-Module for VPN Gateways*, v1.2, 31 March 2022
8. *ID Technologies GoSilent Cube + GoSilent Server v25.01 Security Target*, Version 1.18, December 2022
9. *ID Technologies GoSilent Cube + GoSilent Server v25.01 Common Criteria Guide*, Version 1.8, December 2022
10. *ID Technologies GoSilent Cube + GoSilent Server v25.01 Assurance Activity Report*, Version 0.5, December 2022
11. *ID Technologies GoSilent Cube + GoSilent Server v25.01 Vulnerability Assessment,* Version 0.5, December 2022
12. *ID Technologies GoSilent Cube + GoSilent Server v25.01 Evaluation Technical Report*, Version 0.7, December 2022
13. *ID Technologies GoSilent Cube + GoSilent Server v25.01 Detailed Test Report*, Version 0.5, December 2022
14. *ID Technologies GoSilent Cube + GoSilent Server v25.01 Detailed Test Report Evidence,* Version 0.5, December 2022