National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

CACI idt GoSilent Server and Cube v26.01, Version 1.0

Report Number: CCEVS-VR-VID11685-2026
Dated: 07/23/26
Version: 0.1

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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

NIAP

Matthew Downey

Johns Hopkins University Applied Physics Laboratory

Farid Ahmed

Anne Gugel

Robert Wojcik

Alexander Lee

Common Criteria Testing Laboratory

Furukh Siddique

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the CACI idt GoSilent Server and Cube v26.01 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in July 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. 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 Gateways, Version 2.0,* 25 April 2024 (CFG_NDcPP-FW-VPNGW_V2.0)

This PP-Configuration includes the following components:

- Base-PP: *collaborative Protection Profile for Network Devices*, Version 3.0e (CPP_ND_V3.0E)
- PP-Module: *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4e (MOD_CPP_FW_V1.4E)
- PP-Module: *PP-Module for VPN Gateways*, Version 1.3 (MOD_VPNGW_V1.3)

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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), as interpreted by the Assurance Activities contained in the Protection Profile (PP). 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 and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 Product Compliant List.

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) 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
TOE	CACI idt GoSilent Server and Cube v26.01
Protection Profile	• CPP_ND_V3.0E • MOD_CPP_FW_V1.4E • MOD_VPNGW_V1.3
Security Target	CACI idt GoSilent Server and Cube v26.01 Security Target, v1.2 July 2026
Evaluation Technical Report	Evaluation Technical Report for CACI idt GoSilent Server and Cube v26.01, v0.5 July 2026
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	CACI idt
Developer	CACI idt
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Matthew Downey Farid Ahmed Anne Gugel Robert Wojcik Alexander Lee

3 Architectural Information

3.1 TOE Overview

The GoSilent Server acts as the centralized management and external access system for the TOE integrated into one system. The GoSilent Server provides the management GUI for configuration of GoSilent Server as well as the GoSilent Cube user devices. Operationally, it acts as the central peer for all IPsec connections from the GoSilent Cube devices and provides gateway connectivity to external systems located behind a GoSilent Cube.

The GoSilent Cube is a portable enterprise-grade firewall and VPN, ideal for sensitive communications, secure remote network access, and Internet of Things (IoT) deployments. GoSilent Cube can be setup within minutes by non-technical users. Physical Ethernet connections are supported on both the user side and VPN side of GoSilent Cube.

Together, GoSilent Cube and GoSilent Server provide a secure communications path to one or more systems located "behind" each GoSilent Cube. These systems connect to GoSilent Cube via physical Ethernet. Each GoSilent Cube establishes an IPsec VPN to the GoSilent Server, and all traffic from the user systems is routed over that VPN. Physical Ethernet is supported on the VPN side of GoSilent Cube.

The TOE applies policies to restrict the traffic that is permitted to pass between the user systems and external networks.

Management of the system is performed via a GUI provided by GoSilent Server, accessed via a browser on remote PCs using TLS/HTTPS. Authorized administrators may configure GoSilent Server as well as the GoSilent Cubes.

GoSilent Cubes also provide a GUI accessed from a browser on a user system via a TLS/HTTPS connection. This GUI only provides authorized administrators with the ability to configure that specific GoSilent Cube with enough information to connect to GoSilent Server. All additional configuration information is downloaded from GoSilent Server once the IPsec VPN is established.

Both GoSilent Server and GoSilent Cube generate audit records that are stored locally as well as sent to a remote syslog server via a TLS connection.

3.2 Evaluated Configuration

The GoSilent Server is a software TOE/virtual network device (vND) while GoSilent Cube is a physical network device (pND). The following platforms apply to these components.

Table 2: GoSilent Server and Cube v26.01 Platforms

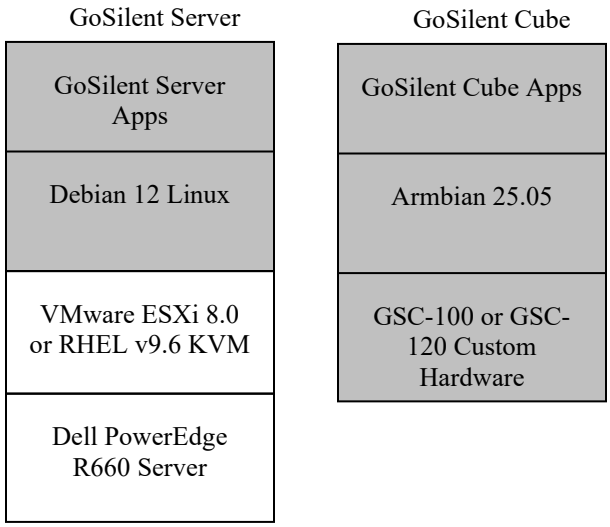
TOE Component	Hardware Model	CPU	CPU Microarchitecture	Virtualization	OS
GoSilent Server	Dell PowerEdge R660 Server	Intel Xeon Silver 4514Y	Raptor Cove	VMware ESXi v8.0	Debian 12
				Red Hat RHEL v9.6 KVM	
GoSilent Cube	CACI idt GSC-100	AllWinner H5/ Cortex A-53	ARM v8-A	N/A	Armbian 25.05
	CACI idt GSC-120				

4 Security Policy

4.1 Physical Boundary

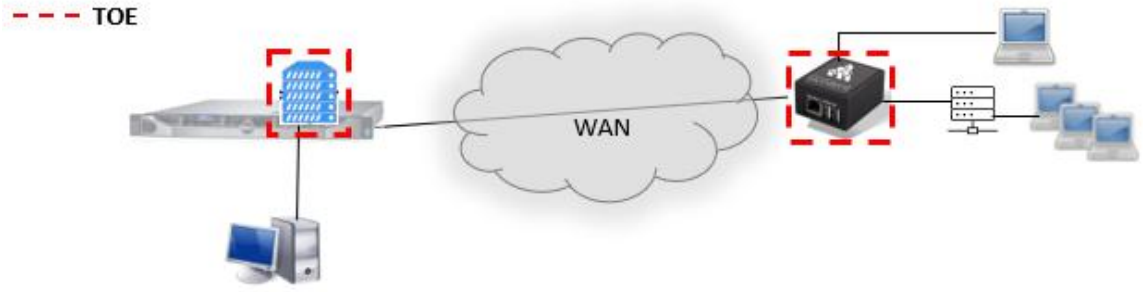
The physical boundaries of the TOE are the vND of the GoSilent Server virtual appliance and the custom physical enclosure of the GoSilent Cube pND. Figure 1 below illustrates the boundaries of the TOE (shaded areas in the figure).

Figure 1: TOE Boundary



The TOE is deployed in a distributed configuration with the GoSilent Server virtual appliance installed on a virtualization platform located at the enterprise destination and the GoSilent Cube at the user device side. The GoSilent Cube can be connected between a specific device and the LAN, or between an access switch with multiple user devices connected and the WAN. Figure 2 below shows the physical TOE deployment and the logical TOE boundary.

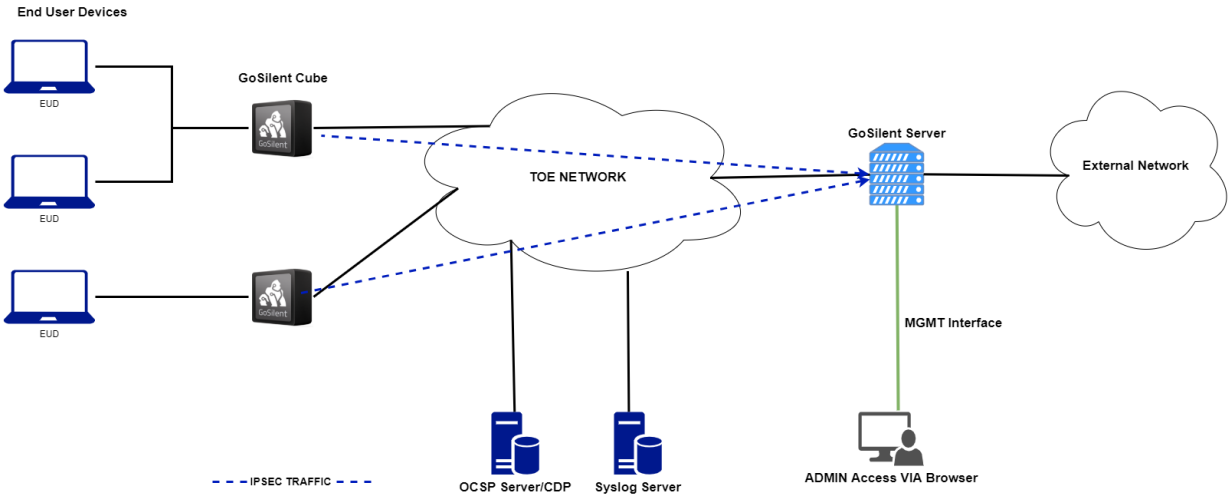
Figure 2: Representative TOE Deployment



The TOE management interfaces are depicted in

Figure 3.

Figure 3: TOE Interfaces



The TOE interfaces are as follows:

- **GUI (GoSilent Server).** Administrative GUI interface for managing GoSilent Server configurations and GoSilent Cubes. The GUI can be accessed via the GoSilent Server MGMT interface or from GoSilent Cube clients whose users are authorized administrators on GoSilent Server.
- **GUI (GoSilent Cube).** User GUI interface that provides limited functionality for initial cube configuration and authorized admin access to the GoSilent Server GUI.
- **Remote Logging.** Forwards TOE audit events to a syslog server for storage.
- **OCSP/CRL.** Certificate checking for IPSec connections are conducted by OCSP while CRLs are leveraged for syslog.
- **VPN Gateway.** VPN connections via IPSec.

The following items are required for the operational environment.

Table 3: Hardware and Software Environmental Components

Components	Mandatory/ Optional	Description
Ethernet dongle	Mandatory	Provides the WAN USB port of each GoSilent Cube for connection of the Cube to the WAN.
TOE Network	Mandatory	Provides connectivity between the TOE components. Since IPsec tunnels are layered on top of this network, the network itself is not required to be trusted.
External Network	Mandatory	GoSilent Server provides user systems with connectivity to systems on an External network, which may be limited to an Enterprise Network or provide much wider access.

Components	Mandatory/ Optional	Description
GoSilent Cube user networks	Mandatory	Physical Ethernet networks located on the user side of GoSilent Cube that provide connectivity between user systems and GoSilent Cube. In the simplest case, this is a direct connection using an Ethernet cable interconnecting the GoSilent Cube RJ45 Device port and a user system. To support multiple user systems, an Ethernet switch can be used.
Syslog Server	Mandatory	The Syslog Server receives audit messages from the TOE over a TLS connections and may be connected to the TOE Network or the External Network.
OCSP Server	Optional	Server accessed via OCSP to determine X.509 certificate revocation status for IPsec connections. The OCSP Server is connected to the TOE Network.
Certificate Distribution Points (CDP)	Optional	Servers accessed using HTTP to determine X.509 certificate revocation status for syslog connections. The CDPs may be connected to the TOE Network or the External Network.
User systems	Mandatory	IT systems using GoSilent Cube as a secure path to external systems.

The Cube devices are delivered to customers via trusted courier. The following checks should be performed upon receipt:

- Confirm that the correct device has been delivered per the packing slip and original order;
- Inspect all packaging to confirm there are no signs of tampering or damage incurred during transport.

The GoSilent Server software can be obtained digitally via URL provided to the customer directly by CACO idt.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions and Threats

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

- Base-PP: collaborative Protection Profile for Network Devices Version 3.0e (CPP_ND_V3.0E)
- PP-Module: *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4e (MOD_CPP_FW_V1.4E)
- PP-Module: *PP-Module for VPN Gateways*, Version 1.3 (MOD_VPNGW_V1.3)

That information has not been reproduced here and CPP_ND_V3.0E/MOD_CPP_FW_V1.4E/ MOD_VPNGW_V1.3 should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 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. A list of excluded functionalities has been documented in Sec 7.2.

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_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 and performed by the Evaluation team.

- This evaluation covers only the specific hardware models and software version identified in this document, and not any earlier or later versions released or in process.

- Apart from the Admin Guide, additional customer documentation for the specific Firewall, VPN Gateway models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

- 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_V3.0E/MOD_CPP_FW_V1.4E/

MOD_VPNGW_V1.3 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- CACI idt GoSilent Server and Cube v26.01 Security Target, v1.2 July 2026
- CACI idt GoSilent Server and Cube v26.01 User Guidance, v1.1, June 2026

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.

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 configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

Please refer to the evaluated configuration listed in section 3.2.

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- Cloud instances of GoSilent Server. GoSilent server is supported on virtual platforms and cloud instances; however, cloud deployments are not addressed by this evaluation.
- WiFi connectivity. The Cube is capable of accepting wireless connections from a client, however no security claims are made with respect to wireless connectivity and is therefore excluded from the evaluation.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for CACI idt GoSilent Server and Cube v26.01, which is not publicly available. The AAR 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 verified the product according to the vendor-provided guidance documentation and ran the tests specified in the CPP_ND_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 Protection Profiles. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here. In particular, sections 3.1 and 3.2 of the AAR describe the configuration of the test environment and the testing tools used.

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 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 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

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 CACI idt GoSilent Server and Cube v26.01 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 CPP_ND_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 Protection Profiles.

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 Evaluation of Development Documentation

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's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the CPP_ND_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 Protection Profiles related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

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 the Assurance Activities specified in the CPP_ND_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 Protection Profiles related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each 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 Evaluation of Test Documentation and the Test Activity

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_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 Protection Profiles and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the CPP_ND_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 Protection Profiles, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

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 CPP_ND_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 Protection Profiles, 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 CPP_ND_V3.0E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.3 Protection Profiles, 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 documentation referenced in Section 6 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

CACI idt GoSilent Server and Cube v26.01 Security Target, v1.2, July 2026

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology 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.
- **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.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. collaborative Protection Profile for Network Devices, Version 3.0e (CPP_ND_V3.0E)
6. PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e (MOD_CPP_FW_V1.4E)
7. PP-Module for VPN Gateways, Version 1.3 (MOD_VPNGW_V1.3)
8. CACI idt GoSilent Server and Cube v26.01 Security Target, v1.2, July 2026
9. Assurance Activity Report for CACI idt GoSilent Server and Cube v26.01, v0.6 July 2026
10. Evaluation Technical Report for CACI idt GoSilent Server and Cube v26.01, v0.5 July 2026
11. CACI idt GoSilent Server and Cube v26.01 User Guidance, v1.1 June 2026