Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : IC3S/MUM01/Symantec/NDcPP/0722/0032/CR

Product / system : Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4

Dated: 01-09-2023

Version: 1.0

Government of India
Ministry of Electronics & Information Technology
Standardization Testing and Quality Certification Directorate
6. CGO Complex, Lodhi Road, New Delhi – 110003 India

Product developer: **Symantec Corporation**

TOE evaluation sponsored by: **Symantec Corporation**

Evaluation facility: CCTL, Acucert Labs LLP, Mumbai
Wing-A, Ground Floor,
Beta Building, Unit No.
3, iThink Techno
Campus, Kanjurmarg
East Mumbai 400 042

Evaluation Personnel: Varsha Shetye, Yogesh Pawar, Yogita Kore

Evaluation Technical Report: IC3S/MUM01/Symantec/NDcPP/0722/0032/ETR

Validation Personnel: Sri Tapas Bandyopadhyay
Sri Ankit Jain

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product (TOE) below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	**Symantec Corporation**
Developer	**Symantec Corporation**
The Target of Evaluation (TOE)	**Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4** **TOE Version: 7.4.1.1**
Security Target	**Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4 Security Target version 1.0**
Brief description of product	The TOE is the Symantec Edge SWG running SGOS software version 7.4. The Symantec Edge SWG is not tied to any specific hardware. The TOE type is a network device. The purpose of the TOE is to provide a layer of security between an Internal and External Network (typically an office network and the Internet). The TOE allows administrators to create and manage configurable policies on controlled protocol traffic to and from the Internal Network users. A policy may include authentication, authorization, content filtering, and auditing. The Edge SWG appliances from Symantec provide companies the ability to deploy a scalable proxy-based security solution to protect their organization against advanced threats. The Edge SWG acts as gateway between web users and the Internet: a single point where all web traffic can be monitored and corporate policies for web use can be enforced. This strategic position makes the Edge SWG a natural place to build in additional network security technologies that defend against a very wide range of cybercrimes, malware, and phishing.
CC Part 2 [CC-II]	**Extended to CC Part 2 Version 3.1 Rev 5**
CC Part 3 [CC-III]	**Conformant CC Part 3 Version 3.1 Rev 5**
EAL	**--** **ST conforms to** **collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND]**
Evaluation Lab	**Common Criteria Test Laboratory, CCTL, Acucert Labs LLP, Mumbai, India**
Date Authorized	**17-12- 2022**

A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Ministry of Electronics and Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third-party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are-

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/MeitY/Govt. of India);
c) Common Criteria Testing Laboratories (CCTL, Acucert Labs LLP, Mumbai)

A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1 Rev 5
- Common Evaluation Methodology (CEM) Version 3.1.
- collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP]
- Supporting Document Mandatory Technical Document: CPP_ND_V2.2E_supporting_doc

A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation body **Common Criteria Test Laboratory (CCTL, Common Criteria Test Laboratory, CCTL, Acucert Labs LLP, Mumba, India has** conducted the evaluation of the product. Hereafter this has been referred as CCTL. The evaluation facility is recognized and empaneled under the IC3S scheme of STQC IT Certification Body.

Symantec Corporation, A division of Broadcom is the developer and sponsor of the TOE under certification.

The certification process is concluded with the completion of this certification report. This evaluation was completed on **11th August 2023** after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL 2) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version and release/build of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant apply for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B.1 Executive Summary

B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

Common Criteria Test Laboratory (**CCTL, CCTL, Acucert Labs LLP, Mumbai, India** has performed the evaluation. The information in the Certification Report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [**CCTL, CCTL, Acucert Labs LLP , Mumbai, India** The evaluation team has evaluated and confirmed that the security target [ST] that is used for evaluation of the product is CC Version 3.1, Rev 5 Part 2 extended and Part 3 conformant and concluded that the Common Criteria requirements for conformance to **collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP]** have been met.

B 1.2 Evaluated product and TOE

The TOE is the **Symantec Edge SWG running SGOS software version 7.4**. The Symantec Edge SWG is not tied to any specific hardware. The TOE type is a network device. The purpose of the TOE is to provide a layer of security between an Internal and External Network (typically an office network and the Internet). The TOE allows administrators to create and manage configurable policies on controlled protocol traffic to and from the Internal Network users. A policy may include authentication, authorization, content filtering, and auditing.

The Edge SWG appliances from Symantec provide companies the ability to deploy a scalable proxy-based security solution to protect their organization against advanced threats. The Edge SWG acts as gateway between web users and the Internet: a single point where all web traffic can be monitored and corporate policies for web use can be enforced. This strategic position makes the Edge SWG a natural place to build in additional network security technologies that defend against a very wide range of cybercrimes, malware, and phishing

For the Symantec Edge SWG with SGOS v7.4, TOE evaluated configuration is comprised of one instance of the SGOS executing on SSP -S410-20 hardware running ISG and a virtual appliance Dell Power Edge R440 hardware platform with ESXi 6.5.

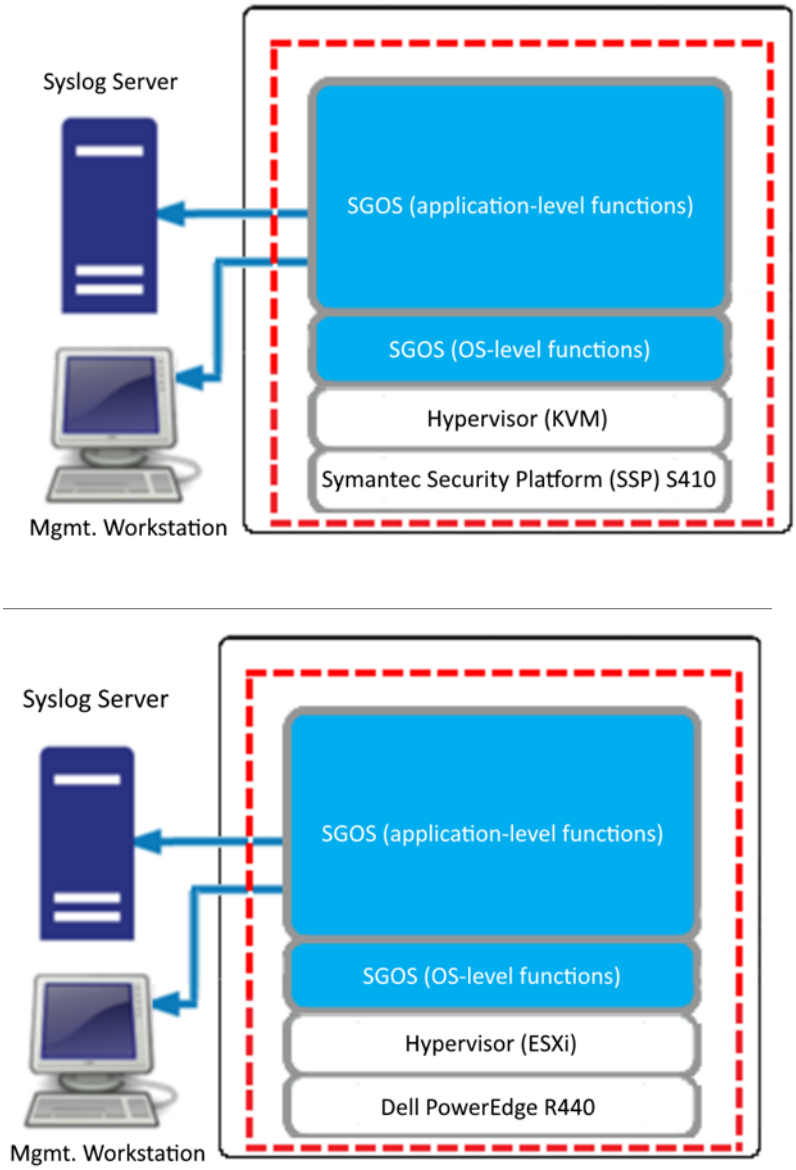

Figure 1: TOE Boundary

The TOE boundary includes the 'SGOS' software version 7.4. Licenses activate different features in the executable.

The TOE physical boundary also includes the following:

- **VMware ESXi 6.5 Hypervisor hosted on Dell Power Edge R440, with Intel 4216**
- **SSP-S410-20 with ISG using Intel 4210**

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter. The Security Functional Requirements (SFRs) are taken from CC Part 2.

B 1.4 Conduct of Evaluation

The common criteria evaluation of the TOE was initiated by the **IC3S Certification** Scheme of STQC

Certification Body vide communication no. IC3S/MUM01/Symantec/NDcPP/0722/0032 dated 25/07/2022.

The Target of Evaluation (TOE) is Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4. The TOE is the **Symantec Edge SWG running SGOS software version 7.4**. The Symantec Edge SWG is not tied to any specific hardware. The TOE type is a network device. The purpose of the TOE is to provide a layer of security between an Internal and External Network (typically an office network and the Internet). The TOE allows administrators to create and manage configurable policies on controlled protocol traffic to and from the Internal Network users. A policy may include authentication, authorization, content filtering, and auditing.

The Edge SWG appliances from Symantec provide companies the ability to deploy a scalable proxy-based security solution to protect their organization against advanced threats. The Edge SWG acts as gateway between web users and the Internet: a single point where all web traffic can be monitored and corporate policies for web use can be enforced. This strategic position makes the Edge SWG a natural place to build in additional network security technologies that defend against a very wide range of cybercrimes, malware, and phishing.

The Edge SWG offers the following features.

- High-speed decryption and re-encryption of SSL/TLS traffic, so attackers cannot use encryption to conceal malware or command and control traffic into and out of the corporate network,
- Universal Policy Enforcement (UPE) from Symantec allows organizations to enforce acceptable web use policies for employees who connect through the Edge SWG. Symantec allows you to centralize your policy creation, maintenance, and installation for simplified, unified administration.
- Out of the box protection - Recommended**, strong, and maximum policies crafted by security** experts.
- Immediate protection with the broadest advanced threat integrations
- Direct cloud application visibility and real-time controls
- Unmatched performance and reliability
- Logs and reports on how users connect to websites.
- Strong user authentication can be incorporated into the policies, supporting a wide variety of identity sources, including NTLM, LDAP, RADIUS, one-time passwords, and certificates
- Integration the world's largest civilian threat intelligence dataset with the Symantec Global Intelligence Network (GIN)
- When paired with other Symantec technologies, it can provide:

  Malware detection using multiple anti-malware engines and detection methods

  Multi-layered deep content inspection and analysis to detect spam and application-level threats in the payloads of network traffic

  Data Loss Prevention (DLP) to identify confidential information and block it from leaving the corporate network

  Cloud Access Security Broker (CASB) features to monitor and control what applications users can access and how documents and files are sent to the cloud

  Web (browser) isolation to create a safe browsing experience, prevent malware from moving from browsers onto employees' systems, and block sharing of credentials on suspicious websites

TOE was evaluated through evaluation of its documentation; independent testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM].

The evaluation has been carried out under written agreement between **CCTL, Acucert Labs LLP, Mumbai** and the developer/ sponsor **M/s Symantec Corporation.**

B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them, which might have an influence on this assessment.

B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B 1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST document].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

B 2 Identification of TOE

The TOE is the **Symantec Edge SWG running SGOS software version 7.4**

Table1: TOE details

Software Version	Image Name	Hash
SGOS 7.4.1.1 SWG Edition Release ID: 287291	EdgeSWG7.4.1_build287291.bcsi	MD5 – 143fbc9d80d2323f9861ac667b8d329e SHA256 – 37c08e40cad8644435d343a4ac7598dbe08b14f2fda2f273e4c8084f749248cb

B 3 Security policy

Following is the list of security features available in the TOE:

Audit Data Generation
User Identity Association
Protected Audit Event Storage
Cryptographic Key Generation
Cryptographic Key Establishment
Cryptographic Key Destruction
Cryptographic Operation (AES Data Encryption/Decryption)
Cryptographic Operation (Signature Generation and Verification)
Cryptographic Operation (Hash Algorithm)
Cryptographic Operation (Keyed Hash Algorithm)
NTP Protocol
Random Bit Generation

SSH Server Protocol
TLS Client Protocol without Mutual Authentication
Authentication Failure Management
Password Management
User Identification and Authentication
Password-based Authentication Mechanism
Protected Authentication Feedback
X.509 Certificate Validation
X.509 Certificate Authentication
X.509 Certificate Requests
Management of Security Functions Behaviour
Management of Security Functions Behaviour
Management of TSF Data
Management of TSF Data
Specification of Management Functions
Restrictions on security roles
Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
Protection of Administrator Passwords
TSF Testing
Reliable Time Stamps
Trusted Update
TSF-initiated Termination
User-initiated Termination
TSF-initiated Session Locking
Default TOE Access Banner
Inter-TSF Trusted Channel
Trusted Path

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 2: Assumptions

ID	Assumption
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 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.

ID	Assumption
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). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
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 ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
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 appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to 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.
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.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.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.

ID	Assumption
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

B.5 Evaluated configuration

The Symantec Edge SWG with SGOS v7.4, TOE evaluated configuration is comprised of one instance of the SGOS executing on SSP -S410-20 hardware running ISG and a virtual appliance Dell Power Edge R440 hardware platform with ESXi 6.5.

TOE description

The TOE is identified as **Symantec Edge SWG with SGOS v7.4**
Product (TOE): Symantec Edge SWG with SGOS v7.4

Software Version	Image Name	Hash
SGOS 7.4.1.1 SWG Edition Release ID: 287291	EdgeSWG7.4.1_build287291.bcsi	MD5 – 143fbc9d80d2323f9861ac667b8d329e SHA256 – 37c08e40cad8644435d343a4ac7598dbe08b14f2fda2f273e4c8084f749248cb

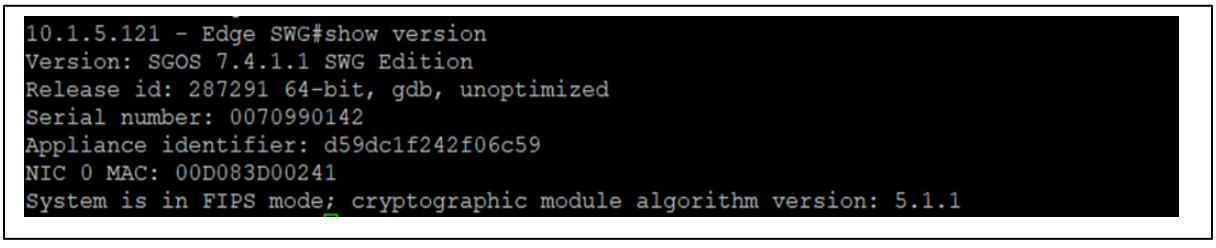

Table 3 - TOE Cryptography Implementation

Cryptographic Method	Use within the TOE
AES	• TLS Traffic Encryption/Decryption • SSH Traffic Encryption/Decryption
RSA	• TLS Session Establishment • SSH Session Establishment
SP800-90A	• TLS Session Establishment • SSH Session Establishment
SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification
HMAC-SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification
SP800-56A	• TLS Session Establishment • SSH Session Establishment
SP800-135rev1	• TLS Session Key Derivation • SSH Session Key Derivation

Table 4 - TOE Documentation

Reference	Title	Version	Date
[CC]	Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4 Common Criteria Administrative Guidance	0.8	August 4, 2023
[ST]	Symantec Edge SWG with SGOS v7.4 Security Target	1.0	August 11, 2023
[CM]	Symantec Edge SWG with SGOS 7.4 Configuration Management	0.4	August 11, 2023
[FSP]	Symantec Edge SWG with SGOS 7.4 Functional Specification Document	0.4	August 11, 2023
[CLI]	Edge SWG 7.4.x Command Line Interface Reference	-	-
[ISG]	ISG 2.1 Administration and Deployment Guide	-	-

TOE Environment:

Table 5 – IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Remote Management Workstation (GUI).	No	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS and TLS protected channels.
Remote Management Workstation (CLI).	Yes	This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels.
Local Management Workstation (CLI).	Yes	This includes any IT Environment Management workstation with a local CLI support that is used by the TOE administrator to support TOE administration through a direct connection.

Component	Required	Usage/Purpose Description for TOE performance
NTP Server	Yes	NTP server supporting SHA-1 integrity verification.
Audit Server	Yes	The audit server is used for remote storage of audit records that have been generated by and pulled from the TOE.
CA/OCSP Server	Yes	A server with a certification authority and certificate revocation list used by the TOE for validating the X.509 certificates used for TLS connection establishment.

Users of the TOE

The TSF maintains the roles Administrator

Table 6: Users

Role	Access
Security Administrator	The Security Administrator role shall be able to administer the TOE locally; The Security Administrator role shall be able to administer the TOE remotely

Technical Decisions

All NIAP TDs issued to date and applicable to NDcPP v2.2e have been considered. Table 7 identifies all applicable TDs.

Table 7 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0527: Updated to Certificate Revocation Testing (FIA_X509_EXT.1)	Y	
TD0528: NIT Technical Decision for Missing Eas for FCS_NTP_EXT.1.4	Y	
TD0536: NIT Technical Decision for Update Verification Inconsistency	Y	
TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	Y	
TD0538: NIT Technical Decision for Outdated link to allowed-with list	Y	
TD0546: NIT Technical Decision for DTLS – clarification of Application Note 63	N	The TOE does not support DTLS.
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Y	
TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test	N	The TOE does not support TLSS functionality.
TD0556: NIT Technical Decisions for RFC 5077 question	N	The TOE does not support TLSS functionality.
TD0563: NIT Technical Decision for Clarification of audit date information	Y	
TD0564: NIT Technical Decision for Vulnerability Analysis Search Criteria	Y	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0569: NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	N	The TOE does not support DTLSS functionality.
TD0570: NIT Technical Decision for Clarification about FIA_AFL.1	Y	
TD0571: NIT Technical Decision for Guidance on how to handle FIA_AFL.1	Y	
TD0572: NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Y	
TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Y	
TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Y	
TD0591: NIT Technical Decision for Virtual TOEs and hypervisors	Y	
TD0592: NIT Technical Decision for Local Storage of Audit Records	Y	
TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server	Y	
TD0632: NIT Technical Decision for Consistency with Time Data for vNDs	Y	
TD0633: NIT Technical Decision for Ipsec IKE/SA Lifetimes Tolerance	N	The TOE does not claim IPSec functionality.
TD0634: NIT Technical Decision for Clarification required for testing IPv6	Y	
TD0635: NIT Technical Decision for TLS Server and Key Agreement Parameters	N	The TOE does not claim TLS Server functionality.
TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH	N	The TOE does not support SSH Client functionality.
TD0638: NIT Technical Decision for Key Pair Generation for Authentication	Y	
TD0639: NIT Technical Decision for Clarification for NTP MAC Keys	Y	
TD0670: NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	N	The TOE does not claim TLSC with Mutual Authentication.

B.6 Document evaluation

B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility by the developer, are given below:

1. **Security Target:** Symantec Edge SWG with SGOS v7.4 Security Target Version 1.0
2. **TOE Functional Specification document**: Symantec Edge SWG with SGOS 7.4 Functional_Specification_Document v0.4
3. **Preparative procedures**: Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4 Common Criteria Administrative Guidance v0.8 , ISG 2.1 Administration and Deployment Guide
4. **Operational User guidance**: Edge SWG 7.4.x Command Line Interface Reference
5. **Configuration Management, Capability and scope and Delivery procedure:** Symantec Edge SWG with SGOS 7.4 CMv0.3

B.6.2 Analysis of document

The developer's documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

Development process: The evaluators have analyzed the functional specification of the TOE and found that the TOE security function interfaces [TSFI} are described clearly and unambiguously.

Guidance Documents: The evaluators have analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information was also clear and unambiguous.

Configuration management: The evaluators have analyzed configuration management documentation and determined that the TOE and its associated components and documents are clearly identified as configurable items (CI).

Delivery Procedure: Customers with an active account may download the TOE securely from: https://support.broadcom.com/group/ecx/ The TOE build maintains integrity throughout the delivery process by limiting access to current customers, supporting downloads over TLS, and providing an MD5 and SHA-256 hash for TOE verification post download.

B 7 Product Testing

Testing consists of the following three steps: Independent Testing by Evaluation Team, and Vulnerability analysis and Penetration testing.

B 7.1 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of test results. The evaluators have examined the TOE and it is found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:

The TOE has been installed properly as per the preparative procedure document. While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as

the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements. Independent testing is designed to verify the correct implementation of security functionalities available to different categories of users and to check whether audit record is being generated for auditable events, also checked for the privilege escalation is prevented.

The tests were designed to cover following TSFs and associated TSFIs of the TOE: The TOE provides the security functions required by the collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP.

Security Audit

The Network Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include:

- Start-up of the TOE from both cold boot and reboot,
- Shutdown of the TOE (when shut down from the local CLI and Remote CLI),
- All administrative actions (both security relevant and non-security relevant) from the local CLI and remote CLI,
- Remote administrative SSH connection establishment,
- Remote administrative SSH connection closure,
- Errors during Remote administrative SSH connection establishment,
- Generation of self-signed certificates,
- Import of certificates,
- Deletion of certificates,
- Successful authentication attempts (from the local CLI and Remote CLI),
- Unsuccessful authentication attempts (from the local CLI and Remote CLI),
- All attempts to update the TOE software,
- Changes to time,
- Start of a local administrative session,
- End of a local administrative session,
- Administration session timeout (from the local CLI and Remote CLI).

The TOE is configured to transmit its audit messages to an external audit server. Communication with the audit server is protected using TLS.

The logs for all the appliances can be viewed via the CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure.

Cryptographic Support

The TOE provides cryptographic support for the following features,

- TLSv1.2 connectivity with the following entities:
    - Audit Server.
- SSH connectivity with the following entities:
    - Management SSH Client.
- Secure software update

Table 8: Cryptographic Support

Cryptographic Method	Use within the TOE
AES	• TLS Traffic Encryption/Decryption • SSH Traffic Encryption/Decryption

Cryptographic Method	Use within the TOE
RSA	• TLS Session Establishment • SSH Session Establishment
SP800-90A	• TLS Session Establishment • SSH Session Establishment
SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification
HMAC-SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification
SP800-56A	• TLS Session Establishment • SSH Session Establishment
SP800-135rev1	• TLS Session Key Derivation • SSH Session Key Derivation

The TOE provides cryptographic support for the services as described in sections 5.2.2.1 through 5.2.2.13 of the ST "Symantec Edge SWG with SGOS 7.4 Security Target v0.9" under FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1/Data Encryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RBG_EXT.1, FCS_SSHS_EXT.1 and FCS_TLSC_EXT.1, security functional requirements.
The CAVP certificate numbers for the cryptographic algorithms are given in Table 15 of the ST .The TOE uses SGOS 7.4 with OpenSSL v3.0 to implement protocol logic as well as all the cryptographic primitives used by the protocols.

Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOE's administrator interfaces (local CLI and remote CLI). The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on any TOE administrative interface.

Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Management can take place over a variety of interfaces including:

- Local console command line administration;
- Remote CLI administration via SSH;

All administration functions can be accessed via remote CLI or via a direct connection to the TOE. The TOE provides the ability to securely manage the below listed functions;

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE.

Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification,

authentication, and access controls to limit configuration to Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, the TOE software (7.4) is custom-built for the appliance.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the security appliances themselves. The TOE verifies all software updates via digital signature (2048-bit RSA/SHA-256) and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE displays an Authorized Administrator specified banner on both the local and remote CLI management interfaces prior to allowing any administrative access to the TOE.

Trusted Path/Channels

The TOE supports several types of secure communications, including,

- Trusted paths with remote administrators over SSH,
- Trusted channels with remote IT environment audit servers over TLS.

B 7.2 Vulnerability Analysis and Penetration testing

The evaluators have considered the threats identified in ST and conducted vulnerability search from the information available in the public domain in search of potential vulnerabilities from public domain, scanning tools are used. Nmap tools was used for scanning to find out open ports. Nessus Vulnerability scanning tool is used with the latest plug in to find out hypothesized potential vulnerabilities present in the TOE. In compliance with AVA_VAN.1, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of examination are as follows:

- https://nvd.nist.gov/view/vuln.search
- http://cve.mitre.org/cve
- https://www.cvedetails.com/vulnerability-search.php
- https://www.kb.cert.org/vuls/search/
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com
- https://www.rapid7.com/db/vulnerabilities

The evaluator examined public domain vulnerability searches by performing a keyword search. The Terms used for this search were based on the vendor's name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- Blue Coat ProxySG
- SGOS v7.4
- SGOS v7.4.1.1
- SGOS
- Symantec Proxy SG Operating
- ISG v2.4.2.1

- cpe:/:broadcom:symantec_proxysg
- Broadcom ProxySG
- Symantec ProxySG
- Symantec ProxySG_firmware
- Secure Gateway
- Symantec Web Proxy
- Symantec Blue Coat ProxySG
- SSP-S410-20
- Dell Power Edge R440
- cpe:2.3:o:vmware:esxi:6.5:650-201701001:*:*:*:*:*:*
- Intel 4210
- Intel 4216
- Opensslv3.0
- TLS v1.2
- SSH
- TCP
- UDP

The vulnerability search was performed on July 5 2022, June 9 2023, June 30 2023, August 4 2023 and August 11, 2023. Any open vulnerabilities applicable to the TOE were identified, along with their mitigations .The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

The evaluator has analyzed the evaluation evidences like, the ST, the Functional Specification, and the Guidance Documentation and as well as the operational environment, stated in the ST and then hypothesized the security vulnerabilities considering five categories of attack to the Security functions, viz. 'Bypassing', 'Tampering', 'Direct Attacks', 'Monitoring' and 'Misuse'.

The evaluator has identified the following Attack scenarios.

Threat perception 1: An expert who is conversant in IT technology would be able to succeed in an attack with two weeks by modifying and applying an attack tool available on the internet

Threat perception 2: Encrypted channel may be intercepted and if attacker becomes successful to decrypt algorithms used

Threat perception 3: Information Flow Function can be tampered if TSF can be made unavailable through DoS attack using misconfiguration

Threat perception 4: Audit record mechanism can be tampered by consuming audit storage space.

Threat perception 5: MiTM attack.

Threat perception 6: Password Complexity Bypass

The relevant attack potentials, corresponding to the identified vulnerabilities have been estimated considering various factors like the 'time to identify & exploit', 'expertise required', 'knowledge of the TOE', 'windows of opportunity' and 'equipment required'. The calculated attack potentials are as follows:

The Evaluator could not able to exploit the hypothesized Security vulnerabilities/ concern of the TOE evolved through analysis of evaluation objects.

Hence, it is concluded that the TOE does not contain any exploitable vulnerability for 'Basic' Attack Potential.

The evaluation team has restricted their Penetration Testing activities to the attack scenarios for which the estimated attack potential is less than 10. Considering the attack potential as 'Basic', the evaluators could exploit no identified vulnerabilities.

Hence, the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'. However, these Vulnerabilities may be exploited with higher attack potential.

Subsequent to the independent review of public domain vulnerability databases and all evaluation evidences, potential vulnerabilities were identified with their attack potentials. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing.

The penetration testing could not exploit any vulnerability in the intended operational environment of the TOE. However, these vulnerabilities may be exploited with higher attack potential.

Residual Vulnerabilities

Considering the attack potential as 'Basic', the evaluators could exploit no identified vulnerabilities. Hence, the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'. However, these vulnerabilities may be exploited with higher attack potential.

The identified vulnerabilities, having attack potential more than 'Basic' were not considered for penetration testing. Hence, these vulnerabilities may be considered as residual vulnerabilities.

B 8 Evaluation Results

The evaluation team has documented the evaluation results in the Evaluation Technical Report [ETR]. The TOE was evaluated through evaluation of its evaluation evidences, documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedures.

Documentation evaluation results:

The documents for TOE and its development life cycle have been analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CC Version 3.1 Revision 5.

Testing:

The independent functional tests yielded the expected results, giving assurance that 'Symantec Edge SWG with SGOS v7.4' behaves as specified in its [ST].

Vulnerability assessment and penetration testing:

The evaluator search on the sources listed in Section A4 of the NDcPP SD v2.2 to determine a list of potential flaw hypotheses that are more recent that the publication date of the NDcPP, and those that are specific to the TOE and its components as specified in NDcPP SD v2.2. The evaluator examined results of information publicly available and found NO vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined in the CEM. Vulnerability assessment was carried out with Nessus tool. The penetration testing with '**Basic**' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

Table 9: Assurance classes and components wise verdict

Assurance classes and components			Verdict
Security target document evaluation		ASE	PASS
1.	ST introduction	ASE_INT.1	PASS
2.	Conformance claims	ASE_CCL.1	PASS
3.	Security problem definition	ASE_SPD.1	PASS
4.	Security objectives	ASE_OBJ.1	PASS
5.	Extended component definition	ASE_ECD.1	PASS

Assurance classes and components			Verdict
6.	Derived Security requirements	ASE_REQ.1	PASS
7.	TOE Summary Specification	ASE_TSS.1	PASS
TOE Development evaluation		ADV	PASS
1	Security-enforcing functional specification	ADV_FSP.1	PASS
TOE Guidance document evaluation		AGD	PASS
1	Operational user guidance	AGD_OPE.1	PASS
2	Preparative procedure	AGD_PRE.1	PASS
TOE Life cycle support evaluation		ALC	PASS
1	Use of a CM system	ALC_CMC.1	PASS
2	Parts of the TOE CM coverage	ALC_CMS.1	PASS
Testing of the TOE		ATE	PASS
1	Independent Testing - Sample	ATE_IND.1	PASS
Vulnerability assessment of the TOE		AVA	PASS
1	Vulnerability Analysis	AVA_VAN.1	PASS

B 9 Validator Comments

The Validator has reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, worksheets, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4 Security Target version 1.0 has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that 'Symantec Edge SWG with SGOS v7.4, all the security functional requirements (SFR) and Security assurance requirements (SAR) as defined in the [ST]. Hence, the TOE is recommended for conformance to collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND]**
- **Certification as per CC version 3.1 Revision 5.**

B 10 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
EAL: Evaluation Assurance Level
ETR: Evaluation Technical Report
FSP: Functional Specification
IC3S: Indian Common Criteria Certification Scheme
IT: Information Technology
PP: Protection Profile
ST: Security Target
TOE: Target of Evaluation
TDS: TOE Design Specification
TSF: TOE Security Function

TSFI: TOE Security Function Interface

B 11 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [ST] : Symantec Edge SWG with SGOS v7.4, Security Target, Version 1.0
6. [ETR]: Evaluation Technical Report No. Evaluation Technical Report for Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4 Security Target, v1.0- v0.5