Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : IC3S/BG01/HALTDOS/EAL2/0317/0008/CR

Product / system : HaltDos Mitigation Platform version 1.1 comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0.

Dated: 11-02-2019

Version: 1.0

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

This report contains a total of 15 pages. In case it needs to be reproduced, all the pages must be included.

Product developer: **Haltdos.com Private Limited**
E – 52, Sector -3, NOIDA, UP, 201301, India

TOE evaluation sponsored by: **Haltdos.com Private Limited**
E – 52, Sector -3, NOIDA, UP, 201301, India

Evaluation facility: **CCTL, ETDC, Bengaluru**
STQC Directorate,
Ministry of Electronics & Information Technology,
Peenya Industrial Estate, Ring Road, Bengaluru,
Karnataka, 560058, India

Evaluation Personnel:

1. E Kamalakar Rao
2. Ankit Jain
3. Ziaul Hasan

Evaluation report: **IC3S/BG01/HALTDOS/EAL2/0317/0008/ETR1.0**

Validation Personnel: Tapas Bandyopadhyay

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY 4
A1 Certification Statement 4
A2. About the Certification Body 4
A3 Specifications of the Certification Procedure 5
A4 Process of Evaluation and Certification 5
A5 Publication 5

PART B: CERTIFICATION RESULTS 6
B.1 Executive Summary 6
B 2 Identification of TOE 8
B 3 Security policy 8
B.4 Assumptions 9
B.5 Evaluated configuration 9
B.6 Document evaluation 11
B 7 Product Testing 12
B 8 Evaluation Results 14
B 9 Validator Comments 15
B 10 List of Acronyms 15
B 11 References 15

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	**Haltdos.com Private Limited ,E – 52, Sector -3, Noida, UP, 201301, India**
Developer	**Haltdos.com Private Limited E – 52, Sector -3, Noida, UP, 201301, India**
The Target of Evaluation (TOE)	**HaltDos Mitigation Platform version 1.1** **comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0.**
Security Target	**HaltDos Mitigation Platform Version 1.1 Security Target , version 1.4**
Brief description of product	The Target of Evaluation (TOE) **is HaltDos Mitigation Platform version 1.1 comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0.** The TOE secures data centre from network and application layer, distributed denial of service (DDoS) attacks. The TOE can be installed on a single, stand-alone appliance that can be deployed in an enterprise IT network to detect, block, and report on various categories of Distributed Denial of Service (DDoS) attacks. The TOE provides Layer 3 to Layer 7 DDoS detection and mitigation (filtering) capability that minimize application downtime in the event of a DDoS attack. The appliance installed with the TOE is usually deployed at ingress points of an enterprise (before or after the ingress router) to detect, block, and report on various categories of DDoS attacks. The TOE continuously monitors all incoming and outgoing traffic and can automatically detect and mitigate various types of DDoS attacks targeting online services.
CC Part 2 [CC-II]	Conformant to CC Part 2 Version 3.1 Rev 5
CC Part 3 [CC-III]	Conformant CC Part 3 Version 3.1 Rev 5
EAL	EAL2+ (Augmentation with ALC_CMC.3 and ALC_CMS.3)
Evaluation Lab	Common Criteria Test Laboratory, ETDC , Bengaluru
Date Authorized	30-06-2017

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 Department of 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, ETDC (Bangalore).

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
- Common Evaluation Methodology (CEM) Version 3.1.

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), STQC IT Services – ETDC , STQC Directorate, Peenya Industrial Estate, Ring Road, Bengaluru, Karnataka, 560058, India** has conducted the evaluation of the product.. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

M/s **Haltdos.com Private Limited, Noida, UP, India** 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 04-02-2019 after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL) 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 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, ETDC, Bangalore), Peenya Industrial Estate, Ring Road, Bengaluru, Karnataka 560058 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], ETDC, and Bengaluru), Peenya Industrial Estate, Ring Road, Bengaluru, Karnataka 560058 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, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

B 1.2 Evaluated product and TOE

HaltDos Mitigation Platform version 1.1, comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0. The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The product build /version number is 1.0-2.0 - 1.0 - 2.0 built date 20-4-2018. The Evaluated Configuration, its security functions, assumed operational environment, architectural information and evaluated configuration are given below (Refer B2 to B5).The TOE & Its Physical Environments & Boundaries are depicted in Figure 1 and Figure 2 .

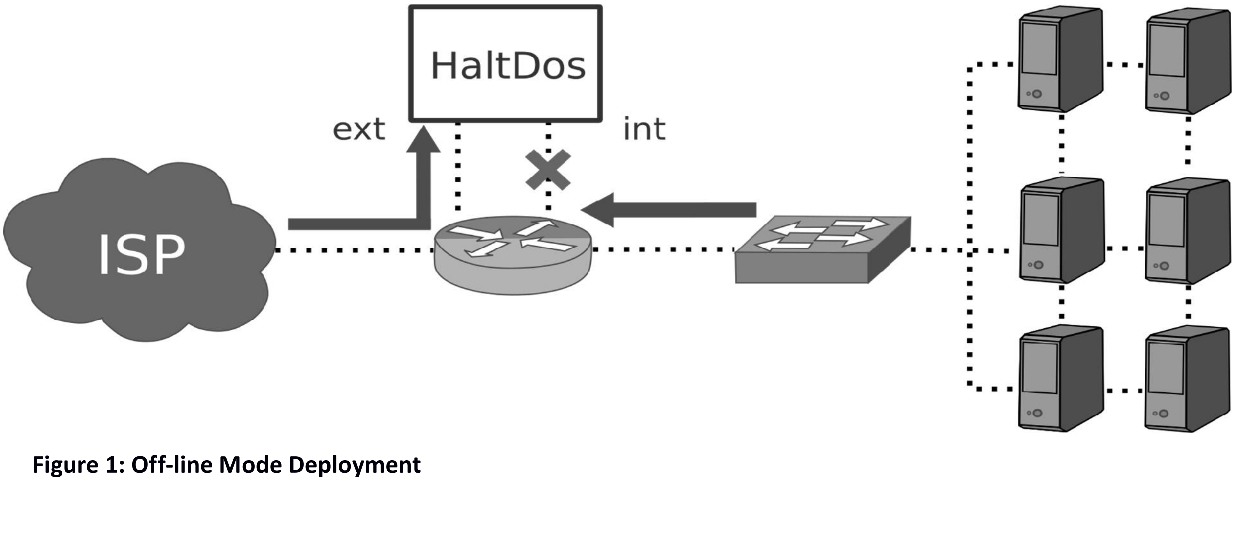

Figure 1: Off-line Mode Deployment

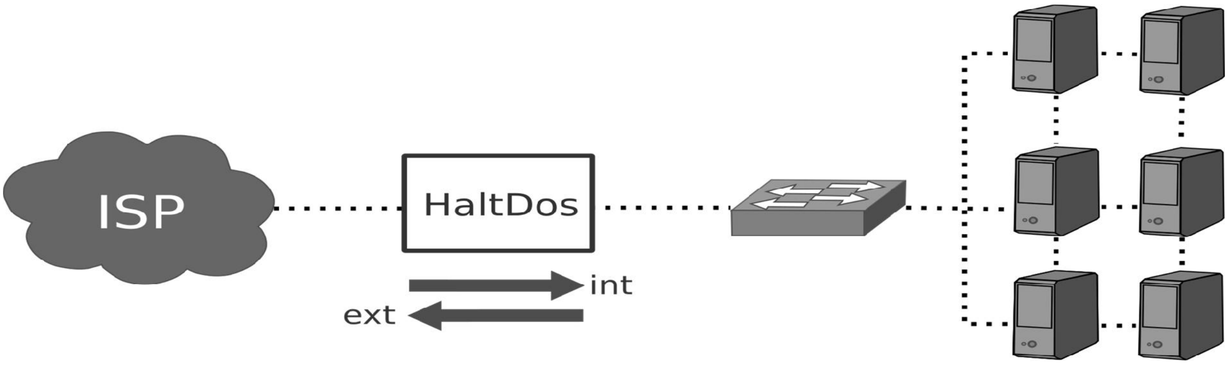

Figure 2: In-line Mode Deployment

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 IT Certification Body vide communication no. STQC/CC/1617/27 dated 23 June 2017.

The Target of Evaluation (TOE) is **HaltDos Mitigation Platform version 1.1 ,comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0.**. The TOE secures data Centre from network and application layer, distributed denial of service (DDoS) attacks. The TOE can be installed on a single, stand-alone appliance that can be deployed in an enterprise IT network to detect, block, and report on various categories of Distributed Denial of Service (DDoS) attacks. The TOE provides Layer 3 to Layer 7 DDoS detection and mitigation (filtering) capability that minimize application downtime in the event of a DDoS attack. The appliance installed with the TOE is usually deployed at ingress points of an enterprise (before or after the ingress router) to detect, block, and report on various categories of DDoS attacks. The TOE continuously monitors all incoming and outgoing traffic and can automatically detect and mitigate various types of DDoS attacks targeting online services.

TOE was evaluated through evaluation of its documentation; independent testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM]. The Evaluation Assurance Level is augmented to **EAL 2+ by adding ALC_CMC.3 and ALC_CMS.3 from the Common Criteria Version 3.1 R5.**

The evaluation has been carried out under written agreement [30-06-2017] between CCTL, ETDC Bengaluru and the developer/ sponsor M/s Haltdos.com Private Limited.

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].
- 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 **HaltDos Mitigation Platform version 1.1, comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0.The TOE has the following identification details:**

- **Build Number: 1.0-2.0-1.0-2.0**
- **Build Date: 20-04-2018**
- **Version Number: 1.1**

B 3 Security policy

Following is the list of security features of the TOE:

- **Audit data generation and User identity association**
- **Audit review, Selectable audit review**
- **Protected audit trail storage**
- **User attribute definition**
- **Verification of secrets**
- **Multiple authentication mechanism ,User authentication before any action**
- **User identification before any action**
- **Management of TSF data**
- **Specification of management functions**
- **Security roles**
- **Failure with Preservation of Secure State**
- **Reliable Time Stamps**
- **DDoS Defence**
- **Security Notifications**
- **Inter-TSF trusted Channel**
- **Trusted Path / Channel**

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 1: Assumptions

Item	Assumption ID	Assumption Description
1	A.BACKUP	Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost.
2	A.CONNECT	The TOE will separate the network on which it is installed and operates into external and internal networks. Information cannot flow between the external and internal networks without passing through the TOE unless the TOE is set into bypass mode
3	A.NOEVIL	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
4	A.PHYSICAL	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

B.5 Evaluated configuration

The Target of Evaluation (TOE) is **HaltDos Mitigation Platform version 1.1, comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0.**. The TOE secures data Centre from network and application layer, distributed denial of service (DDoS) attacks.The Target of Evaluation (TOE) is HaltDos Mitigation Platform version 1.1. It is a software solution comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0. The TOE can be installed on a single, stand-alone appliance to protect Internet Protocol (IP) networks from threats against Distributed Denial of Service (DDoS) attacks. The TOE provides Layer 3 to Layer 7 DDoS detection and mitigation (filtering) capability that minimize application downtime in the event of a DDoS attack. The appliance installed with the TOE is usually deployed at ingress points of an enterprise (before or after the ingress router) to detect, block, and report on various categories of DDoS attacks. The TOE continuously monitors all incoming and outgoing traffic and can automatically detect and mitigate various types of DDoS attacks targeting online services. The TOE is identified as **HaltDos Mitigation Platform v1.1**:

Build Number: 1.0-2.0-1.0-2.0, **Build Date:** 20-04-2018

TOE Components	Version	Size	hash value (SHA512)
hdInspector	1.0	3.27 MB	79c4b843ec505f5dd2b1129f2aa35229528ee00a2be5f1181f723bc51cd147e45311d4e5ddd37613c4b9b08a9c2f29ea3124769086885e07a6b5d6f7e523e847
hdDeviceUI	2.0	157 MB	27d4d596c51980fa19b427d21eddc3cdcd60ba811912de1810a099a26b57e01fd1e7c52072840f77e9915d340adf6c04718bf17927ea3edbdf273c79a5a9c966
hdDetection Service	1.0	69.4 MB	85d046c6d8958ce7e0ad05d5e38717e993307d63a4c9cb61ed19c0eebf4429800b79fc731224f9469889571ca6e62c34192fd8c6383992873fba

			ba78db3f93b0
hdCLI	2.0	10.3 KB	02fc5c16d2d8f981dffab2ac98c21668435efe08 95c7408d7b69f34e53965cb65586108477199d 9577d7ecea9892b8d9d4950b965c6983d36ad4 17634d4349b0

All four binaries are archived as zip then ENTIRE SIZE IS 221MB and then sha512 is used to find the hash.
ED56FB350236F119259AE8E4B1EDBEADC48DAF A5C91FF109EF4A1DEBA0D97C15CD923E6A0637
F2445F88C5C035FBF3BC89A417622AE8202994314AE136850132
The TOE is flexible to run in multiple operational modes. The following operational modes of deployment are supported:

1. **In-line Mode**
   Active: With filtering enabled (Active mode)
   Bypass: With filtering disabled (Bypass mode)
2. **Off-line Mode** through span port or network tap, with filtering disabled

In off-line mode, the TOE monitors traffic from a span port or network tap, which collectively are referred to as monitor ports. The router or switch sends the traffic along its original path and mirrors to the appliance running the TOE. The TOE analyses the mirror traffic and detects possible DDoS attacks, and but does not perform any DDoS mitigation.

Only the traffic coming from external network (usually the internet) should be sent to the appliance running the TOE on the EXT# interface. The traffic coming from protected network (usually the internal traffic) can optionally be sent to the INT# interfaces. The TOE in off-line mode never forwards traffic from EXT# ports to INT# ports or vice-versa.

Off-line mode is most commonly used in trial implementations. For example, before deploying The TOE in in-line mode and allowing it to affect the enterprise network traffic, it can be deployed in off-line mode for fine-tuning as per the enterprise IT network. The TOE requires a Linux operating system with Ubuntu 16.04 LTS as the officially supported operating system. The TOE uses MySQL v5.7 database as a data store and Intel DPDK framework is used for receiving and sending packets.

TOE Environment:

TOE is running on the top of the Ubuntu 16.04 operating system. It has four components –

- hdDeviceUI is running on tomcat server.
- hdDetectionService is running on tomcat server.
- hdInspector is running on Intel DPDK to intercept traffic between #INT and #EXT.
- hdCLI to access system from remote system over trusted path (SSH).

To access TOE, the following interfaces are exposed:

- INT#: Network interface connecting the TOE with internal network
- EXT#: Network interface connecting WAN / Router to the TOE
- MGT#: Network interface that is configured for access to organization's security administrator / Analyst.

Excluded from the TOE:

The following assets are included in the IT Environment and are not part of the TOE:

- Optional NTP Server (highly recommended for enterprise time syncing)

- Optional SMTP Server (for notifications)
- Optional RADIUS Server (for AAA)
- Operating System (Ubuntu 16.04 LTS)
- Database (MySQL v5.7.17)
- Web Server (Apache Tomcat v8.0)
- Intel DPDK platform v17.02
- Appliance on which the TOE runs
- Web browser (and its host platform) is not included in the TOE boundary

  The network assets communicating on the network proving data flow through the TOE

The following functionality is not included in the scope of the evaluation:

- HaltDos Programmable API

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, is given below:

1. **Security Target**
2. **TOE Functional Specification document**:
3. **Preparative procedures**: Preparatory Guidance Document
4. **Operational User guidance**: Operational User Guidance, AGD_OPE:
5. **Configuration Management, Capability and scope**
6. **TOE Design document**
7. **Security Architecture**
8. **Functional Test Document**
9. **Test Coverage document**
10. **Life Cycle Model document**
11. **Delivery Procedure**
12. **Development Security**

B.6.2 Analysis of document

The developers 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.

Life-cycle support documents: The Life cycle support process document, containing information on Configuration Management, delivery procedure , development security document were evaluated.

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).

B 7 Product Testing

Testing effort required for EAL2 consists of the following three steps: Developers test and test coverage analysis, Independent Testing by Evaluation team, Vulnerability analysis and Penetration testing by Evaluation team.

B7.1 IT Product Testing by Developer

The developer's testing covers the security functional behaviour of all TSFIs and interactions of all subsystems. The relevance, coverage and depth of the developer tests has been examined and verified by the evaluators during the evaluation. The evaluators have verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results and test coverage analysis, as documented in the [ETR].

The evaluators have reviewed the developer's test coverage analysis and found them to be complete and satisfactory. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

B 7.2 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:

a. **Security Audit**

The TOE's auditing capabilities include recording information about system processing and access to the TOE. Subject identity (user login name) and outcome are recorded for each event audited. The audit records generated by the TOE are protected by the TOE. The audit trail is comprised of the TOE change log and the syslog. The audit records can be offloaded for long-term storage.

b. **Identification and authentication**

Each user must be successfully identified and authenticated with a username and password by the TSF. The TOE provides a password-based authentication mechanism to administrators. Access to security functions and data is prohibited until a user is identified and authenticated.

c. **Security management**

The TOE allows only authorized users with appropriate privileges to administer and manage the TOE. Only authorized administrators with appropriate privileges may modify the TSF data related to the TSF, security attributes, and authentication data. The TOE maintains 4 default roles (authorities):

Administrator (Read, Write, & Execute all), Visitor (read-only access from Web UI), Network analyst (Read, Write and Execute only network configurations) and Security Analyst (Read, Write and Execute only security configurations). In addition, a system administrator is the Linux OS administrator user. Only system administrator can operate the CLI.

d. Resource Utilization (DDoS Protection):

The TOE sits at the perimeter of the network, referred to as the edge, to protect Internet Protocol (IP) networks against DDoS attacks by successfully identifying and filtering DDoS attacks, while forwarding legitimate traffic to the network without impacting service. The TOE can function in in-line active (monitoring and filtering), in-line Bypass (monitoring without filtering) or off-line modes. The TOE provides capabilities to filter traffic by multiple means. These means include filtering on Whitelist, Blacklist, Rate Limits, malformed HTTP, and TCP SYN Rate configuration specifications to name a few. Visual alerts for Web GUI users and alarms can be configured to warn the recipient of an event or action that has taken place. The formats can take the form of an email or syslog message.

e. Protection of Security Functions

The TOE transfers all packets passing through the TOE only after processing the traffic based on traffic attributes. If a hardware failure occurs and the TOE does not repair itself, the TOE forces the appliance to go into a hardware bypass mode. This shunts the “EXT#” and “INT#” ports, maintaining all traffic flow through the equipment. Thus, the DDoS filtering function may be unavailable, but the flow of traffic will not be impeded. The communication between the remote manager and the TOE are protected from disclosure and modification. The TOE provides reliable timestamps on its own or with the support of an NTP Server in the IT environment. The TSF is protected because the hardware, the OS and the application the logical access to the TOE is controlled by the identification and authentication functionality provided by the TOE.

f. TRUSTED PATH/CHANNELS

The TOE requires the establishment of HTTPS (SSL/TLS) connection from the remote administrator’s browser. The TOE also requires the establishment of SSH connection in order to access the TOE remotely to use the CLI. The TOE communicates with external authentication mechanisms via trusted channel. The TOE provides a communication channel between itself and the external authentication mechanisms that is logically distinct from other communication channels and provides assured identification of its ends and protection of the channel data from modification or disclosure.

Additional tests carried out:

1. Tests related to detection and mitigation of following DDoS attacks by using Traffic Filtering Techniques:
2. Blacklist mitigation (based on country and IP both) ,Whitelist Attack, TOR IP ,IP Reputation ,Invalid Packet Size ,Connection Proxy
3. Test related to hardware bypass on failure of power.
4. Tests related to detection and mitigation of following DDoS attacks by using Traffic Shaping Techniques :ICMP flood , UDP flood , DNS flood, TCP flood, SYN flood, HTTP flood
5.

B 7.3 Vulnerability Analysis and Penetration testing

In search of potential vulnerabilities from public domain, scanning tools are used. Scanning was conducted to find out open ports and their vulnerabilities. OpenVAS scanning tool is used with the latest feeds to find out hypothesized potential vulnerabilities present in the TOE.

The TOE documents like, Security Target (ST), TOE architecture & Design (TDS), TOE Preparatory guidance document etc. were analyzed to find out potential security vulnerability and the same is listed in.

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.

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 potential vulnerabilities with higher than 'Basic' attack potential are treated as residual vulnerabilities.

Penetration testing scenarios are summarized as below:

- Authentication with default credentials
- Inheriting privileges or other capabilities that should otherwise be denied; i.e., whether users of different roles can escalate their privileges beyond their defined privileges as given in ST, bypassing implemented mechanism in SSR8010 environment
- Inheriting privileges or other capabilities that should otherwise be denied; i.e., whether users of different roles can escalate their privileges beyond their defined privileges as given in ST, bypassing implemented mechanism.
- Denial of service through flooding of crafted packets

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.

B7.4 Site Visit

The evaluator also have visited the development site to assess the configuration management system, delivery system and overall development security of the site.

B 8 Evaluation Results

The evaluation team has documented the evaluation results in the [ETR].
The TOE was evaluated through evaluation of its evaluation evidences, documentation, testing and vulnerability assessment and site visit 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 CCv3.1 for EAL1.

Testing:
The independent functional tests yielded the expected results, giving assurance that '**HaltDos Mitigation Platform version 1.1 comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService**

version 1.0 and hdCLI version 2.0' behaves as specified in its [ST].

Vulnerability assessment and penetration testing:

The penetration testing with '**Basic**' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

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] 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 'HaltDos Mitigation Platform version 1.1 comprising of hdInspector version 1.0, hdDeviceUI version 2.0, hdDetectionService version 1.0 and hdCLI version 2.0"satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL2+ (Augmentation in respect of SAR configuration management system components ALC-CMC.3 and ALC_CMS.3) Certification**.

However, it should be noted that there are no **Protection Profile** compliance claims.

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] : HaltDos Mitigation Platform Security target version 1.4
6. [ETR]: Evaluation Technical Report No. STQC/CC/16-17/27/ETR1.0 /v1.0