HaltDos Mitigation Platform

Version 1.1

Security Target

Version 1.4

September 17, 2018

Prepared For

Haltdos.com Private Limited
E – 52, Sector -3,
NOIDA, UP, India – 201301
Ph: 0120-4545911 Fax: 0120-4243669

www.haltdos.com

Revision History

Date	Version	Author	Description
April 10, 2017	1.0	Anshul Saxena	First Draft
Jan 03, 2017	1.1	Anshul Saxena	Second Draft as per recommendations
April 25, 2018	1.2	Anshul Saxena	Third draft as per recommendation
June 22, 2018	1.3	Anshul Saxena	Fourth draft as per recommendation
September 17, 2018	1.4	Anshul Saxena	Final draft

Table of Contents

List of Tables and Figures

1 Security Target Introduction

1.1 Security Target Reference

ST Title:	HaltDos Mitigation Platform
ST Version:	v1.4
ST Author:	Haltdos.com Private Limited
ST Date:	September 17, 2018

1.2 TOE Reference

TOE Identification: 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.
Refer section 1.4.8.2 for the list of dependencies (hardware/software/firmware) needed by the TOE but excluded from evaluation.

TOE Vendor: Haltdos.com Private Limited

1.3 TOE Overview

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.

Following is the list of security features of the TOE:

- Audit data generation
- 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

Further details about the security requirements are mentioned in section 6. All the features mentioned above are under evaluation.
This Security Target (ST) defines the Information Technology (IT) security requirements for the TOE. The TOE is being evaluated at assurance level EAL2+.

Refer section 1.4.8.1 for the lists of the software components that describe the TOE and are under evaluation. Also refer to section 1.4.8.2 for the list of dependencies (hardware/software/firmware) needed by the TOE but are excluded from the evaluation.

1.3.1 TOE Type

The TOE is a Distributed Denial of Service (DDoS) detection and mitigation platform.

1.3.2 TOE Build Number

The TOE has the following identification details:

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

1.3.2.1 Identification Method:

The TOE uses the following mechanism to uniquely identify each platform version release and its associated components:

- **Component Versioning:**
  Each component (hdInspector, hdUI, hdCLI, hdDetectionService) has a version of its own. Whenever a component is changed and ready for release, its version is incremented by 1. For example, if hdCLI has a current version of v1.0, the next version released will be v2.0.
- **Build Numbering:**
  Build number has the following format:

<hdInspector Version> **-** <hdUI Version> **-** < hdDetectionService Version> **-** <hdCLI Version>

1.3.2.2 Platform Versioning:

The TOE can be identified by the unique reference provided as the platform version. Versions of the TOE (HaltDos Mitigation Platform) is classified into the following releases:

- **Major Releases**: These are the major updates of the platform provided by the development team. Versions v1.0, v2.0, v3.0 and so on are assigned to the major releases.
- **Minor releases**: These are the minor updates within a major release provided by the development team. Versions v1.1, v1.2, v1.3 and so on are assigned to the minor releases, overall 9 minor releases are provided ranging from 1 to 9 i.e. v1.1 to v1.9
- **Development releases**: These are the development updates within a minor release provided by the development team. Versions v1.1101, v1.1102, v1.1103 and so on are assigned to the development releases.

1.4 TOE Description

1.4.1 Acronyms

Table 1-1 and Table 1-2 define product specific and CC specific acronyms respectively.

Acronym	Definition
AAA	Authentication, Authorization, & Accounting
API	Application Programming Interface
CDN	Content Delivery Network
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CSV	Comma Separated Value
DDoS	Distributed Denial of Service
DNS	Domain Name Server
FCAP	Flow Capture fingerprint expression language
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MSSP	Managed Security Service Provider
NIC	Network Interface Card
NTP	Network Time Protocol
PPS	Packets Per Second
RDN	Registered Domain Name
RADIUS	Remote Authentication Dial-in User Service for Authentication, Authorization and Auditing
SIP	Standard Initiation Protocol
SMTP	Simple Mail Transport Protocol

SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Security Layer
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

TABLE 0-1: PRODUCT SPECIFIC ACRONYMS

Acronym	Definition
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

TABLE 1-2: CC SPECIFIC ACRONYMS

1.4.2 Description

The Target of Evaluation (TOE) is HaltDos Mitigation Platform version 1.1 comprises 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.

It is recommended that the appliance running the TOE be hardware bypass capable. This ensures that the environment factors such as power failures, hardware failures, or software failures affecting the proper functioning of the TOE will result in bypassing all network traffic albeit unmitigated.

The TOE is flexible to run in multiple operational modes. The following operational modes of deployment are supported:

- In-line Mode
  - Active: With filtering enabled (Active mode)
  - Bypass: With filtering disabled (Bypass mode)
- 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 also 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.

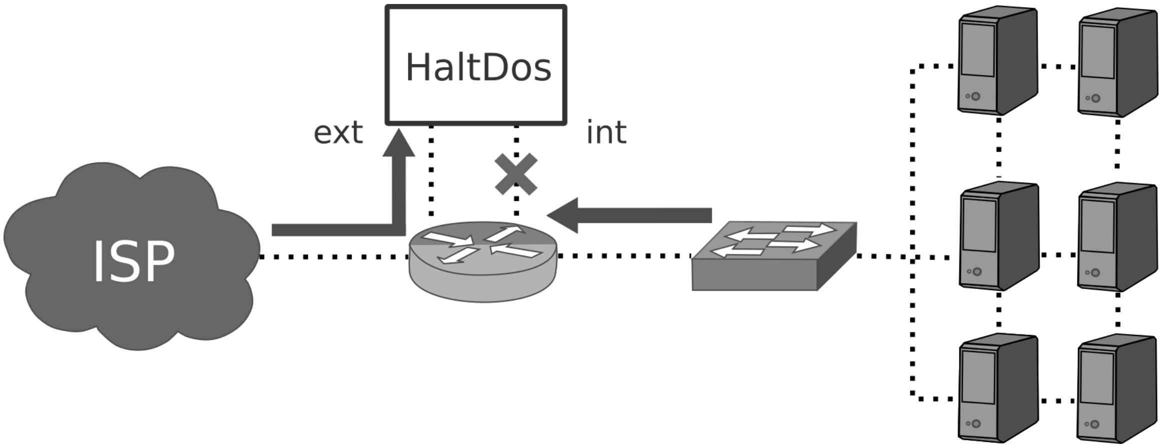


FIGURE 1-1: OFF-LINE MODE DEPLOYMENT

In in-line mode deployment, the appliance running the TOE acts as a physical cable between the external network (usually the internet) and the protected network (usually internal network). In in-line deployment all of the traffic between external and protected network flows through the TOE.

During deployment an ethernet cable from the external network (an upstream router or the service provider's equipment) is connected to an EXT# interface of the appliance running the TOE. The corresponding INT# interface on the same appliance is connected to the equipment in the protected network (usually a firewall or a router or a switch).

When in Active mode, the TOE analyses the traffic, detects DDoS attacks (if any), and applies appropriate mitigations (traffic filtering) before forwarding. When in Bypass mode, the TOE analyses the traffic but only detects DDoS attacks (if any). No mitigations (traffic filtering) is performed in Bypass mode.

Bypass mode of operation generates information that can be used to set/customize the TOE settings for accurate attack detection and mitigation. When policy is ready for operational implementation in production environment, the administrator can change the protection mode to “Active”.

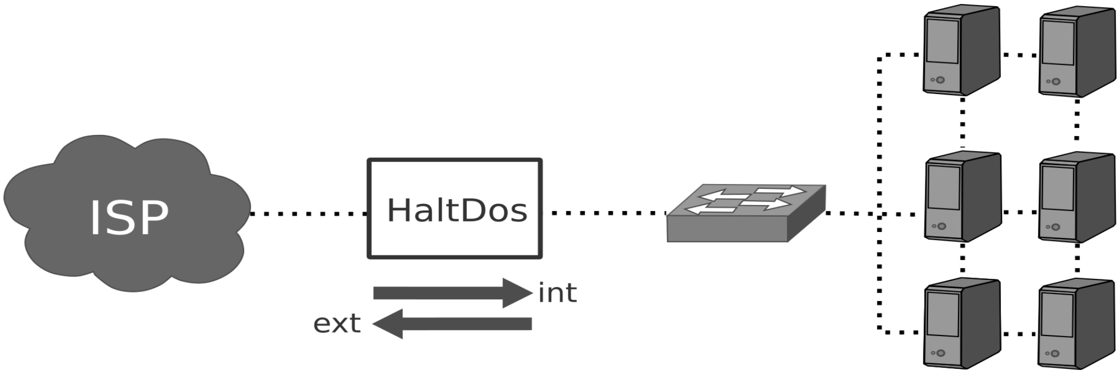


FIGURE 1-2: IN-LINE MODE DEPLOYMENT

1.4.2.1 TOE Dependencies

The TOE is a software solution comprising of various software components (refer section 1.2) that can be installed on a single stand-alone appliance. The TOE requires a linux operating system with Ubuntu 16.04 LTS as the officially supported operating system. MySQL v5.7 database is used as a data store by the TOE and Intel DPDK framework is used for receiving and sending packets. All the dependencies are open source software and (except for the linux operating system) all dependencies are managed, maintained and compiled by the developer. The table below presents common environmental considerations for the appliance running the TOE:

Power Options	550W (1+1) Redundant hot plug PSU AC: 100 to 127 VAC, 50 to 60 Hz, 6 A max 200 to 240 VAC, 50 to 60 Hz, 3 A max DC: -48 to -60 VDC, 13 A Max
Environment	Temperature, operating: 60º to 95ºF (0º to 35ºC) Humidity, operating: 8% to 90% Humidity, non-operating: 95%, non- condensing at temperatures of 73º to 104ºF (23º to 40ºC)
Physical Dimensions	Chassis: 1U/2U rack height Height: 0.28cm Width: 48.2 cm
Monitoring Compatibility	Optional integration with management consoles supporting SNMP v2 or SNMP V3

TABLE 1-3: HALTDOS APPLIANCE COMMON FEATURES

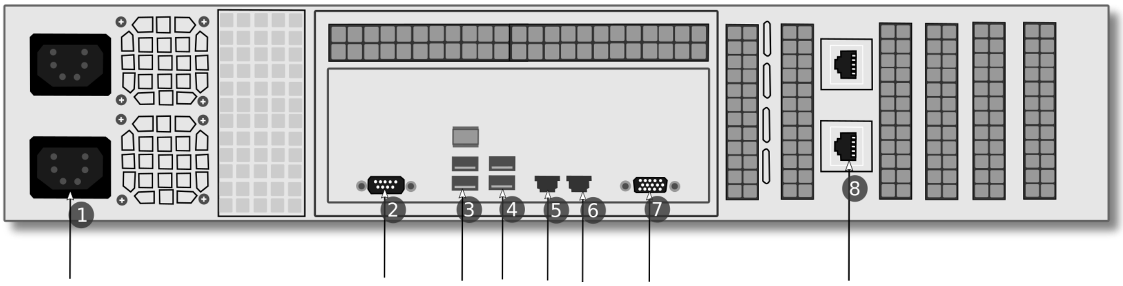


FIGURE 1-3: BACK PANEL OF THE HALTDOS APPLIANCE WITH 1G COPPER INTERFACES

1	Power Supply (AC module).	**2**	Serial port (optional)
3	USB0 and USB1 (1 on the top, 0 on the bottom)	**4**	USB2 and USB3 (3 on the top, 2 on the bottom)
5	Management port, MGT (GbE NIC 1 connector)	**6**	IPMI port (GbE NIC 1 connector)
7	VGA port to connect monitor.	**8**	Protection ports (1G copper is shown) 1G. The protection ports are configured as port pairs. Each pair consists of an external (EXT) port and an internal (INT) port.

* Minimum configuration needed to run the TOE.

The following diagrams show how the protection ports are numbered for each of the available interfaces:

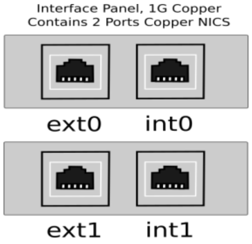


FIGURE 1-4: PROTECTION INTERFACES

The network path to be protected is connected to any two like-numbered interfaces. The “EXT#” interface always connects to the external network, and the “INT#” interface always connects to the protected network, as shown in Figure 1-2: In-line mode Deployment.

1.4.3 User Description

User authorities provide the means to organize the TOE users into different levels of permitted system access. When a user account is created, it must be assigned to a user authority. The user account inherits the access levels that are assigned to that authority. The TOE contains the following predefined user authorities.

Authority	Access
ADMINISTRATOR	Users with this authority have full read and write access on all pages of the Web GUI.
NETWORK_ANALYST	Users with this authority have full read and write access on all network related aspects in the Web GUI.
VISITOR	Users with this authority have read-only access to most of the Web GUI pages and can edit and update their own user account settings. Users in this group cannot change any configuration settings.
SECURITY_ANALYST	Users with this authority have full read and write access on all security related aspects and have read only access to other pages in Web GUI.
SYSTEM ADMINISTRATOR	These are Linux OS users on the TOE appliance that have administrator privileges. These users can log onto the appliance via SSH to run system commands and access the CLI to maintain and configure the TOE. Some of the CLI commands make API calls to Web GUI. For such command, this user must also be ADMINISTRATOR on Web GUI

TABLE 1-4: PREDEFINED USER AUTHORITY

This grouping of users into authorities that restricts/permits TSF functionality for any user is referred in Common Criteria as “roles”.

1.4.4 User Interfaces

1.4.4.1 Web based User Interface (GUI)

The main administrative interface after the TOE has been installed is a web based GUI that is accessed by connecting to the IP address of the MGT interface of the TOE. This is provided by hdDeviceUI software that is written in Java and is capable of showing network statistics via graphs and dashboards, traffic monitoring, attack alarm notifications, attack summaries, real time and historic traffic details, audit trail and configuration management.

hdDeviceUI uses HTTPS protocol for secure sessions over the MGT interface. This interface is not available through the INT# or EXT# interfaces. The first time GUI is accessed, the user must accept the SSL certificate to complete the secure connection.

The GUI menu bar indicates which menu is active and provides the ability to navigate the GUI menus and pages. The menus that are available depend on the user authority to which the authorized user is assigned. The menu bar is divided into the following menus:

Menu	Description
Home	Displays the key points of traffic monitored by the TOE
Events	Displays the information about the recent events that occurred in the TOE
Dashboard	Displays information about the traffic that the TOE monitors and mitigates.

Action	Provides ability to view, configure and manage security settings of the TOE.
Alarms	Provides ability to view, set alarms for traffic passing through the TOE.
Web Analytics	Provides the ability to view and configure rules for Web Analytics done by the TOE.
Report	Provides the functions to view report and statistics of the traffic that the TOE monitors.
Settings	Provides the functions to configure and maintain system settings of the TOE appliance.

TABLE 1-5: MENU BAR OF HDDEVICEUI

1.4.4.2 Command Line Interface (CLI)

The command line interface is provided through hdCLI. It allows authenticated user to enter commands on the terminal. Typically, the CLI is used for installing and upgrading the software and completing the initial configuration. However, some advanced functions can only be configured by using the CLI.

The HaltDos CLI can be accessed either directly or remotely. The following figure shows the options and ports that can be used to connect to the appliance in order to access the CLI.

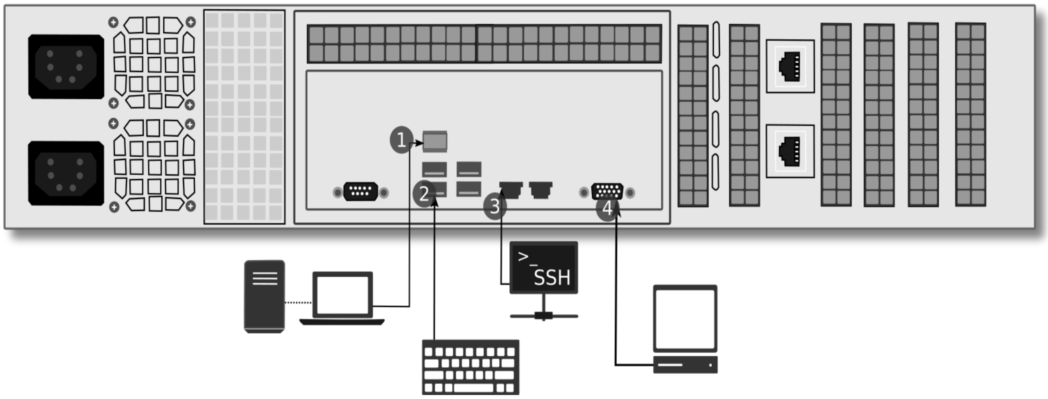


FIGURE 1-5: OPTIONS FOR CONNECTING TO THE CLI

The following table describes the connections in the figure:

Item	Connection
1	Serial port for console access on server
2	USB port with keyboard and VGA connector with monitor (direct connection)
3	Management port MGT with SSH

TABLE 1-6: CONNECTION OPTIONS

The CLI functionality is limited to:

- Installing and reinstalling the solution
- Retrieving and Updating configuration
- Backup and Restoration
- Setting hardware bypass settings
- Downloading updates
- Generating reports

1.4.5 TOE Data Description

TSF Data includes information used by the TSF in making decisions. It includes the systems parameters set by administrators to configure the security of the TOE security attributes, authentication data and traffic control attributes. Examples of TSF Data include administrative roles and audit logging parameters.

User Data includes the Data created by external and internal IT entities that does not affect the operation of the TOE. User Data is separate from the TSF data. The information flows created by Clients and Servers are examples of User Data.

1.4.6 Product Guidance

The following product guidance documents are provided with the TOE:

Reference Title	**ID**
HaltDos User Guide	[ADMIN]
HaltDos Release Notes	[RELEASE]

TABLE 1-7: TOE USER GUIDANCE DOCUMENTS

1.4.7 Business View of the TOE

The TOE is a high throughput, high performance software-based DDoS detection and mitigation platform that can run of qualifying hardware and can stay updated with evolving technology and threats through software updates without requiring any hardware replacements. With its multi-layered and multi-vector approach, it can defend against a wide range of DDoS attacks within seconds to ensure high uptime of protected online services such as website and web services.

It has following features:

- Provides multi-layered security (Layer 3 to Layer 7)
- Always on protection with real time metrics and analytics
- Alerts on attack, attack signature, customer misbehaviour and audit trails

1.4.8 Physical Scope of the TOE

The physical boundary of the TOE is the entire appliance running the TOE. The TOE will be evaluated in the “in-line mode” deployment scenario.

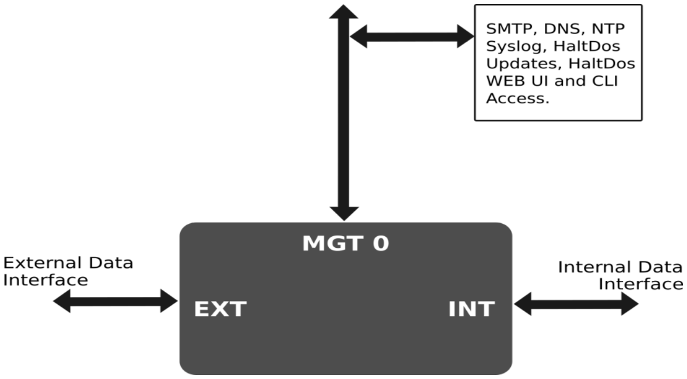

SMTP, DNS, NTP Syslog, HaltDos Updates, HaltDos WEB UI and CLI Access.
MGT 0
External Data Interface
EXT
INT
Internal Data Interface

FIGURE 1-6: TOE PHYSICAL BOUNDARY

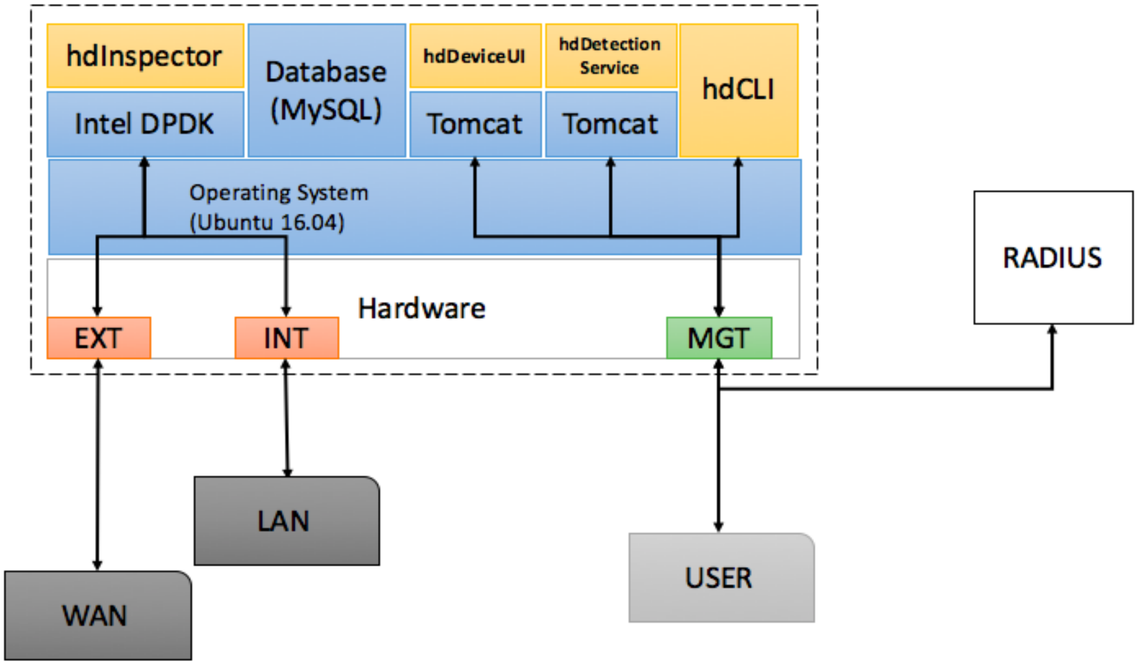


FIGURE 1-7: TOE ENVIRONMENT

1.4.8.1 Included in the TOE:

The scope of the evaluation includes the following product components and/or functionality (marked in yellow in Figure 1-7):

TOE and its user interfaces:

- HaltDos Web Interface (hdDeviceUI)
- HaltDos Command Line Interface (hdCLI)
- HaltDos Detection Service (hdDetectionService)
- HaltDos Inspector (hdInspector)

TOE configuration conditions for evaluation:

- In-line Mode
- Default passwords must be changed during installation.
- Use of CLIs are scoped to those functions described in Section 1.4.4.2

1.4.8.2 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

1.4.9 Logical Scope of the TOE

TOE provides the following security functionality:

- **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.

- **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.

- **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). There is also a system administrator who is the Linux OS administrator user. Only system administrator can operate the CLI.

- **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.

- **Protection of TSF:**
  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.

- **Trusted Channel/Path:**
  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 end points and protection of the channel data from modification or disclosure.

1.4.10 Environment of the TOE

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.

Following are the components of the TOE environment:

- 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

1.4.11 Delivery Method

Before the components are scheduled for delivery, the appliance along with the platform goes through verification and acceptance testing at the developer premise. Once verification is completed, the hardware is reset with a bare minimum software installation including:

- Ubuntu 16.04 operating system
- TOE installation script

The appliance is the packed in a shipping box and once the shipment is done, the following are shared with the end user over the registered email:

- Shipment details
- Purchase Order
- Delivery Challan (containing the serial no. and model no.) of hardware
- The TOE license
- Hardware Manual and User Guidance documents

The delivered appliance can be identified by the unique identifier serial number assigned by the developers. Following is the format used for generating the serial number:

```
Format: hd-<haltdos-model>-number
Example: hd-swift-01
```

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2+ by adding ALC_CMC.3 and ALC_CMS.3 from the Common Criteria Version 3.1 R5.

This document conforms to the Common Criteria (CC) for Information Technology (IT) Security Evaluation, Version 3.1, Revision 5, dated April 2017.

2.2 Protection Profile Claim

This ST does not claim conformance to any existing Protection Profile.

2.3 Package Claim

This ST claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2+.

- hdInspector claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2.
- hdDeviceUI claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2.
- hdDetectionService claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2.
- hdCLI claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2.

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.

3 Security Problem Definition

3.1 Threats

The TOE must counter the threats to security listed in Table 3-1. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

Item	Threat ID	Threat Description
1	T.AUDIT	Unauthorized attempts by users and external IT entities to access network resources through the TOE, TOE data or TOE security functions may go undetected because the actions they conduct are not audited or audit records are not reviewed, thus allowing an attacker to escape detection.
2	T.DDoSATTACK	An External IT Entity or group of External IT Entities may exhaust service resources of the TOE or Internal IT Entities by passing information flows through the TOE by DDoS attacks thus making the resources unavailable to its intended users.
3	T.FAILURE	A Hardware, Software and/or Power failure of the TOE may interrupt the flow of traffic between networks thus making them unavailable.
4	T.MANAGE	An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete TSF data on the TOE
5	T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
6	T.PROCOM	An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

TABLE 3-1: TOE THREATS

3.2 Assumptions

The assumptions regarding the security environment and the intended usage of the TOE are listed in Table 3-2.

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, wilfully 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.

TABLE 3-2: ASSUMPTIONS

3.3 Organizational Security Policies

There are no Organizational Security Policies defined for the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are listed in Table 4-1.

Item	Objective ID	Description
1	O.AUDIT	The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.
2	O.DDoSALERT	The TOE will provide the capability to alert administrators when DDoS attacks are detected and other customizable events, conditions, and system errors.
3	O.DDoSMITIGATE	The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDoS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDoS attacks, and authorized users who may overuse resources.
4	O.FAILSAFE	The failure of the TOE must not interrupt the flow of traffic through the TOE between networks.
5	O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions.
6	O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
7	O.PROCOM	The TOE will provide a secure session for communication between the TOE and the remote administrator's browser trying to access the Web GUI or remote access to the CLI

TABLE 4-1: TOE SECURITY OBJECTIVES

4.2 Security Objectives for the Operational Environment

The security objectives for the Operational Environment are listed in Table 4-2.

Item	Environment Objective	Description
1	OE.AUDIT	The IT environment must provide a long term audit and alert store for the TOE.
2	OE.BACKUP	Those responsible for the TOE must ensure that the audit files, configuration files are backed up and disk usage is monitored to ensure audit information is not lost.
3	OE.CONNECT	Those responsible for the TOE must ensure that the TOE is installed and operated on a network and separates the network into external, internal and management networks. Information cannot flow between the networks without passing through the TOE unless the TOE is set into hardware bypass

4	OE.NOEVIL	Those responsible for the TOE must ensure that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains and the authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
5	OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

TABLE 4-2: SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

4.3 Security Objectives Rationale

Item	TOE Objective	Threat
1	O.AUDIT	T.AUDIT
2	O.DDoSALERT	T.MANAGE
3	O.DDoSMITIGATE	T.DDoSATTACK
4	O.FAILSAFE	T.FAILURE
5	O.IDAUTH	T.NOAUTH
6	O.MANAGE	T.MANAGE
7	O.PROCOM	T.PROCOM

TABLE 4-3: MAPPING OF TOE SECURITY OBJECTIVES TO THREATS/POLICIES

Item	Environment Objective	Threat/Policy/Assumption
8	OE.AUDIT	T.AUDIT
9	OE.BACKUP	A.BACKUP
10	OE.CONNECT	A.CONNECT
11	OE.NOEVIL	A.NOEVIL
12	OE.PHYSICAL	A.PHYSICAL

TABLE 4-4: MAPPING OF SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT TO THREATS/POLICIES/ASSUMPTIONS

Table 4-5 shows that all the identified Threats to security are countered by Security Objectives. Rationale is provided for each Threat in the table.

Item	Threat ID	Objective	Rationale
1		O.AUDIT The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.	This threat is mitigated by O.AUDIT which requires that the TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security thus providing administrators the ability to investigate incidents.
		OE.AUDIT The IT environment must provide a long term audit for the TOE.	OE.AUDIT requires that IT environment must provide a long term audit store for the TOE thus providing administrators with a longer history to investigate incidents with.
2	T.DDoSATTACK An External IT Entity or group of External IT Entities may exhaust service resources of the TOE or Internal IT Entities by passing information flows through the TOE by DDoS attacks thus making the resources unavailable to its intended users.	O.DDoSMITIGATE The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDoS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDoS attacks, and authorized users who may overuse resources.	This threat is mitigated by O.DDoSMITIGATE, which requires that the TOE must limit resource usage to an acceptable level (stop clients from overusing resources and stop DDoS attacks). The TOE must also be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DOS and DDoS attacks, and authorized users who may overuse resources.
3	T.FAILURE A Hardware, Software and/or Power failure of the TOE may interrupt the flow of traffic between networks thus making them unavailable.	O.FAILSAFE The failure of the TOE must not interrupt the flow of traffic through the TOE between networks.	This threat is mitigated by O.FAILSAFE which ensures that the flow of traffic through the TOE is not interrupted during TOE failure creating a DDoS scenario.

4	T.MANAGE An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete TSF data on the TOE	O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	This threat is mitigated by O.MANAGE, which requires that The TOE must protect stored TSF data from unauthorized disclosure, modification, or deletion. The TOE provides role based access control to management functions.
		O.DDoSALERT The TOE will provide the capability to alert administrators when DDoS attacks are detected and other customizable events, conditions, and system errors.	This threat is mitigated by O.DDoSALERT which provides the alerting required to warn administrators about events that happened or are happening that may require further management intervention.
5	T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions.	This threat is mitigated by O.IDAUTH, which provides for unique identification and authentication of administrative users.
6	T.PROCOM An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.	O.PROCOM The TOE will provide a secure session for communication between the TOE and the remote administrator's browser trying to access the GUI or remote access to the CLI.	This threat is mitigated by O.PROCOM which requires that the TSF must provide a secure session for communication between the TOE and the remote administrator's web browser trying to access the Web GUI or remotely accessing the CLI.

TABLE 4-5: ALL THREATS TO SECURITY COUNTERED

Table 4-6 shows that the security objectives for the operational environment uphold all assumptions. Rationale is provided for each Assumption in the table.

Item	Assumption ID	Objective	Rationale
1	A.BACKUP Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost.	OE.BACKUP Those responsible for the TOE must ensure that the audit files, configuration files are backed up and disk usage is monitored to ensure audit information is not lost.	This objective provides for the backup of the TOE audit and configuration files by administrators to ensure data loss minimization due to hardware or software errors.
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.	OE.CONNECT Those responsible for the TOE must ensure that the TOE is installed and operated on a network and separates the network into external, internal and management networks. Information cannot flow between the networks without passing through the TOE.	This objective provides for placing the TOE at the network perimeter and ensuring that information flow cannot flow between internal and external networks without TOE inspection unless the TOE is set into hardware 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, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	OE.NOEVIL Those responsible for the TOE must ensure that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains and the authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	This objective provides for competent and non-hostile personnel to administer the TOE. This objective ensures the TOE is delivered, installed, managed, and operated by competent individuals.
4	A.PHYSICAL The TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	OE.PHYSICAL Those responsible for the TOE must ensure that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access	This objective provides for the protection of the TOE from untrusted software and users. This objective provides for the physical protection of the TOE software.

		facilities, which will prevent unauthorized physical access.	

TABLE 4-6: ALL ASSUMPTIONS UPHELD

5 Extended Components Definition

All of the components defined below have been modelled on components from Part 2 of the CC Version 3.1. The extended components are denoted by adding "_EXT" in the component name.

Item	SFR ID	SFR Title
1	DDoS_DEF_EXT.1	DDoS Defence
2	DDoS_NOT_EXT.1	Security Notifications
3	FIA_UAU_EXT.2	User Authentication before any action

Table 5-1: Extended Components

5.1 DDoS_DEF_EXT.1 DDoS Defence

5.1.1 Class: DDoS: Distributed Denial of Service

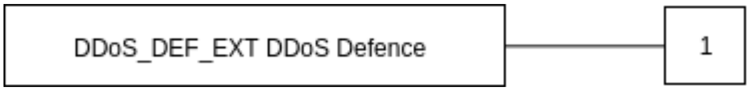
This class was explicitly created. The families in this class specify the functional requirements that pertain to the security features of a DDoS detection and mitigation product. While this SFR was modelled on existing FRU requirements in the CC Part 2, these requirements needed further modification to meet the specific needs of DDoS detection and mitigation implementation rather than intrusion detection.

5.1.2 Family: DDoS Defence (DDoS_DEF)

5.1.2.1 Family Behaviour

This family provides requirements for the TSF enforcement of detection and mitigation of DDoS attacks. The requirements of this family ensure that the TOE will protect networks against DDoS attacks.

5.1.2.2 Component levelling



DDoS_DEF_EXT.1 DDoS defence provides a mechanism to mitigate DDoS attacks. Component definition and rationale are provided in section 5.1.3 and 5.1.4.

5.1.2.3 Management

The following actions could be considered for the management functions in FMT:

- Management of TSF data.

5.1.2.4 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Detection and Actions taken due to detected potential attacks.

5.1.3 Definition

DDoS_DEF_EXT.1 DDoS Defence

- Hierarchical to: No other components
- Dependencies: No other components

DDoS_DEF_EXT.1.1 The TSF shall be able to detect the following types of DDoS attacks

- SYN Flood
- TCP Flood
- HTTP Flood
- ICMP Flood
- UDP Flood
- DNS Query Flood
- DNS Amplification Flood
- TCP Connection Flood

DDoS_DEF_EXT.1.2 The TSF shall be able to mitigate the detected DDoS attacks

DDoS_DEF_EXT.1.3 The TSF shall be provide the following additional information flow control capabilities

- Geo IP based filtering
- Custom Rules

5.1.4 Rationale

DDoS_DEF_EXT.1 had to be explicitly stated because the CC Part 2 does not have any DDoS mitigation related SFRs that can describe the functions of the TOE. DDoS_DEF is modelled as a Family of the standard class FRU (Resource Utilization) as it is the only class that deals with availability and prioritization of resources.

5.2 DDoS_NOT_EXT.1 Explicit: Security Notifications

5.2.1 Class: DDoS: Distributed Denial of Service

This class was explicitly created. The families in this class specify the functional requirements that pertain to the security features of a DDoS detection and mitigation product. While this SFR was modelled on existing IDS requirements that have been used in validated Protection Profiles, these requirements needed further modification to meet the specific needs of DDoS detection and mitigation implementation rather than intrusion detection.

5.2.2 Family: Security Notifications (DDoS_NOT)

5.2.2.1 Family Behaviour

This family defines the notifications generated by the TSF as a result of trigger events that happen while the TSF is detecting and mitigating DDoS attacks. This family also defines the destination(s) of the notifications that are generated. The scanners would generally collect static configuration information and send that onto an analytical component which would cause the notifications to be generated.

5.2.2.2 Component levelling

DDoS_NOT_EXT.1 Security notification provides a mechanism for detecting DDoS Attacks and Notify the users accordingly. Component definition and rationale are provided in section 5.2.3 and 5.2.4.

5.2.2.3 Management

The following actions could be considered for the management functions in FMT:

- Configuration of the notification destination by an administrator

5.2.2.4 Audit

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

- Basic: time notification generated, source and destination of notification, notification type

5.2.3 Definition

DDoS_NOT_EXT.1 Explicit: Security Notifications

Hierarchical to: No other components
Dependencies:

DDoS_DEF_EXT.1	DDoS Defence

DDoS_NOT_EXT.1.1

The TSF shall send a visual notification when events occur during the assessment.
The events generated from TOE components contains the following information:

- Created Date: The timestamp at which the event was created
- Created By: username for user generated events or system for system generated events
- Status: status of the event (ENDED/ ONGOING/ NULL)
- Category: category of the event
- Sub-category: refinement of category of the event.
- Direction: traffic flow for which the event was created (INBOUND/ OUTBOUND/ NULL).
- Message: message to be displayed to the user.

Visual notifications are available at:

- Web GUI: hdDeviceUI
- Email addresses of the registered users

List of Events (Categories):

- Attack events
- Alarm events
- System events

DDoS_NOT_EXT.1.2

The TSF shall send a notification when events occur during the assessment process.
Following are the notification types.

- Web based UI notification: list of events displayed in hdDeviceUI.
- Email notification: email sent to the registered users on event generation.

List of notification recipients:

- All registered users on hdDeviceUI

List of events/alert categories:

- System
- Configuration
- Attack
- Alarm
- User
- Report
- Operational
- Disk Usage

Further description of the alert categories can be referred from section 6.1.5.2.

5.2.4 Rationale

DDoS_NOT_EXT.1 is modelled on IDS_RCT.1 Analyser react (EXP) as defined in IDS System Protection Profile Version 1.7 July 25, 2007. This SFR was modified to apply to the various events that can be generated by any detection and mitigation type system rather than only the detection of an intrusion. This SFR uses the term "notification" rather than "alert" because there is no guarantee that the recipient will acknowledge or read the event information in a timely manner. For example, if the TOE sends this information via email (SMTP Server or native messaging within the product) there is no guarantee that the recipient will acknowledge or read the event information in a timely manner. Nor is the TOE expected to handle incoming responses such as an acknowledged receipt or read.

5.3 FIA_UAU_EXT.2 User authentication before any action

5.3.1 Class FIA: Identification and authentication

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017 Version 3.1 Revision 5.

5.3.2 Family: User authentication (FIA_UAU)

5.3.2.1 Family Behaviour

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

5.3.2.2 Component levelling

FIA_UAU_EXT Password-based Authentication Mechanism 2
2

FIA_UAU_EXT.2 The password-based authentication mechanism provides administrative users a locally based authentication mechanism. Component definition and rationale are provided in section 5.3.3 and 5.3.4. Refer to section 6.1.2 for list of user attributes, management of data and password policy.

5.3.2.3 Management

The following actions could be considered for the management functions in FMT:

- Management of the authentication data by an administrator
- Management of the authentication data by the user associated with this data

5.3.2.4 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- **Minimal:** Unsuccessful use of the authentication mechanism
- **Basic:** All use of the authentication mechanism

5.3.3 Definition

FIA_UAU_EXT.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1

Hierarchical to: FIA_UAU_EXT.2 User authentication before any action

The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

5.3.4 Rationale

FIA_UAU_EXT.2 is modelled closely on the standard component FIA_UAU.2: User authentication before any action. FIA_UAU_EXT.2 needed to be defined as an extended component because the standard component was broadened by adding the text “either by the TSF or by an authentication service in the Operational Environment invoked by the TSF”.

6 Security Requirements

This section provides the security functional and assurance requirements for the TOE.

6.1 Security Functional Requirements for the TOE

Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined as:

- **Iteration:** allows a component to be used more than once with varying operations
- **Assignment:** allows the specification of parameters
- **Selection:** allows the specification of one or more items from a list
- **Refinement:** allows the addition of details

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in ***[italicized bold text]****.*
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in <u>***italicized bold and underlined text***</u>.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *Extended components* defined in Section 5 have been denoted with the suffix "_EXT" following the family name.

The functional security requirements for the TOE consist of the following components taken directly from Part 2 of the CC and the extended components defined in Section 5 and summarized in Table 6-1 below.

Security Audit	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of Secrets
FIA_UAU.5	Multiple authentication mechanism
FIA_UAU_EXT.2	User authentication before any action
FIA_UID.2	User identification before any action
Security Management	
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialization
Security	
FPT_FLS.1	Failure with Preservation of Secure State
FPT_STM.1	Reliable Time Stamps
Distributed Denial of Service	
DDoS_DEF_EXT.1	DDoS Defence
DDoS_NOT_EXT.1	Security Notifications
Trusted Path/Channels	
FTP_ITC.1	Inter-TSF trusted Channel
FTP_TRP.1	Trusted Path/Channel
User Data Protection	
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
FDP_ITC.1	Import of User Data without Security Attributes
FDP_ITT.1	Transfer of User Data
Cryptographic Support	
FCS_COP.1a	Cryptographic operation
FCS_COP.1b	Cryptographic operation
FCS_COP.1c	Cryptographic operation

TABLE 6-1: FUNCTIONAL COMPONENTS

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.
Dependencies:

FPT_STM.1	Reliable time stamps

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the ***[not specified]*** level of audit; and
- ***[the following auditable events: events listed in column 3 of Table 6-2]***

SFR ID	SFR Title
FAU_GEN.1	None
FAU_GEN.2	None
FAU_SAR.1	None
FAU_SAR.3	None
FAU_STG.1	Disk usage is getting full.
FIA_ATD.1	None
FIA_SOS.1	None
FIA_UAU.5	None
FIA_UAU_EXT.2	User login and logout
FIA_UID.2	User login and logout
FMT_MTD.1	Configuration or updates to any of the TOE Settings
FMT_SMF.1	All Actions defined in FMT_MTD.1
FMT_SMR.1	None
FPT_FLS.1	Failure with Preservation of Secure State
FPT_STM.1	None
DDoS_NOT_EXT.1	Security Notifications
FTP_ITC.1	None
FTP_TRP.1	None

TABLE 6-2: FUNCTIONAL COMPONENTS

**Application Note: The TOE records DDoS events in a separate log file, Blocked Host Log, which is not part of the audit trail and is available to view via a different function in the Web GUI.*

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: ***[the additional information identified in Table 6-3]***.

Information	Description
Username	The user who made the change, or "system" if it is a system-generated change.
Sub-System	The sub-system that made the change. CLI, hdDeviceUI, hdDetectionService, hdInspector
Log Priority levels	There are four priority levels for logs-DEBUG, WARN, ERROR AND INFO.
Description	A description of the change. For example, if a protection group is created, the description displays the settings that are configured.

TABLE 6-3: AUDIT RECORD INFORMATION

Application Note: The "…outcome (success or failure) of the event" will only be included if applicable.

6.1.1.2 FAU_GEN.2 User Identity Association

Hierarchical to: No other components.
Dependencies:

FAU_GEN.1	Audit Data Generation
FIA_UID.1	Timing of identification

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

Hierarchical to: No other components.
Dependencies:

FAU_GEN.1	Audit Data Generation

FAU_SAR.1.1

The TSF shall provide ***[Administrators]*** with the capability to read ***[following audit data]*** from the audit records:

- CLI logs
- Syslog logs
- Haltdos logs

- Access logs
- website logs
- Detection Service logs

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.
Dependencies:

FAU_SAR.1	Audit Review

FAU_SAR.3.1

The TSF shall provide the ability to apply ***[searching]*** of audit data based on:

All possible combinations of the following fields:

- Username
- Timestamp
- Sub-system

6.1.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.
Dependencies:

FAU_GEN.1	Audit Data Generation

FAU_STG.1.1

The TSF shall protect the stored records from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to ***[prevent]***unauthorized modifications to the audit records in the audit trail.

6.1.2 Class FIA: Identification and authentication

6.1.2.1 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

- Username
- Email
- Password
- Access Rights (role)

6.1.2.2 FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet ***[the parameters of the TOE Password Policy (See Table 6-4)]***.

Password Criteria
must be at least 8 characters long
must be no more than 72 characters long
can include special characters, spaces, and quotation marks
cannot be all digits
must consist of at least one digit
must consist of at least one uppercase and one lowercase letter
cannot be only letters followed by only digits (for example, abcd123)
cannot be only digits followed by only letters (for example, 123abcd)
cannot consist of alternating letter-digit combinations (for example, 1a3A4c1 or a2B4c1d)

TABLE 6-4: TOE PASSWORD POLICY RULES

6.1.2.3 FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.5.1

The TSF shall provide ***[Local Password Authentication and ability to invoke external authentication mechanism when configured]*** to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the ***[Following rules]:***

- TOE invoke authentication mechanism in the following precedence order: RADIUS, LOCAL. If authentication from RADIUS succeeds = Login Success. If authentication from RADIUS fails, LOCAL authentication is invoked. If local authentication succeeds = Login Success. If the local authentication fails = Login Failure.

- If RADIUS server is not configured or down, LOCAL authentication is attempted. If LOCAL authentication fails: Login failure.

Application Note: The TOE only claims compatibility with RADIUS servers.

6.1.2.4 FIA_UAU_EXT.2 User Authentication Before any Action

Hierarchical to:

FIA_UAU.1	Timing of authentication

Dependencies:

FIA_UID.1	Timing of identification

FIA_UAU_EXT.2.1

TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.5 FIA_UID.1 Timing of Identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1
The TSF shall allow list of TSF-mediated actions on behalf of the user to be performed before the user is identified.

Following is the list of TSF-mediated actions:

- Forgot Password: user can request for resetting their passwords. An email validation link will be sent to the registered email addressed.
- I am a first time user: user can request for creating their passwords. An email validation link will be sent to the registered email addressed.

FIA_UID.1.2
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.6 FIA_UID.2 User Identification Before any Action

Hierarchical to:

FIA_ UID.1	Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1

The TSF shall require each user to be successfully identified before allowing any other TSF mediated actions on behalf of that user.

6.1.3 Class FMT: Security Management

6.1.3.1 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies:

FMT_SMR.1	Security roles
FMT_SMF.1	Specification of Management Functions

FMT_MTD.1.1
The TSF shall restrict the ability to ***[change default, query, modify, delete, and [other operations as specified in Table 6-5]*** the ***[TSF Data as specified in Table 6-5]*** to ***[the role as specified in Table 6-5].***

Operations	TSF Data or object	Role
Login to CLI (Access)	hdCLI	System Administrator**
Login to Web GUI (Access)	hdDeviceUI	Administrator, Security Analyst, Network Analyst, Visitor
Capture	the network packets in real time	Administrator, Security Analyst, Network Analyst
Change	the global protection level	Administrator, Security Analyst
Configure, Run, Restore	the backup and restore data	System Administrator
Edit	the user accounts attributes	Administrator, Security Analyst* , Network Analyst* , Visitor*
Edit	the IP interface configuration settings	System Administrator
Edit	the local user and authentication	Administrator
Edit	the authorization configuration settings	System Administrator, Administrator
Edit	the accounting AAA configuration settings	System Administrator
Edit	the DNS configuration settings	Administrator
Edit	the HTTP configuration settings	Administrator
Edit and View	the logging, configuration settings	Administrator
View	the server log	System Administrator
Edit	the NTP configuration settings	System Administrator
Edit	the SSH configuration settings	System Administrator
Edit	the system attributes	System Administrator
Edit and Apply	the IP access rules (Policy)	System Administrator, Administrator
Explore	historical blocked hosts log	System Administrator

Install and uninstall	software packages	Administrator, System Administrator
Edit	the TOE system files	System Administrator
Manage	the General Configuration Settings	Administrator
Manage	the In-line Active State Setting	Administrator
Manage	the notification configuration settings	Administrator, Security Analyst, Network Analyst
Manage	the system events configuration settings	Administrator, Security Analyst, Network Analyst
Manage	the SSH keys	System Administrator
Manage	the system disks	System Administrator
View	the TOE system files	System Administrator
Restore	Restore device state from backup	System Administrator
Set	the system clock	System Administrator
Show	the running or saved configuration settings	Administrator, Security Analyst, Network Analyst
Shutdown	the TOE system	System Administrator
Start and Stop	the TOE services	System Administrator
View	Access rights configuration settings	Administrator

TABLE 6-5: MANAGEMENT OF TSF DATA

*VISITOR can only edit own account attributes for updating password or username attributes. A VISITOR cannot change his own authority assignment or his registered email id.

*SECURITY ANALYST can only edit own account attributes for updating password or username attributes. A SECURITY ANALYST cannot change his own authority assignment or his registered email id.

*NETWORK ANALYST can only edit own account attributes for updating password or username attributes. A NETWORK ANALYST cannot change his own authority assignment or his registered email id.

**SYSTEM ADMINISTRATOR is LINUX OS users with root privileges on the TOE appliance. These users can log onto the appliance via SSH to run system commands and access the CLI to maintain and configure the TOE. Some CLI command makes API calls to GUI.

6.1.3.2 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:

- Operations as specified in Table 6-5 on the TSF Data as specified in Table 6-5 (See FMT_MTD.1)

6.1.3.3 FMT_SMR.1 Security Roles

Hierarchical to: No other components.
Dependencies:

FIA_UID.1	Timing of Identification

FMT_SMR.1.1

The TSF shall maintain the roles ***[ADMINISTRATOR, SECURITY ANALYST, NETWORK ANALYST, VISITOR AND SYSTEM ADMINISTRATOR]*.**

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.1.3.4 FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.
Dependencies:

FDP_IFC.1	Subset of Information Flow Control
FMT_SMR.1	Security Roles
FMT_SMF.1	Specification of Management

FMT_MSA.1.1

The TSF shall enforce the ***[Packet Filter SFP]*** to restrict the ability to ***[modify, [no other operations]]*** the security attributes ***[network traffic filter rules and configuration data] to [the role administrator]***.

6.1.3.5 FMT_MSA.3 Static Attribute Initialization

Hierarchical to: No other components.
Dependencies:

FMT_MSA.1	Management of Security Attributes
FMT_SMR.1	Security Roles

FMT_MSA.3.1

The TSF shall enforce the ***[Packet Filter SFP]*** to provide ***[restrictive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the ***[no roles]*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4 Class FPT: Protection of TSF

6.1.4.1 FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur:

- Power Failure
- Hardware Failure
- Software Failure

6.1.4.2 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1
The TSF shall be able to provide reliable time stamps for its own use.

6.1.5 Class DDoS: Distributed Denial of Service

6.1.5.1 DDoS_DEF_EXT.1 DDoS Defence

Hierarchical to: No other components.
Dependencies: No dependencies.

DDoS_DEF_EXT.1.1

The TSF shall be able to detect the following types of DDoS attacks

- Botnet
- Generic Bandwidth
- Slow HTTP
- Malformed HTTP

DDoS_DEF_EXT.1.2

The TSF shall be able to mitigate the detected DDoS attacks.

DDoS_DEF_EXT.1.3

The TSF shall provide the following additional information flow control capabilities

Capability to:

- Configure TOE to function in inline active (with filtering), off-line (only monitoring) or in-line bypass modes
- Configurable Detection Level (low, medium, high).

Note: See Section 8 for terminology and more details on inline active (with filtering), off-line (only monitoring) or in-line bypass modes Whitelist, Blacklist, Service Definitions and TCP SYN Rate Config etc.

For additional details on description of DDoS attack types and mitigation mechanisms, see Section 7.6.

6.1.5.2 DDoS_NOT_EXT.1 Explicit: Security Notifications

Hierarchical to: No other components.
Dependencies:

DDoS_DEF_EXT.1	DDoS Defence

DDoS_NOT_EXT.1.1

The TSF shall send a visual notification to [hdDeviceUI] when [the events) listed in Table 6-6] occurs during the assessment process.

DDoS_NOT_EXT.1.2

The TSF shall send a ***[email and log message]*** notification to ***[the assigned event notification recipient's EmailId, configured SNMP manager, configured syslog server]*** when ***[the Alert type(s) listed in Table 6-6]*** occurs during the assessment process.

Alert Type	Causes	UI Event	Log	Email
System	System settings are changed	Yes	Yes	No
Configuration	Someone changes the security settings.	Yes	Yes	No
Attack	DDoS attack detected	Yes	Yes	Yes
Alarm	User defined rules get triggered	Yes	Yes	Yes
User	User permissions, role or addition or removal of users	Yes	Yes	No
Report	System report is generated	Yes	Yes	Yes
Operational	License expiry or system failure notifications	Yes	Yes	Yes
Disk Usage	Disk usage running high	Yes	Yes	Yes

TABLE 6-6: SECURITY NOTIFICATIONS

6.1.6 Class FTP: Trusted Path/Channels

6.1.6.1 FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit ***[the TSF]*** to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for ***[authentication decision handling].***

6.1.6.2 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_TRP.1.1

The TSF shall provide a communication path between itself and ***[remote]*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***[modification and disclosure]*****.**

FTP_TRP.1.2

The TSF shall permit ***[remote users]*** to initiate communication via the trusted path.

FTP_TRP.1.3
The TSF shall require the use of the trusted path for ***[initial user authentication, [and all remote user actions]].***

6.1.7 Class FDP: User Data Protection

6.1.7.1 FDP_IFC.1 Subset Information Flow Control

Hierarchical to: No other components.
Dependencies:

FDP_IFF.1	Simple Security Attributes

FDP_IFC.1.1

The TSF shall enforce the ***[Packet Filter SFP]*** on ***[Subjects: users (external entities) that send and/or receive information through the TOE to one another; Information: data sent from one subject through the TOE to one another; Operation: pass the data].***

Application Note: The Packet Filter SFP is given in FDP_IFF. The subject definition in FDP_IFC.1.1 belongs to a former CC version. Thus the subjects are identical to the users defined in the external entities definition in chap. 3.3.

6.1.7.2 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components.
Dependencies:

FDP_IFC.1	Subset Information Flow Control
FMT_MSA.3	Static Attribute Initialization

FDP_IFF.1.1

The TSF shall enforce the ***[Packet Filter SFP]*** based on the following types of subject and information security attributes: ***[Subjects: users (external entities) that send and/or receive information through the TOE to one another; Subject security attributes: none; Information: data sent from one subject through the TOE to one another; Information security attributes: source address of subject, destination address of subject, transport layer protocol, interface on which the traffic arrives and departs, port, time]***.

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***[Subjects on a network connected to the TOE can cause information to flow through the TOE to a subject on another connected network only if all the information security attribute values are permitted by all information policy rules]***.

FDP_IFF.1.3

The TSF shall enforce the [reassembly of fragmented IP datagrams before inspection].

FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: ***[none]***.

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules:

- The TOE shall reject requests of access or services where the information arrives on a network interface and the source address of the requesting subject is found malicious according to configured policy rules on the TOE.

Application Note: The subject definition in FDP_IFF.1.1 belongs to a former CC version. Thus the subjects are identical to the users defined in the external entities definition in chap. 3.3.

6.1.7.3 FDP_ITC.1 Import of User Data without Security Attributes

Hierarchical to: No other components.
Dependencies:

FDP_IFC.1	Subset Information Flow Control
FMT_MSA.3	Static Attribute Initialization

FDP_ITC.1.1

The TSF shall enforce the ***[User Data SFP]*** when importing ***[Geo IP database, TOR IP feeds, IP Reputation and Software Updates]*** from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: ***[none]***.

6.1.7.4 FDP_ITT.1 Basic Internet Transfer Protection

Hierarchical to: No other components.
Dependencies:

FDP_IFC.1	Subset Information Flow Control

FDP_ITT.1.1

The TSF shall enforce the ***[User Data SFP]*** to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

6.1.8 Class FCS: Cryptographic Support

6.1.8.1 FCS_COP.1 Cryptographic Operation (a)

Hierarchical to: No other components.
Dependencies:

FDP_ITC.1	Import of User Data without Security Attributes

FCS_COP.1.1a

The TSF shall perform symmetric encryption and decryption in accordance with a specified cryptographic algorithm AES and cryptographic key sizes 256 bits that meet the following: **FIPS 197**.

6.1.8.2 FCS_COP.1 Cryptographic Operation (b)

Hierarchical to: No other components.
Dependencies:

FDP_ITC.1	Import of User Data without Security Attributes

FCS_COP.1.1b

The TSF shall perform asymmetric encryption and decryption in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes up to 2048 bits that meet the following: **PKCS#1 v2.1**.

6.1.8.3 FCS_COP.1 Cryptographic Operation (c)

Hierarchical to: No other components.
Dependencies:

FDP_ITC.1	Import of User Data without Security Attributes

FCS_COP.1.1c

The TSF shall perform cryptographic hashing in accordance with a specified cryptographic algorithm SHA1 and cryptographic key sizes not applicable that meet the following: **FIPS 180-3**

6.2 Security Assurance Requirements for the TOE

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2+ taken from Part 3 of the Common Criteria. None of the assurance components are refined, ALC_CMC.3 and ALC_CMS.3 are added instead of ALC_CMC.2 and ALC_CMS.2 for augmenting EAL 2. The assurance components are listed in Table 6-7.

Assurance Class	**Assurance components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target	ASE_CCL.1 Conformance claims

evaluation	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

TABLE 6-7: EAL2 ASSURANCE COMPONENTS

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6.2.1 ADV_ARC.1 Security Architecture Description

Developer action elements:

ADV_ARC.1.1D
The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.
ADV_ARC.1.2D
The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
ADV_ARC.1.3D
The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C
The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstraction described in the TOE design document.
ADV_ARC.1.2C
The security architecture description shall describe the security domain maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C
The security architecture description shall describe how the TSF initialization process is secure.
ADV_ARC.1.4C
The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5C
The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

6.2.2 ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_FSP.2.1D
The developer shall provide a functional specification.
ADV_FSP.2.2D
The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C
The functional specification shall completely represent the TSF.

ADV_FSP.2.2C
The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C
The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C
For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C
For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C
The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

6.2.3 ADV_TDS.1 Basic design

Developer action elements:

ADV_TDS.1.1D
The developer shall provide the design of the TOE.

ADV_TDS.1.2D
The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C
The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C
The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C
The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C
The design shall summarize the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.1.5C
The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C
The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

6.2.4 AGD_OPE.1 Operational user guidance

Developer action elements:

AGD_OPE.1.1D
The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C
The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C
The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C
The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C
The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C
The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C
The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C
The operational user guidance shall be clear and reasonable.

6.2.5 AGD_PRE.1 Preparative procedures

Developer action elements:

AGD_PRE.1.1D
The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C
The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C
The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

6.2.6 ALC_CMC.3 Authorisation controls

Developer action elements:

ALC_CMC.3.1D
The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D
The developer shall provide the CM documentation.

ALC_CMC.3.3D
The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.3.1C
The TOE shall be labelled with its unique reference.

ALC_CMC.3.2C
The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C
The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C
The CM system shall provide measures such that only authorised changes are made to the configuration items.

ALC_CMC.3.5C
The CM documentation shall include a CM plan.

ALC_CMC.3.6C
The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C
The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C
The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

6.2.7 ALC_CMS.3 Implementation representation CM coverage

Developer action elements:

ALC_CMS.3.1D
The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.3.1C
The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.

ALC_CMS.3.2C
The configuration list shall uniquely identify the configuration items.

ALC_CMS.3.3C
For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

6.2.8 ALC_DEL.1 Delivery procedures

Developer action elements:

ALC_DEL.1.1D
The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D
The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C
The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

6.2.10 ALC_DVS.1 Identification of security measures

Developer action elements:

ALC_DVS.1.1D
The developer shall produce and provide development security documentation.

Content and presentation elements:

ALC_DVS.1.1C
The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

6.2.11 ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_LCD.1.1D
The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D
The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C
The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C
The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

6.2.12 ASE_CCL.1 Conformance claims

Developer action elements:

ASE_CCL.1.1D
The developer shall provide a conformance claim.

ASE_CCL.1.2D
The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C
The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C
The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C
The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C
The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C
The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C
The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C
The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C
The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C
The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C
The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

6.2.13 ASE_ECD.1 Extended components definition

Developer action elements:

ASE_ECD.1.1D
The developer shall provide a statement of security requirements.

ASE_ECD.1.2D
The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C
The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C
The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C
The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C
The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C
The extended components shall consist of measurable and objective elements such that conformance or non-conformance to these elements can be demonstrated.

6.2.14 ASE_INT.1 ST introduction

Developer action elements:

ASE_INT.1.1D
The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C
The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C
The ST reference shall uniquely identify the ST.

ASE_INT.1.3C
The TOE reference shall identify the TOE.

ASE_INT.1.4C
The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C
The TOE overview shall identify the TOE type.

ASE_INT.1.6C
The TOE overview shall identify hardware/software/firmware required by the TOE.

ASE_INT.1.7C
The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C
The TOE description shall describe the logical scope of the TOE.

6.2.15 ASE_OBJ.2 Security objectives

Developer action elements:

ASE_OBJ.2.1D
The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D
The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C
The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C
The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C
The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C
The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C
The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C
The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

6.2.16 ASE_REQ.2 Derived security requirements

Developer action elements:

ASE_REQ.2.1D
The developer shall provide a statement of security requirements.

ASE_REQ.2.2D
The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C
The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C
All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C
The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C
All operations shall be performed correctly.

ASE_REQ.2.5C
Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C
The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C
The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C
The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C
The statement of security requirements shall be internally consistent.

6.2.17 ASE_SPD.1 Security problem definition

Developer action elements:

ASE_SPD.1.1D
The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C
The security problem definition shall describe the threats.

ASE_SPD.1.2C
All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C
The security problem definition shall describe the OSPs.

ASE_SPD.1.4C
The security problem definition shall describe the assumptions about the operational environment of the TOE.

6.2.18 ASE_TSS.1 TOE summary specification

Developer action elements:

ASE_TSS.1.1D
The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C
The TOE summary specification shall describe how the TOE meets each SFR.

6.2.19 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D
The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C
The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

6.2.20 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D
The developer shall test the TSF and document the results.

ATE_FUN.1.2D
The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C
The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C
The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C
The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C
The actual test results shall be consistent with the expected test results.

6.2.21 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D
The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C
The TOE shall be suitable for testing.

ATE_IND.2.2C
The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

6.2.22 AVA_VAN.2 Vulnerability analysis

Developer action elements:

AVA_VAN.2.1D
The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C
The TOE shall be suitable for testing.

6.3 Security Requirements Rationale

6.3.1 Assurance Rationale

EAL 2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and protected by other products designed to address threats that correspond with the intended environment.

Haltdos has chosen to augment EAL 2 by adding the assurance component ALC_CMC.3 and ALC_CMS.3, to assure that all the components of the TOE are under a secure and reliable process for the refinement and modification, this provides an assurance that the functional working of the components are not compromised during deployment / updating.

6.3.2 Dependencies Satisfaction Rationale

Table 6-8 shows the dependencies between the functional requirements including the extended components defined in Section 5.

SFR ID	SFR Title	Dependencies
Security Audit		
FAU_GEN.1	Audit data generation	FPT_STM.1
FAU_GEN.2	User identity association	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	Audit review	FAU_GEN.1
FAU_SAR.3	Selectable audit review	FAU_GEN.1
FAU_STG.1	Protected audit trail storage	FAU_SAR.1
Identification and Authentication		
FIA_ATD.1	User attribute definition	None
FIA_SOS.1	Verification of Secrets	None
FIA_UAU.5	Multiple authentication mechanism	None
FIA_UAU_EXT.2	User authentication before any action	FIA_UID.1
FIA_UID.2	User identification before any action	None
Security Management		
FMT_MTD.1	Management of TSF data	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	Specification of management functions	None
FMT_SMR.1	Security roles	FIA_UID.1
FMT_MSA.1	Management of Security Attributes	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	Static Attribute Initialization	FMT_MSA.1 FMT_SMR.1
Security		
FPT_FLS.1	Failure with Preservation of Secure State	None
FPT_STM.1	Reliable Time Stamps	None
Distributed Denial of Service		
DDoS_DEF_EXT.1	DDoS Defence	None
DDoS_NOT_EXT.1	Security Notifications	DDoS_DEF_EXT.1
Trusted Path/Channels		
FTP_ITC.1	Inter-TSF trusted Channel	None

FTP_TRP.1	Trusted Path/Channel	None
User Data Protection		
FDP_IFC.1	Subset Information Flow Control	FDP_IFF.1
FDP_IFF.1	Simple Security Attributes	FDP_IFC.1 FMT_MSA.3
FDP_ITC.1	Import of User Data without Security Attributes	FDP_IFC.1 FMT_MSA.3
FDP_ITT.1	Transfer of User Data	FDP_IFC.1
Cryptographic Support		
FCS_COP.1a	Cryptographic operation	FDP_ITC.1
FCS_COP.1b	Cryptographic operation	FDP_ITC.1
FCS_COP.1c	Cryptographic operation	FDP_ITC.1

Table 6-8: TOE Dependencies Satisfied

6.3.3 Functional Requirements vs Objectives Satisfaction Rationale

Table 6-9 traces each SFR back to the security objectives for the TOE demonstrating that ALL SFRs map to ALL security objectives for the TOE.

SFR ID	SFR Title	Objectives
Security Audit		
FAU_GEN.1	Audit data generation	O.AUDIT
FAU_GEN.2	User identity association	O.AUDIT
FAU_SAR.1	Audit review	O.AUDIT
FAU_SAR.3	Selectable audit review	O.AUDIT
FAU_STG.1	Protected audit trail storage	O.AUDIT
Identification and Authentication		
FIA_ATD.1	User attribute definition	O.IDAUTH
FIA_SOS.1	Verification of Secrets	O.IDAUTH
FIA_UAU.5	Multiple authentication mechanism	O.IDAUTH
FIA_UAU_EXT.2	User authentication before any action	O.IDAUTH
FIA_UID.2	User identification before any action	O.IDAUTH
Security Management		
FMT_MTD.1	Management of TSF data	O.MANAGE
FMT_SMF.1	Specification of management functions	O.MANAGE
FMT_SMR.1	Security roles	O.MANAGE
FMT_MSA.1	Management of Security Attributes	O.MANAGE
FMT_MSA.3	Static Attribute Initialization	O.DDoSMITIGATE
Security		
FPT_FLS.1	Failure with Preservation of Secure State	O.FAILSAFE
FPT_STM.1	Reliable Time Stamps	O.AUDIT
Distributed Denial of Service		
DDoS_DEF_EXT.1	DDoS Defence	O.DDoSMITIGATE
DDoS_NOT_EXT.1	Security Notifications	O.DDoSALERT

Trusted Path/Channels		
FTP_ITC.1	Inter-TSF trusted Channel	O.PROCOM O.IDAUTH
FTP_TRP.1	Trusted Path/Channel	O.PROCOM O.MANAGE
User Data Protection		
FDP_IFC.1	Subset Information Flow Control	O.DDoSMITIGATE
FDP_IFF.1	Simple Security Attributes	O.DDoSMITIGATE
FDP_ITC.1	Import of User Data without Security Attributes	O. MANAGE
FDP_ITT.1	Transfer of User Data	O.AUDIT
Cryptographic Support		
FCS_COP.1a	Cryptographic operation	O.PROCOM
FCS_COP.1b	Cryptographic operation	O.PROCOM
FCS_COP.1c	Cryptographic operation	O.PROCOM O.MANAGE

Table 6-9: Mapping of TOE SFRs to TOE Security Objectives

The Table 6-10 provides the rationale for how each objective is satisfied by the TOE.

Objective ID	SFR ID/Title	Rationale
O.AUDIT The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.	FAU_GEN.1	Audit records are generated for security-relevant events.
	FAU_GEN.2	The user/source is associated with the audit events is recorded.
	FAU_SAR.1	The TOE provides the ability to review and manage the audit trail of the system.
	FAU_SAR.3	The TOE is capable of providing searching capabilities of the audit records. The TOE is capable of providing selection capabilities for auditing to include or exclude auditable events from the set of audited events.
	FAU_STG.1	The TOE is able to protect audit records stored internally.
	FPT_STM.1	The TOE provides the timestamp required for the audit record. The TOE supports the setting of the time manually or configuring an external NTP server.
	FDP_ITT.1	The TOE validates unauthorized modification of user data such as Geo IP, TOR IP, IP Reputation feeds and software updates when it is downloaded from external environment.

O.DDoSALERT The TOE will provide the capability to alert administrators when DDoS attacks are detected and other customizable events, conditions, and system errors.	DDoS_NOT_EXT.1	The TOE is capable of generating notifications based upon administratively defined set of events, conditions, or system errors. The notifications can be sent via email or logging message.
O.DDoSMITIGATE The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDoS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDoS attacks, and authorized users who may overuse resources.	DDoS_DEF_EXT.1	The TOE protects Internet Protocol (IP) networks against DDoS attacks by successfully identifying and mitigating attacks via mechanisms such as filtering, Whitelists, Blacklists, TCP SYN rate monitoring, etc.
	FDP_IFC.1	The TOE protects the network by filtering out malicious DDoS attack packets thereby ensuring availability of network resources to legitimate users.
	FDP_IFF.1	The TOE protects the network from filtering out known malicious IP addresses, and packets that match configured policy on the TOE.
	FMT_MSA.3	The TOE allows legitimate users with sufficient privileges to update security policy on the TOE to adjust the type of traffic to be allowed / disallowed in and out of the network.
O.FAILSAFE The failure of the TOE must not interrupt the flow of traffic through the TOE between networks.	FPT_FLS.1	FPT_FLS.1 ensures that the TOE preserves a secure state when there is a hardware, software or power failure.
O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions.	FIA_ATD.1	User attributes required for identification and authentication are stored by the TOE.
	FIA_UAU.5	Provides for local authentication and the invocation of an external authentication mechanism (only claiming the ability to interface with RADIUS servers).
	FIA_UAU_EXT.2	All authorized users are successfully authenticated before allowing any management actions on behalf of that user.
	FIA_UID.2	All users are successfully identified before allowing any other TSF-mediated actions on behalf of that user.
	FIA_SOS.1	Provides the enforced password policy for native password authentication.

	FTP_ITC.1	Provides trusted communications to the external authentication mechanisms that can optionally be used to identify and authenticate the requesting user.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_MTD.1	The TOE allows for the appropriate management TSF data within each Security function.
	FMT_SMF.1	Ensures that the TOE security Function data may only be modified by an authorized user.
	FMT_SMR.1	This objective is met by supporting multiple management roles (ADMINISTRATOR, VISITOR, SECURITY ANALYST, NETWORK ANALYST and SYSTEM ADMINISTRATOR).
	FMT_MSA.1	The TOE provides a set of default security policy which can be configured only by authorized users of the TOE with sufficient privileges.
	FTP_TRP.1	Provides for the trusted path required for remote management of the TOE.
	FDP_ITC.1	The TOE periodically downloads updates (Geo IP, TOR IP, IP Reputation feeds & software updates) from trusted developer repository at update.haltdos.com. This periodic update allows the TOE to be up to date with latest malicious IPs and enables continuous protection against known attack sources.
	FCS_COP.1c	The TOE validates periodic updates (TOR IP, IP Reputation feeds & software updates) by validating its hash value to detect unauthorized modification during transit.
O.PROCOM The TOE will provide a secure session for communication between the TOE and the remote administrator's browser trying to access the hdDeviceUI or remote access to the CLI .	FTP_ITC.1	The TOE requires the establishment of an SSL/TLS connection from the TOE users' browser when connecting to hdUI over HTTPS.
	FTP_TRP.1	The TOE requires the establishment of an SSH connection in order to access the TOE remotely to use the CLI.
	FCS_COP.1a	The TOE requires the establishment of an SSL/TLS connection from the TOE users' browser when connecting to hdUI over

		HTTPS. HTTPS uses asymmetric & symmetric encryption for creating SSL tunnel.
	FCS_COP.1b	The TOE requires the establishment of an SSL/TLS connection from the TOE users' browser when connecting to hdUI over HTTPS. HTTPS uses asymmetric & symmetric encryption for creating SSL tunnel.
	FCS_COP.1c	The TOE validates periodic updates (Geo IP, TOR IP and IP Reputation feeds) by validating its hash value to detect unauthorized modification during transit.

TABLE 6-10: ALL TOE OBJECTIVES MET BY SECURITY FUNCTIONAL REQUIREMENTS

7 TOE Summary Specification

Section 7 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 1.4.9 Logical Scope of the TOE.

The following subsections describe how the TOE meets each SFR listed in Section 6.

Security Class	SFRs	Security Functions
Security audit	FAU_GEN.1	SA-1
	FAU_GEN.2	
	FAU_SAR.1	SA-2
	FAU_SAR.3	
	FAU_STG.1	SA-3
Protection of TSF	FPT_FLS.1	FPT-1
	FPT_STM.1	FPT-2
Identification and authentication	FIA_ATD.1	IA-1
	FIA_SOS.1	IA-2
	FIA_UAU.5	
	FIA_UAU_EXT.2	
	FIA_UID.2	
Security Management	FMT_MTD.1	SM-1
	FMT_MSA.3	
	FMT_MSA.1	
	FMT_SMF.1	SM-2
	FMT_SMR.1	SM-3
Trusted Communication	FTP_ITC.1	TC-1
	FCS_COP.1a	
	FCS_COP.1c	TC-2
	FDP_ITC.1	
	FDP_ITT.1	
	FCS_COP.1a	TC-3
	FTP_TRP.1	TC-4
	FCS_COP.1a	
	FCS_COP.1b	
Resource Utilization (DDoS Protection)	DDoS_DEF_EXT.1	DDoS-1 DDoS-2
	FDP_IFC.1	
	FDP_IFF.1	
	DDoS_NOT_EXT.1	DDoS-3

TABLE 7-1: SECURITY FUNCTIONAL REQUIREMENTS MAPPED TO SECURITY FUNCTIONS

7.1 Security Audit

7.1.1 SA-1: Audit Generation

The TOE's audit trail equates to the TOE audit logs and syslog (2 different files with overlap) which is stored on the appliance.

Audit records are generated within the TOE by the TSF for the events listed in FAU_GEN.1. Audit records contain a timestamp, the information of the entity triggering the event (username or system), the event (e.g. Configuration changes, CLI command usage, Deployment mode changes), and a summary of the event as well as the additional information listed in Table 6-2 and Table listed in Section Table 6-3.

7.1.2 SA-2: Audit Review

An authorized SYSTEM ADMINISTRATOR user can read all the logs (audit data) generated. The Web GUI ADMINISTRATOR user can also view events on the event page with the ability to search on various information is provided.

Following is the list of filters that can be applied on the Web GUI(hdDeviceUI) for viewing the events on the events page (in Web GUI events cannot be filtered based on sub-systems defined in section 6.1.1.1):

Information	**Description**
Username	The user who made the change, or "system" if it is a system-generated change.
Created After	The date after which the change has happened
Created before	The date before which change was made
Event type	Type of the event
Search box	Allows user to search on data from any column on the page except the date.

TABLE 7-2: AUDIT SEARCH FIELDS

The TOE displays search results in chronological order with the most recent event displayed first. Audit logs in the appliance are available in /var/log/haltdos/ folder. The sub-systems defined in section 6.1.1.1 generate their respective logs with the assigned name and timestamp in the folder /var/log/haltdos. These logs can be viewed and filtered by using standard UNIX commands such as grep / tail / less.

Sub-System	**Command**
hdCLI	less /var/log/haltdos/website.<yyyy-MM-dd>.log
hdDeviceUI	less /var/log/haltdos/website.<yyyy-MM-dd>.log
hdDetectionService	less /var/log/haltdos/detection.<yyyy-MM-dd>.log
hdInspector	less /var/log/haltdos/haltdos.log

TABLE 7-3: SUB-SYSTEM LOGS

7.1.3 SA-3: Audit Protection

The TSF protects the stored audit records on the TOE from unauthorized deletion and modifications via the TSFIs. The Audit data resides on the TOE Platform and can only be accessed using the Web GUI or if the user is a SYSTEM ADMINISTRATOR on the TOE appliance. The Web GUI does not provide an option for users to delete or modify the change Log (aka audit log) but allows users to search and view logs only.

The TOE does automatically delete oldest audit data log file (syslog and change log) when the maximum number of rotated syslog files to be retained is met (i.e. max limit is set to 5 then on 6th rollover the oldest rotated file is deleted. The max limit is configurable via Web GUI to a max limit of 6 months. It is highly recommended that the TOE be configured to use an external ftp server to continually off load the audit for long term storage. The TOE supports the manual exporting of the syslog files via the CLI / service logging remote *<IP address>.*

The TOE also supports the manual exporting of the syslog files via remote access. The TOE does not allow for the modification or deletion of any of the TOE's audit data (Change Log or syslog) via the CLI commands or the Web GUI.

7.2 Protection of TSF

7.2.1 FPT-1: Failure with preservation of secure state

Secure State for this product is defined as the state when the TOE Platform provides uninterrupted access to resources on the Internal Network to intended users. The failure of the TOE must not make the resources unavailable.

The flow of network traffic is not interfered with, monitored, or filtered, during the boot cycle as the TOE is in bypass mode. The TOE must initialize successfully in order for the TOE to be placed out of bypass mode for operational use.

The appliance running the TOE must be bypass capable. If power failures, hardware failures, or software issues affect the TOE during operational use, the TOE is placed in bypass mode and the network traffic is passed through the appliance unaffected thus preventing resources being made unavailable.

In the case of a power supply failure, the redundant power architecture (if configured) will take over and maintain safe operation. In case of complete power supply failure, the TOE passes traffic without any monitoring or filtering in an uninterrupted manner.

7.2.2 FPT-2: Reliable Time Stamps

An administrator can set or reset the clock in appliance running the TOE by remotely accessing it using SSH.

An administrator can optionally configure the appliance running the TOE to use an NTP server using the SSH. The TOE can provide its own timestamp through a system call to the supporting operating system which is part of the appliance. It is highly recommended that the enterprise network being protected have its time synchronized with a NTP server. The TOE supports the use of an NTP server to update the system's time clock.

7.3 Identification and Authentication

7.3.1 IA-1: User Attributes

The TSF maintains the following security attributes for each individual TOE user for use with local password authentication only:

- Username
- Password
- Authority
- Email

7.3.2 IA-2: User I&A

The TSF requires each user to self-identify before being allowed to perform any other actions. The TSF requires an administrator to be successfully authenticated with a password before being allowed any other management actions. Authentication is handled via local password protection or the TOE invokes an external authentication mechanism (RADIUS) for the authentication decision. The TOE tries each method according to the following precedence order: RADIUS (if configured), LOCAL. Below is a table of scenarios to help in understanding the authentication enforcement described above.

The top left corner sets the scenario. The Method Status is indicating whether any external authentication mechanisms are Available (operational and network reachable) or are NOT available (not reachable on network). The precedence order set shows the order in which authentication method may be called. The Final Outcome / Method row shows the final decision the TOE would enforce and which authentication server was the final decision maker.

Method Status: Available **Precedence Order Set: R, L**		**Scenario 1**		**Scenario 2**		**Scenario 3**	
1	RADIUS	Success	Stops	Failure	Next	Failure	Next
2	LOCAL			Success	Stops	Failure	Stops
	Overall Outcome / Method	**Success**	**RADIUS**	**Success**	**LOCAL**	**Failure**	**LOCAL**
Method Status: NOT Available **Precedence Order Set: R, L**		**Scenario 1**		**Scenario 2**		**Scenario 3**	
1	RADIUS	Network Error		Network Error		N/A	
2	LOCAL	Success	Stops	Failure	Stops		
	Overall Outcome / Method	**Success**	**LOCAL**	**Failure**	**LOCAL**		

TABLE 7-4: AUTHENTICATION SCENARIO EXAMPLES

TOE Password Policy

Local passwords have a software enforced password policy. The password policy is within the user manual. The requirements are:

- must be at least 8 characters long
- must be no more than 72 characters long
- can include special characters, spaces, and quotation marks
- cannot be all digits
- must consist of at least one uppercase and one lowercase letter
- Must consist of at least one digit
- cannot be only letters followed by only digits (for example, abcd123)
- cannot be only digits followed by only letters (for example, 123abcd)
- cannot consist of alternating letter-digit combinations (for example, 1a3A4c1 or a2B4c1d) Additionally information:

WARNING: Default username and password

For accessing the CLI for the very first time, one must use the default username and password. The default username is **haltdos**. The default password is **H@ltd0s#1**. It is imperative for security purposes that this password be changed after the first-time logging into the system.

7.4 Security Management

7.4.1 SM-1: Management of TSF Data

The allowed operations on TSF Data and the administrative roles required to execute them are defined in Table 6-5: Management of TSF Data (See Section 6.1.3.1 FMT_MTD.1 Management of TSF data).

7.4.2 SM-2: Specification of Management Functions

The TOE is capable of performing the security management functions as defined in Table 6-5: Management of TSF Data of Section 6.1.3.1 FMT_MTD.1 Management of TSF data. The functions defined for FMT_SMF are exactly the same as the functions defined in the FMT_MTD requirement.

All management functions and access rights are limited by role-based management as defined in Section 7.4.3 SM-3: Security Roles below.

When accessing the management functions via the Web GUI:

A successfully authenticated user can navigate menus and pages by using typical navigational controls. The Web GUI menu bar indicates which menu is active or inactive and only allows the user to access those menus based on the privileges inherited from the user's assigned group.

The menu bar is divided into the following menus: Home, Events, Dashboard, Action, Alarms, Web Analytics and Settings (details of which were given in the introduction section). An ADMINISTRATOR has access to all the web menus. A VISITOR only has access to the Administration menu functions that allow the user to change his/her own password and email address. A user without logging won't have access to any of the menus and is pushed back to the login page.

The functions defined in the FMT_MTD.1 Table 6-5 are divided amongst the 7 web menus (predominantly in the Administration) and are either submenus (provide further division) or pages that display the actual data such as list of users or a page of a particular user's attributes.

Additionally, there are some administrative functions that can only be handled by using CLIs. Typically, the CLI is used for installing and upgrading the software and completing the initial configuration. However, there are additional advanced functions that can only be configured using the CLI.

7.4.3 SM-3: Security Roles

The TOE supports the following 4 user authorities (roles):

- **ADMINISTRATOR:** Users in this group have full read and write access on all pages of the Web GUI. One having ADMINISTRATOR rights can add other users.
- **VISITOR:** Users in this group have read-only access to most of the Web GUI pages and can edit and update their own user account settings. Users in this group cannot change any settings.
- **NETWORK ANALYST:** Users in this group have read and write access to all the network settings of the TOE. They have read and write access to Alarm settings, Dashboards, and Website analytics.
- **SECURITY ANALYST:** Users in this group have read and write access to all the security settings of the TOE. They have read and write access to Alarm settings, Dashboards and Action settings.
- **SYSTEM ADMINISTRATOR:** this is a Linux root user for appliance running the TOE. This user cannot login to the hdDeviceUI since the user is not registered with hdDeviceUI in the database.

The TOE runs on Linux OS platform and therefore also supports Linux OS users. Linux OS users with administrative privileges have access to run CLI commands to manage and configure the TOE. This document refers administrative Linux OS users as SYSTEM ADMINISTRATOR

See Section 6.1.3.1 FMT_MTD.1 Management of TSF data table for details on the specific function available to each role.

7.5 Trusted Communications

7.5.1 TC-1: Trusted Channel for Authentication

Communication between the TOE and RADIUS Server require that the entire data payload of the packet is encrypted, leaving only the standard RADIUS header in clear text and encrypts the user's password between the TOE and RADIUS Server.

7.5.2 TC-2: Trusted Channel for IP Reputation, Tor IP & Software Updates

During an IP Reputation and Tor IP Updates, HaltDos Web Service uses HTTPS (Port 443) to download the latest IP Reputation and Tor IP lists threat feed by communication with HaltDos Update Repository at updates.haltdos.com. The hash of each downloaded file is validated to ensure that the files have not been modified during transit. By default, this update run automatically every 24 hours.

7.5.3 TC-3: Trusted Path for CLI Access

The TOE also requires the establishment of an SSH connection in order to access the TOE remotely to use the CLI. The remote platform connects to the TOE using the standard SSH-2 protocol through OpenSSH version 7.2 which provides confidentiality and integrity of data over an insecure network. The remote user's host platform must therefore be on a network where it can access TCP Port 22, or a custom configured port such as 8022. The crypto cipher suites supported by OpenSSH are default crypto suites in the OpenSSH utility and can be customized as necessary.

7.5.4 TC-4: Trusted Path for hdDeviceUI

The TOE also requires the establishment of a HTTPS connection in order to access the TOE from management interface on a web browser. hdDeviceUI runs on the Tomcat server which listens on TCP port 8443. Communication between the user (browser) and the TOE happens over encrypted path over SSL protocol.

7.6 Resource Utilization (DDoS Protection)

7.6.1 DDoS-1: DDoS Detect

BOTNET attacks

A DDoS botnet is a large set of compromised computers that are controlled remotely by a server. The controlling server is known as a CnC (command-and-control) server. Usually, the computers in a botnet, which are known as bots, become compromised without their users' knowledge. The bots are infected with malware that enables them to generate a high-volume traffic attack that targets a victim server. Victim servers can include Web, DNS, and SMTP servers.

The bots can use a variety of protocols, including HTTP, IRC, and other proprietary protocols, to communicate with the CnC server and other bots. For example, a bot can send information about itself, receive attack commands from the CnC server, or share "hello" messages between itself and other bots.

Depending on the botnet family, the messages themselves can be in plain text or encoded. The botnet family also determines the type of attacks that are supported. These attacks can include one or more of the following types of floods: HTTP, UDP, TCP, and ICMP. When the bots receive commands from the CnC server, such as the attack method and target IP addresses, they collectively engage in DDoS attacks against the specified targets.

Some botnets are available for hire, whereby an individual can purchase the services of a botnet for a specific period. The service allows the individual to choose one or more target servers for the entire botnet to attack.

A voluntary botnet is one in which users allow their computers to become part of the botnet with the intention of attacking a victim server. When a computer becomes a member of the botnet, it accepts commands from the CnC server; for example, the attack method and target IP address. The bot joins the rest of the botnet to flood the victim server with traffic.

Some of the tools that attackers use contains a feature whereby users can allow their computers to become part of a botnet.

To prevent botnet attacks, the TOE performs the following tests:

- **Basic Botnet Prevention filtering:**
  When enabled, the TOE checks the packet headers for incomplete fields, known as malformed packets. In case of HTTP traffic, the HTTP headers can also be incomplete. The TOE blocks packets that are malformed (not conforming to RFC) packets. For certain types of malformed or incomplete packets, the TOE temporarily blocks the source host if the configured thresholds are breached.

- **Botnet Signatures filtering**
  When enabled, the TOE uses the IP reputation and TOR IP Feed to detect DDoS botnet attacks, voluntary botnet attacks and attacks from malicious IP addresses. It is essential to keep the IP reputation and TORIP feeds updated in order to mitigate and detect emerging DDoS attacks.

  The TOE also implement feature of traffic shaping. The TOE analyses all the traffic assign them suspicion score based on their various fields like source port, destination port and other and based on the suspicion score relevant actions are taken.

- **Prevent Slow Request Attacks filtering**
  During a slow HTTP attack, the attacker makes several connections and, on each connection, sends a partial request for data to the victim server. In response, the server allocates resources such as memory to each connection and waits for subsequent requests to arrive. The attacker sends a very small portion of the request at a rate almost equal to, but less than, the server's timeout setting. Therefore, the server stays busy processing the small requests but it takes a long time to time out. Eventually, the server starts to deny legitimate connection requests from other clients.

For example, if the server's timeout period is 300 seconds, the attacker sends 5 bytes of a 500 byte request every 299 seconds (just before the server times out). The attack occupies the server's resources on that connection for 29,900 seconds (299 * 500/5).

When enabled, the TOE checks for HTTP requests that contain less than configurable TCP payload fields (in bytes). The TOE blocks those requests that breach this limit and temporarily blocks the source host of any requests that match these criteria because they are likely to be part of a slow HTTP attack.

The Prevention of Slow Request Attacks is enhanced when it works in conjunction with the aggressive aging settings which tracks established TCP connections and blocks the traffic when a connection remains idle for too long. Traffic is also blocked when the bit rate for a single request drops below a configured minimum with minimum TCP payload setting.

- **Generic Bandwidth Flood Attacks**

HTTP flood is a continuous submission of the same HTTP request or a set of HTTP request messages to a victim Web server's resources. Typically, the attacker sends the requests at a high rate and forces the Web server to respond to each request. As a result, the Web server remains busy and denies service to legitimate requests.

Floods can originate from malware or from an attack tool that uses underlying operating system facilities to connect to the victim, create HTTP requests, and perform the attack. Some attack methods can provide flexibility in creating a traffic pattern (for example, randomized payloads), while others can provide better performance in terms of speed. The method that the attacker uses to construct the requests determines the nature of the attack, which in turn affects how the DDoS traffic is mitigated.

Many of the protection settings help to prevent this type of attack. Examples of these settings are as follows:

- The ICMP Flood Detection settings detect ICMP (ping) flood attacks.
- The Rate-based Blocking settings protect against floods by enforcing traffic thresholds.
- The Connection Proxy settings and the TCP SYN Flood Detection settings detect certain connection flood attacks.

7.6.2 DDoS-2 Additional Filter Control

The TOE monitors the network traffic and mitigates attacks by using the configurational settings configured by user and detection profiles.

Detection profile helps user to configure different sensitivity levels for different protocols and their respective triggers helping the TOE to identify various flood attacks.

The TOE can be put into 3 different modes In-line active(with filtering), In-line bypass(In-line without filtering) and off-line. The **In-line active mode** is a state within the in-line deployment mode, in which The TOE monitors traffic, detects and mitigates DDoS attacks. The In-line bypass mode is a state within the in-line deployment mode, in which the TOE monitors traffic and detects DDoS attack but does not mitigate (filter) them. The **off-line mode** is a deployment mode, in which the TOE analyses traffic without forwarding it and only detects DDoS attacks.

Key points for the traffic filtering:

a) The TOE support ALL protocol on Ethernet - they either get forwarded or dropped.
b) Product inspects for DDoS in the following: TCP, UDP, ICMP and DNS.
c) Packets inspected must be IPv4.
d) ARP are always forwarded.
e) All other traffic can be dropped or forwarded based on configuration.
f) There is no filtering from the LAN to the WAN network traffic.

The following table describes the filter types, settings, and DDoS classification that the filter supports.

Settings List	**Setting: Description**
Blacklist Countries	**Country box:** Type the name or select one or multiple Countries whose IP is to be blacklist. In the Blacklisted Countries selection list, the countries are listed alphabetically.
Blacklist	In the **Blacklisted Prefix box**, an administrator can type a IP prefix or multiple source IP prefixes. All the traffic with this source IP or Destination IP will be dropped. Allowed Prefixes are 8 – 32 Ex.- 192.168.1.0/24
Whitelist	In the **Whitelist Hosts box**, an administrator can type an IP prefix or multiple source IP prefixes. All the traffic with this source IP or Destination IP will be bypasses directly to server without passing through rest of the mitigations even if it was blacklisted. Allowed Prefix are 24 – 32 Ex.- 192.168.1.3/25
Online IP Reputation Feed	**NO ACTION: -**Disable Checking for Malicious IPs. **ADD SUSPICION: -**Add Suspicion to traffic whose source IP is present in the IP Reputation feed. **DROP:-** Drop the traffic whose source IP is present in the IP Reputation feed.
Blacklist Tors IP	**Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. If Enabled all the traffic whose source IP is present in the tor IP feed will be dropped.
Minimum TCP Payload Length	**Payload Length box:** Type the minimum TCP payload length to be allowed. To disable this setting, put value as 0. **Consecutive Threshold box**:- If the Minimum payload length is breached consecutive times for the specified threshold then the source will be temporarily suspended.
Minimum HTTP incomplete header length	**Minimum incomplete header length box:** Set the minimum incomplete http header length of the incoming TCP Packet, below which the connection will be dropped. To disable this setting, enter the value 0.

NX domain per source	**Threshold box:** Set the maximum number of NXDomain DNS queries per source IP to be allowed. To disable this setting, put value as 0. **Duration box**:- If the above threshold is breached for a source within the specified duration then the source will be temporarily suspended
DNS Query Lock Down	**Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. If Enabled only valid queries will be allowed and rest will be dropped.
Max concurrent connections	**Value box:** Sets the maximum concurrent TCP connections, protected application servers can handle.
Concurrent connections per source	**Value box:** Limits the maximum number of simultaneous TCP connections any source IP can establish with protected application servers when not under attack. Set 0 to disable mitigation.
Concurrent connections per source (under attack)	**Value box:** Limits the maximum number of simultaneous TCP connections any source IP can establish with protected application servers when under attack. Set 0 to disable mitigation.
Aggressive Aging	**Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. If Enabled stale connections older than **Connection Expiry Duration** will be terminated.
Connection expiry duration	**Value box:** Time after which the TCP connection will be considered stale and will be scheduled for deletion. Disable **Aggressive Aging** to disable this mitigation.
Connection proxy	**Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. If Enabled provides protection against TCP Flood attacks such as TCP SYN Flood, etc.
Connection proxy trigger threshold	**Value box:** If **Connection Proxy** is enabled, specify the number of active connections after which the proxy will be enabled for all subsequent connection requests. Disable **Connection Proxy** to disable this mitigation or set its value as 0.
HTTP requests per source	**Value box:** Set the number of HTTP requests per second per source to be allowed. If any source exceeds this threshold, then that source is temporarily suspended. Set 0 to disable mitigation.
Progressive challenge threshold	**Value box:** Set the number of HTTP requests per second per source to be allowed before the progressive challenge is sent. If the challenge is not successful then source is suspended. Set 0 to disable mitigation.
HTTP flood protection	**Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. If Enabled it turns on protection against HTTP Floods.
HTTP request limit by URL	**Value Box:** Enter the number of HTTP requests per particular URL to be allowed per second. A HTTP request is any type of request such as GET, POST, HEAD, or OPTIONS. To disable this setting, disable HTTP Flood Protection
Default HTTP requests per second	**Method:** Select a method out of GET, POST, PUT, DELETE, or HEAD for which you want to enable HTTP Flood Protection **Host:** Enter the HTTP Host for which you want to enable HTTP Flood Protection

	URL: Enter the specific URL to enable the HTTP Flood Protection for it **Threshold:** Enter the threshold which if breached by a source for the specified URL, Host and Method will be temporarily suspended.
Traffic Shaping Overall Limits	**Maximum Inbound bps box (in mbps):** Type the maximum amount of inbound traffic (in mbps) to allow **Maximum Outbound bps box(in mbps):** Type the maximum amount of outbound traffic (in mbps) to allow
Traffic Shaping TCP Limits	**Maximum TCP Inbound bps box (in mbps):** Type the maximum amount of inbound TCP traffic (in mbps) to allow Set 0 to disable this mitigation **Maximum TCP Outbound bps box (in mbps):** Type the maximum amount of outbound TCP traffic (in mbps) to allow Set 0 to disable this mitigation
Traffic Shaping UDP Limits	**Maximum UDP Inbound bps box(in mbps):** Type the maximum amount of inbound UDP traffic (in mbps) to allow Set 0 to disable this mitigation **Maximum UDP Outbound bps box (in mbps):** Type the maximum amount of outbound UDP traffic (in mbps) to allow Set 0 to disable this mitigation
Traffic Shaping ICMP Limits	**Maximum ICMP Inbound bps box (in mbps):** Type the maximum amount of inbound ICMP traffic (in mbps) to allow Set 0 to disable this mitigation **Maximum ICMP Outbound bps box (in mbps):** Type the maximum amount of outbound ICMP traffic (in mbps) to allow Set 0 to disable this mitigation
Traffic Shaping DNS Limits	**Maximum DNS Inbound bps box (in mbps):** Type the maximum amount of inbound DNS traffic (in mbps) to allow Set 0 to disable this mitigation **Maximum DNS Outbound bps box (in mbps):** Type the maximum amount of outbound DNS traffic (in mbps) to allow Set 0 to disable this mitigation

Table 7-5: Available protection settings for each standard server type

7.6.3 DDoS-3 Notification

When the TOE detects events, attacks, change in configuration, adding a user or editing a user access, trigger of alarms in the system, it creates alerts to inform the user. The TOE can be configured to send notification messages to specific destinations to communicate certain alerts.

The alert type specifies the event category that can trigger a specific notification. An administrator can associate each notification destination with one or more of these alert types.

Alert Type	***Causes***
System	Hardware or system component events and other events that affect the system's health. For example, change in configuration, adding a new user, generation of report, editing a user access
Attack	Alerts are generated if the TOE detects any attack
Alarm	Alerts are generated if user created alarms are triggered

TABLE 7-6: ALERT TYPES

The TOE supports following types of notifications:

- Email: The TOE sends email notifications to the users with the authorized access decided by the administrator. The notifications appear to come from the sender address that is specified.
- Notification Alerts: User also get a notification alert in its profile page in WEB GUI

The TOE also visually displays the alert event on 2 different locations in the Web GUI. The first visual alert is on the Events page. The Events page displays all the events allowing user to filter among those events according to its need.

8 Glossary of Terms

a

AAA (Authentication, Authorization, & Accounting) — An acronym that describes the process of authorizing access to a system, authenticating the identity of users, and logging their behaviours.
active mode — A state within the in-line deployment mode, in which the TOE mitigates attacks in addition to monitoring traffic and detecting attacks. **address** — A coded representation that uniquely identifies a particular network identity.
alert — A message informing the user that certain events, conditions, or errors in the system have occurred.
anomaly — An event or condition in the network that is identified as an abnormality when compared to a predefined illegal traffic pattern.
API (Application Programming Interface) — A well-defined set of function calls providing high-level controls for underlying services.
ASCII (American Standard Code for Information Interchange) — A coded representation for standard alphabetic, numeric, and punctuation characters, also referred to as "plain text".
authentication — An identity verification process.

b

blacklist — A list of hosts and destinations block — To prevent traffic from passing to the network, or to prevent a host from sending traffic.
bot — A program that runs run automated tasks over the Internet.
botnet — A set of compromised computers (bots) that respond to a controlling server to generate attack traffic against a victim server.
bps — Bits per second.
bypass mode —A state in which the TOE just detects and analyse the traffic and not mitigate it.

c

CA (Certificate Authority) — A third party that issues digital certificates for use by other parties. CAs are characteristic of many public key infrastructure (PKI) schemes.
CDN (Content Delivery Network) — A collection of Web servers that contain duplicated content and are distributed across multiple locations to deliver content to users based on proximity.
CIDR (Classless Inter-Domain Routing) — Method for classifying and grouping Internet addresses.
CLI (command line interface) — A user interface that uses a command line, such as a terminal or console (as opposed to a graphical user interface).
client — The component of client/server computing that uses a service offered by a server.
cloud — A metaphor for the Internet.
CSV (comma-separated values) file — A file that stores spreadsheet or database information in plain text, with one record on each line, and each field within the record separated by a comma.
customer edge — The location at the customer premises of the router that connects to the provider edge of one or more service provider networks. **customer edge router** — A router within a customer's network that is connected to an ISP's customer peering edge.

d

Dark IP — Regions of the IP address space that are reserved or known to be unused.
data center — A centralized facility that houses computer systems and associated components, such as telecommunications and storage systems, and is used for processing or transmitting data.
DDoS (Distributed Denial of Service) — An interruption of network availability typically caused by many, distributed malicious sources.
Deployment mode — Indicates how the TOE is installed in the network: in-line or off-line through a span port or network tap (monitor).
DNS (Domain Name System) — A system that translates numeric IP addresses into meaningful, human consumable names and vice-versa.
DNS server — A server that uses the Domain Name System (DNS) to translate or resolve human-readable domain names and hostnames into the machine-readable IP addresses.
DoS (Denial of Service) — An interruption of network availability typically caused by malicious sources.

e

edge — The outer perimeter of a network.
encryption — The process by which plain text is scrambled in such a way as to hide its content.
Ethernet — A series of technologies used for communication on local area networks.
exploit — Tools intended to take advantage of security holes or inherent flaws in the design of network applications, devices, or infrastructures.

f

failover — A configuration of two devices so that if one device fails, the second device takes over the duties of the first, ensuring continued service.
FCAP — A fingerprint expression language that describes and matches traffic information.
Fibre Channel — Gigabit-speed network technology primarily used for storage networking.
fingerprint — A pattern or profile of traffic that suggests or represents an attack. Also known as a signature.
firewall — A security measures that monitors and controls the types of packets allowed in and out of a network, based on a set of configured rules and filters.
FQDN (Fully Qualified Domain Name) — A complete domain name, including both the registered domain name and any preceding node information.
FTP (File Transfer Protocol) — A TCP/IP protocol for transferring files across a network.

g

Gb — Gigabit.
GB — Gigabyte.
Gbps — Gigabits per second.
global protection level — Determines which protection settings are in use for the entire system.
GMT (Greenwich Mean Time) — A world time standard that is deprecated and replaced by UTC.
GRE (Generic Routing Encapsulation) — A protocol that is used to transport packets from one network through another network.

GREtunnel — A logical interface whose endpoints are the tunnel source address and tunnel destination address.

h

handshake — The process or action that establishes communication between two telecommunications devices.
header — The data that appears at the beginning of a packet to provide information about the file or the transmission.
heartbeat — A periodic signal generated by hardware or software to indicate that it is still running.
host — A networked computer (client or server); in contrast to a router or switch.
HTTP (HyperText Transfer Protocol) — A protocol used to transfer or convey information on the World Wide Web.
Its original purpose was to provide a way to publish and retrieve HTML pages.
HTTPS (HyperText Transfer Protocol over SSL) — The combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) transport mechanism.

i

ICMP (Internet Control Message Protocol) — An IP protocol that delivers error and control messages between TCP/IP enabled network devices, for example, ping packets.
IMAP (Internet Message Access Protocol) — An application layer Internet protocol that allows a local client to access email on a remote server. (Also known as Internet Mail Access Protocol, Interactive Mail Access Protocol, and Interim Mail Access Protocol.)
interface — An interconnection between routers,switches, or hosts.
IP (Internet Protocol) — A connectionless network layer protocol used for packet delivery between hosts and devices on a TCP/IP network.
IP address — A unique identifier for a host or device on a TCP/IP network.
IPS (Intrusion Prevention System) — A computer security device that exercises access control to protect computers from exploitation.
ISP (Internet Service Provider) — A business or organization that provides to consumers access to the Internet and related services.

l

LAN (Local Area Network) — A typically small network that is confined to a small geographic space.

k

Kbps — Kilobits per second.

m

malformed — Refers to requests or packets that do not conform to the RFC standards for Internet protocol. Such requests or packets are often used in DDoS attacks.
Mbps — Megabits per second.
MBps — Megabytes per second.

MIB (Management Information Base) — A database used by the SNMP protocol to manage devices in a network.
mitigation — The process of using recommendations to apply policies to the network to reduce the effects of an attack.
monitor mode — A deployment mode in which the TOE is deployed out-of-line through a span port or network tap. the TOE monitors traffic and detects attacks but does not mitigate the attacks.
MSSP (Managed Security Service Provider) — An Internet service provider (ISP) that provides an organization with network security management, **multicast** — Protocols that address multiple IP addresses with a single packet (as opposed to unicast and broadcast protocols).

n

netmask — A dotted quad notation number that routers use to determine which part of the address is the network address and which part is the host address.
network tap — A hardware device that sends a copy of network traffic to another attached device for passive monitoring.
NIC (Network Interface Card) — A hardware component that maintains a network interface connection. notification — An email message, SNMP trap, or syslog message that is sent to specified destinations to communicate certain alerts.
NXDomain — A response that results when DNS is unable to resolve a domain name.
NTP (Network Time Protocol) — A protocol that synchronizes clock times in a network of computers.

o

off-line mode — A state within the in-line deployment mode, in which the TOE analyses traffic and detects attacks without performing mitigations. **In-line mode** — A deployment mode in which the TOE acts as a physical connection between two endpoints.
All of the traffic that traverses the network flows through the TOE.
out-of-band — Communication signals that occur outside of the channels that are normally used for data.

p

packet — A unit of data transmitted across the network that includes control information along with actual content.
password — A secret code used to gain access to a computer system.
payload — The data in a packet that follows the TCP and UDP header data.
PCAP (packet capture) file — A file that consists of data packets that have been sent over a network.
pps — Packets per second.
ping — An ICMP request to determine if a host is responsive.
policy — The set of rules that network operators determine to be acceptable or unacceptable for their network.
POP (Post Office Protocol) — A TCP/IP email protocol for retrieving messages from a remote server.
PoP (Point of Presence) — A physical connection between telecommunications networks.
port — A field in TCP and UDP packet headers that corresponds to an application level service (for example TCP port 80 corresponds to HTTP).
prefix — The initial part of a network address, which is used in address delegation and routing.
protection category — A group of related protection settings that detect a specific type of attack traffic.

protection group — A collection of one or more protected hosts that are associated with a specific type of server.
protection level — Defines the strength of protection against a network attack and the associated intrusiveness and risk of blocking legitimate traffic. The protection level can be set globally or for specific protection groups.
protection mode — A state within the in-line deployment mode, in which the mitigations are either in-live active or off-line.
protocol — A well-defined language used by networking entities to communicate with one another.

r

radius — Remote Authentication Dial-In User Service is a client/**server** protocol and software that enables remote access **servers** to communicate with a central **server** to authenticate dial-in users and authorize their access to the requested system or service.
rate limit — The number of requests, packets, bits, or other measurement of data that a host is allowed to send within a specified amount of time.
RDN (Registered Domain Name) — A domain name as registered, without any preceding node information
real time — When systems respond or data is supplied as events happen.
redundancy — The duplication of devices, services, or connections so that, in the event of a failure, the duplicate item can perform the work of the item that failed. **refinement** — The process of continually gathering information about anomalous activity that is observed on a network.
regular expression — A standard set of rules for matching a specified pattern in text. Often abbreviated as regex or regexp.
report — An informational page that presents data about a traffic type or event.
route — A path that a packet takes through a network.
router — A device that connects one network to another. Packets are forwarded from one router to another until they reach their ultimate destination.

s

secret key — A secret that is shared only between a sender and receiver of data.
server type — A class of servers that the TOE protects and that is associated with one or more protection groups.
SIP (Standard Initiation Protocol) — An IP network protocol that is used for VoIP (Voice Over IP) telephony.
signature — A pattern or profile of traffic that suggests or represents an attack. Also known as a fingerprint.
SMTP (Simple Mail Transfer Protocol) — The de facto standard protocol for email transmissions across the Internet.
SNMP (Simple Network Management Protocol) — A standard protocol that allows routers and other network devices to export information about their routing tables and other state information.
span port — A designated port on a network switch onto which traffic from other ports is mirrored.
spoofing — A situation in which one person or program successfully masquerades as another by falsifying data (usually an IP address) and thereby gains an illegitimate advantage.
SSH (Secure Shell) — A command line interface and protocol for securely accessing a remote computer. SSH is also known as Secure Socket Shell.
SSL (Secure Sockets Layer) — A protocol for secure communications on the Internet for such things as Web browsing, email, instant messaging, and other data transfers.
SSL certificate — A file that is installed on a secure Web server to identify a Web site and verify that the Web site is secure and reliable.
syslog — A file that records certain events or all of the events that occur in a particular system. Also, a service for logging data.

t

target — A victim host or network of a malicious denial of service (DoS) attack.
TCP (Transmission Control Protocol) — A connection-based, transport protocol that provides reliable delivery of packets across the Internet.
TCP/IP — A suite of protocols that controls the delivery of messages across the Internet.
throughput — The data transfer rate of a network or device.
TLS (Transport Layer Security) — An encryption protocol for the secure transmission of data over the Internet. TLS is based on, and has succeeded, SSL.

u

UDP (User Datagram Protocol) — An unreliable, connectionless, communication protocol.
unblock — To remove a source or destination from the temporarily blocked list without adding it to the whitelist.
UNC (Universal Naming Convention) — A standard which originated from UNIX for identifying servers, printers, and other resources in a network.
URI (Uniform Resource Identifier) — A protocol, login, host, port, path, etc. in a standard format used to reference a network resource, (for example http://haltdos.com).
URL (Uniform Resource Locator) — Usually a synonym for URI.
UTC (Universal Time Coordinated) — The time zone at zero degrees' longitude, which replaces GMT as the world time standard.

v

VLAN (Virtual Local Area Network) — Hosts connected in an infrastructure that simulates a local area network, when the hosts are remotely located, or to segment a physical local network into smaller, virtual pieces.
VoIP (Voice over Internet Protocol) — Routing voice communications (such as phone calls) through an IP network.
volumetric attack — A type of DDoS attack that is generally high bandwidth and that originates from a large number of geographically distributed bots.
VPN (Virtual Private Network) — A private communications network that is often used within a company, or by several companies or organizations, to communicate confidentially over a public network using encrypted tunnels.
vulnerability — A security weakness that could potentially be exploited.

w

WAN (Wide Area Network) — A computer network that covers a broad area. (Also Wireless Area Network, meaning a wireless network.)
Web UI (User Interface) — A Web-based interface for using an HaltDos Networks product.
whitelist — A list of hosts whose traffic is passed without further inspection. To add a host to the whitelist.

widget — A graphical element in a user interface that displays information about an application and allows the user to interact with the application.

X

XML (eXtensibleMarkup Language) — A metalanguage written in Standard Generalized Markup Language (SGML) that allows one to design a markup language for easy interchange of documents on the World Wide Web.