DNSVault Security Target

Common Criteria: EAL2

Document version: 1.0

Document date: 31-JAN-2017

Document management

Document identification

Document title	DNSVault Security Target
Document version	1.0
Document date	31-JAN-2017
Author	BAE Systems Applied Intelligence

Table of Contents

1 Security Target introduction (ASE_INT.1)

1.1 ST reference

ST Title	DNSVault Security Target
ST Version	1.0
ST Date	31-JAN-2017

1.2 TOE reference

TOE Title	DNSVault
TOE Version	Version 4.8

1.3 Document organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 Defined terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronyms used in this documentation.

Table 1 – Defined terms

Term	Description
ACL	Access Control Lists are address match list that the client can set up and nickname for future use in allow-query-on, allow recursion, allow recursion-on, black hole and allow transfer.
CPU	Central Processing Unit
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol is a standardised network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
DNSSEC	Domain Name System Security Extension is a suite of Internet Engineering Task Force (IETF) specification for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extension to DNS data, authentication denial of existence and data integrity but not availability.
FreeBSD	FreeBSD is a free Unix-like operating system descended from Research Unix via the Berkeley Software Distribution (BSD).
DNS Record	A DNS (Domain Name Server) record (also known as a zone file) is a small set of instructions for resolving specified Internet domain names to the appropriate number form of an Internet Protocol address (an IP address). A DNS record is basically a list of directions for where to send the web user.
RRL	Response Rate Limiting (RRL) is an enhancement to implementations of the DNS protocol that can help mitigate DNS amplification attacks.
RPZ	Response Policy Zones (RPZ) is mechanism for use by Domain Name System recursive resolvers to allow customised handling of the resolution of collections of domain name information (zones).
SSH	Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

Term	Description
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TSIG	TSIG (Transaction SIGnature) is a computer networking protocol defined in RFC 2845.
Unauthorised user	Unauthorised user can mean a legitimate user with access rights to certain web resource, an external entity that has no rights to any protected resource or data.
Users	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, users of the TOE access the TOE through a web browser.
User data	Data created by and for the user, which does not affect the operation of the TSF.
Normal User	A user who is granted access to the TOE web console and can perform a predefined set of tasks that could be modified by the Administrator.

1.5 TOE overview

1.5.1 TOE usage and major security functions

The Target of Evaluation is DNSVault version 4.8, which will hereafter be referred to as the 'TOE' or 'DNSVault' throughout this document. The TOE is a DNS management system; installed in DNSVault Series of appliances (e.g. 2000, 5000 and 10000 series) and has the capability to view, manage and secure DNS services. With the built-in network protection and built-in Load Balancing, the TOE provides advanced DNS management features with an intuitive web console on a high availability platform with real-time disaster recovery capabilities. This allows IT departments to truly provide DNS services in almost zero downtime. Alternatively, the TOE can be used as a tool for managing DNSSEC services on existing DNS network while protecting core DNS services from security threats and service failures.

Below are the main features of the TOE:

a) DNSVault Web console

The TOE provides a web console interface that enables users to manage the DNS easily rather than using command line, which can reduce human error.

b) DNSVault DNS View Support

The TOE provides a DNS view support that enables users to configure single domain with different address record and it can be configured to respond to different network subnet. It can be manage via the web console.

c) DNSVault Simple Load Balancing Features

The TOE provides a simple High availability and Load Balancing features in one package. The high availability feature transparently keeps all DNS service always running if one of the DNS servers is down. The high availability features does not only cover the IP level but also works on the service level where it will monitor DNS service and if the DNS service is down in one server, it will automatically transfer all DNS queries to the other DNS server. Furthermore, the high availability features can also be configured as active-active, where it will load balance all traffic across the virtual IP. This feature provides a simple and easy solution to distribute DNS query across DNSVault nodes.

d) DNSVault Network Protection

i. Built-in Firewall – The TOE is fully equipped with a state of the art mini firewall. The TOE firewall module works flawlessly standalone to provide access control list for DNS services, HTTP/HTTPS Web console and SSH CLI remote management. Each service can be configure to allow from all, deny from all or access list based rules. This firewall will protect and secure DNSVault from unintended access from hackers or persons with bad intentions. The firewall can also be configured to allow a specific service to run on certain network subnet. This will further thwart unprivileged access to the DNSVault Management console.

ii. V-Shield – V-shield is a protection technology that marries an intrusion detection system with an intrusion prevention system which can intelligently identify malicious and strange activities for all service that the TOE provides and quickly block access from the source address. V-shield works perfectly to protect the TOE from strange DNS queries, http/https password brute force and SSH password brute force. Furthermore, it has an option to block the source address for a certain period of time and release it again or to add it to a whitelist so that it will not get blocked again if the source address is a false positive.

iii. DNS Rate Limit – The TOE also support DNS rate limiting security functions which can significantly control and nullify DNS amplification attacks. The RRL can be configured to minimise DNS response when a client does a repeated DNS query to the appliance. The RRL configurations are fully compliance with standard BIND RRL configurations.

e) DNSVault SNMP implementation

The TOE supports Simple Network Management Protocol (SNMP). It can be configured to use SNMPv1, SNMPv2, and SNMPv3. The SNMP configurations can be setup using the web console. The SNMP user can view all system status, including CPU resource use, memory use, storage use for each partition, system load, networking information, and other information that will be listed below using the Object Identifiers (OID). For DNS statistics, all information will be group under the SNMP Table. The DNS statistics information included in the SNMP are incoming query type statistics, outgoing query type statistics, name server status statistics, and some network statistics that are used by the DNS service. SNMP traps can be configured with conditional threshold to be sent to the SNMP trap server.

f) DNSVault Centralized Management

The TOE features an advance Centralize Nodes Management where each nodes status and configuration can be managed on a single dashboard. All DNSVault appliance nodes status can be viewed on the Centralize Node Management Server. DNSVault Centralized Management dashboard will show all the important status information such as system uptime, memory utilization, CPU utilization, HDD utilization, IP address list and total DNS statistics for each DNSVault appliance in the network.

g) DNSSEC

The TOE support DNSSEC which has the capabilities to protect applications (and caching resolvers serving those applications) from using forged or manipulated DNS data, such as those created by DNS cache poisoning. All answers from DNSSEC protected zones are digitally signed. By checking the digital signature, a DNS resolver is able to check if the information is identical (i.e. unmodified and complete) to the information published by the zone owner and served on an authoritative DNS server.

h) Response Policy Zone (RPZ)

Response Policy Zone (RPZ) can be used to protect a user from accessing malicious websites. By providing simple DNS RPZ management via the web console, DNSVault further improves protection against online threats that depend on DNS technology by proactively protecting a user from getting infected and at the same time, disabling and preventing an infected client from connecting to the Botnet Command Center.

The following table highlights the range of security functions implemented by the TOE.

Table 2 – TOE Security Function

Security function	Description
Security audit	The TOE generates audit records for security events. The Administrator is the only role with access to the audit trail and has the ability to view all user activities such as the date and time of the event, type of event, subject identity and outcome of the event.
Identification and authentication	The TOE requires that each user is successfully identified (user ID) and authenticated (password) before any interaction with protected resources is permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to management functions based on the role of the user.
TSF Protection	The TOE includes its own time source for providing reliable time stamps that are used in audit records, DNSSEC operation and TSIG operation. The TOE also protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 5 minutes, it will automatically route users to the login page.
Secure Communication	The TOE is able to protect user data from disclosure and modification using SSL as a secure communication between a user's browser and the TOE.

1.5.2 TOE type

The TOE is a DNS management system designed to view, manage and secure DNS services. The TOE provides security functionality such as Security Audit, Identification and Authentication, Security Management, TSF Protection and Secure Communication. The TOE can be categorised as a ***Network and Network-Related Devices and Systems*** in accordance with the categories identified on the Common Criteria Portal (http://www.commoncriteriaportal.org) that lists all the certified products.

1.5.3 Supporting hardware, software and/or firmware

The underlying hardware and software that is used to support the TOE are:

Table 3 – Supporting Hardware and Software

Minimum System Requirements	
Appliances	
Hardware	**DNSVault 2000 Series** - Designed to serve small to medium enterprise and regional branch, office application. DNS Queries per second: 2,000. **DNSVault 5000 Series** - Designed to serve medium to large enterprises and regional branch, office applications. DNS Queries per second: 5,000.

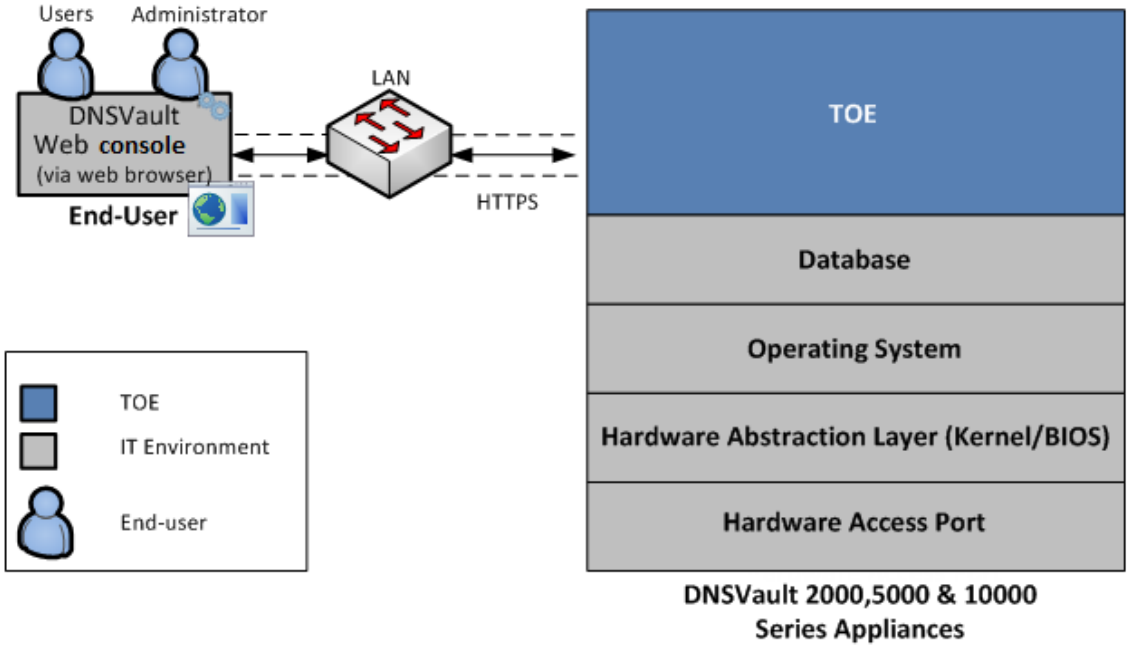
Minimum System Requirements	
Appliances	
	DNSVault 10000 Series - Designed to serve medium to large enterprises and regional branch, office applications. DNS Queries per second: 10,000.
End User	
Web Browser	Internet Explorer 11 Firefox 30 Chrome 35

1.6 TOE description

1.6.1 Physical scope of the TOE

A typical installation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

Figure 1 - Physical Scope of the TOE



Below are the descriptions of the components stated in Figure 1 above.

Table 4 – Components of the TOE architecture

Component	Description
TOE	The TOE is DNSVault version 4.8.

Component	Description
Operating System	DNSVault utilises FreeBSD as the operating system. FreeBSD is a free Unix-like operating system descended from Research Unix via the Berkeley Software Distribution (BSD). FreeBSD has several unique features such as NanoBSD, ZFS, and Geli.
Database	The database for these appliances is MySQL. MySQL is used for adding, accessing and managing content.
Hardware Abstraction Layer (Kernel/BIOS)	Kernel Customised kernel to meet appliance requirement. BIOS Type • 32Mb SPI Flash EEPROM with AMI BIOS BIOS Features • DMI 2.3 • PCI 2.3 • ACPI 2.0 • USB Keyboard support • SMBIOS 2.3 These components are applicable to all series of DNS Vaults.
Hardware Access Port	Ports • 2x Front USB ports • 2x Back USB ports • 1 x Serial COM port(general-purpose interface) • 4 x network port (include console port) • IPMI port • VGA port These hardware access ports are applicable to all series of DNS Vaults. However, it can also be modified depending on client's requests.

1.6.2 Logical scope of the TOE

The logical boundary of the TOE is summarized below.

a) **Security Audit.** The TOE generates audit records for security events. The Administrator is the only role with access to the audit trail and has the ability to view all user activities such as the date and time of the event, type of event, subject identity and outcome of the event.

b) **Identification & Authentication.** All users are required to be identified and authenticated before any information flows are permitted. The TOE checks the credentials presented by the user at the login page against the authentication information stored in the database.

c) **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access

them. The Administrator has the privileged to control access to the network. The functions above are restricted based on this role.

d) **TSF Protection.** The TOE includes its own time source for providing reliable time stamps that are used in audit records, DNSSEC operation and TSIG operation. The TOE also protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 5 minutes, it will automatically route users to the login page.

e) **Secure Communication.** The TOE provides a secure SSL channel between the end-user and the TOE.

2 Conformance Claim (ASE_CCL.1)

The ST and TOE are conformant to version 3.1 (REV 4) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 4), September 2012

- **Part 3 conformant, EAL2.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 4), September 2012. Evaluation is EAL2.

3 Security problem definition (ASE_SPD.1)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate;

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate; and

c) any relevant ***organisational security policy*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Identifier	Threat statement
T.EAVESDROP	An unauthorised person may eavesdrop on the communication between the end user and the appliance.
T.MANAGEMENT	An unauthorised user modifies management data that they are not authorised to access, resulting in loss of integrity of the data that the TOE uses to enforce the security functions.
T.UNAUTHORISED_ACCESS	An unauthorised user could gain unauthorised access to the TOE data by bypassing the identification and authentication requirements.

3.3 Organisational security policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

Identifier	Assumption statement
A.ADMIN	It is assumed that the person who manages the TOE is not hostile and is competent.
A.ENVIRONMENT	The TOE will provide appropriate authentication and authorisation controls for all users.

Identifier	Assumption statement
A.PASSWORD	It is assumed that users will keep their passwords secret and not write them down or disclose them to any other system or user. It is also assumed that the user's password length is between a minimum of 8 and a maximum of 18 alphanumeric characters.
A.PATCH	It is assumed that the TOE is patched and hardened to protect against known vulnerabilities and security configuration issues.
A.PHYSICAL	It is assumed that the TOE is in a secure operating facility with restricted physical access.
A.SSL_CONFIG	It is assumed that the web console has valid SSL certificates installed (not revoked or expired) and are sourced from a trusted entity.

4 Security objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security objectives for the TOE

Identifier	Objective statements
O.ACCESS	The TOE must ensure that only authorised users are able to access protected resources or functions.
O.COMM	The TOE must ensure that user data traversing across the network to the appliance is protected from disclosure and loss of integrity.
O.MANAGE	The TOE must allow an administrator to effectively manage the TOE, while ensuring that appropriate controls are maintained over those functions.
O.USER	The TOE must ensure that all users are identified and authenticated before accessing protected resources or functions.

4.3 Security objectives for the environment

Identifier	Objective statements
OE.ADMIN	The owners of the TOE must ensure that the administrator who manages the TOE is not hostile and is competent.
OE.AUTHDATA	The users of the TOE must not disclose their password that protects the TSF data.
OE.ENVIRONMENT	Those responsible for the TOE must ensure that there are appropriate authentication and authorisation controls for all users.
OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is in a secure operating facility with restricted physical access.
OE.PATCH	Those responsible for the TOE must ensure that the TOE is patched and hardened to protect against known vulnerabilities and security configuration issues.

Identifier	Objective statements
OE.SSL_CONFIG	Those responsible for the TOE must ensure that the web console has valid SSL certificates installed (not revoked or expired) and are sourced from a trusted entity.

4.4 Security objectives rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

Table 5 – Objective to assumptions/threats mapping

OBJECTIVES / THREATS/ ASSUMPTIONS	T.EAVESDROP	T.MANAGEMENT	T.UNAUTHORISED_ACCESS	A.ADMIN	A.ENVIRONMENT	A.PASSWORD	A.PATCH	A.PHYSICAL	A.SSL_CONFIG
O.ACCESS		✔	✔						
O.COMM	✔								
O.MANAGE		✔							
O.USER		✔	✔						
OE. ADMIN				✔					
OE.AUTHDATA						✔			
OE. ENVIRONMENT					✔				
OE. PATCH							✔		
OE. PHYSICAL								✔	
OE.SSL_CONFIG									✔

4.4.1 TOE security objectives rationale

The following table demonstrates that all security objectives for the TOE are traced back to the threats in the security problem definition.

Table 6 – Tracing of objectives to threats

Threats/OSPs	Objectives	Rationale
T.EAVESDROP	O.COMM	This objective ensures that all user data transferred from the user to the web console will be secured using HTTPS, protecting the user data from unauthorised disclosure and loss of integrity.
T.MANAGEMENT	O.USER	This objective ensures that the TOE identifies and authenticates all users before they access protected resources or functions.
	O.MANAGE	This objective ensures that the TOE provides the tools necessary for the authorised Administrator to manage the security-related functions and that those tools are usable only by users with appropriate authorisations.
	O.ACCESS	This objective ensures that the TOE restricts access to the TOE objects to authorised users
T.UNAUTHORISED_ACCESS	O.ACCESS	This objective ensures that the TOE restricts access to the TOE objects to the authorised users.
	O.USER	This objective ensures that the TOE identifies and authenticates all users before they access protected resources or functions.

4.4.2 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment are traced back to assumptions or OSPs in the security problem definition.

Table 7 – Environment security objective rationale

Assumptions	Objective	Rationale
A.ADMIN	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
A.ENVIRONMENT	OE.ENVIRONMENT	This objective ensures that those responsible for the TOE ensure appropriate authentication and authorisation controls are enforced for all users.

Assumptions	Objective	Rationale
A.PASSWORD	OE.AUTHDATA	This objective ensures that those responsible for the TOE ensure that the user will know the password but not disclose it to anyone else.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that those responsible for the TOE ensure that the operating system and database hosting the TOE is in a secure operating facility with restricted physical access.
A.PATCH	OE.PATCH	This objective ensures that those responsible for the TOE ensure that the TOE is patched and hardened to protect against known vulnerabilities and security configuration issues.
A.SSL_CONFIG	OE.SSL_CONFIG	This objective ensures that those responsible for the TOE ensure that the web console has SSL certificates installed are valid (not revoked or expired) and are sourced from a trusted entity.

5 Security requirements (ASE_REQ.2)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 4) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text for **additions** and strike-through for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Security functional requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Table 8 – List of SFRs

Identifier	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FDP_ACC.1	Subset access control

Identifier	Title
FDP_ACF.1	Security attribute based access control
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1a	Management of TSF data (Settings)
FMT_MTD.1b	Management of TSF data (Password)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps
FTA_SSL.3	TSF-initiated termination
FTP_TRP.1	Trusted path

5.2.2 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: ~~a) Start-up and shutdown of the audit functions;~~ b) All auditable events for the **[*not specified*]** level of audit; and c) **[the following auditable events:]** • **User and Administrator login** • **User and Administrator logout** • **Data modification by User and Administrator**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[none].**
Dependencies:	FPT_STM.1 Reliable time stamps

Note:	None

5.2.3 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide **[Administrator]** with the capability to **read [all audit information]** from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Note:	None

5.2.4 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the **[Access Control SFP]** on **[object listed in the table below]**.

Table 9 – Access Control List

Subject	Object	Operation
User **(user defined role)**	**View**	**Create/Update/Delete Host**
Administrator	**Full access control to all modules**	**All functions assigned to administrator:** • **Appliance Management module:** ○ **View Hardware Info** ○ **View Audit Info** ○ **View/Edit Settings for Network, SNMP, Time (NTP), SMTP, Reporting and Time Zone** ○ **Add/Edit/Delete individual and group email** ○ **View System Information** ○ **Create/Edit/Delete User Account** ○ **Modify settings for Account policy**

			○ **Add/Edit/Revoke Nodes** ○ **Edit Firewall settings** ○ **Edit V-Shield settings** ○ **Edit Rate Limit settings** ○ **Perform software updates** ○ **Perform Backup/Restore operation** ○ **Perform maintenance** ○ **Perform hardware shutdown/reboot** • **DNS Management module** ○ **Access and perform Domain operation** ○ **Create/Delete Access Control List** ○ **Create/Delete Geo locations List** • **Reports module** ○ **View Graph Statistics** ○ **View Contents**

Dependencies:	FDP_ACF.1 – Security attribute based access control
Notes:	None.

5.2.5 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the **[access control SFP]** to objects based on the following: **[as listed in Table 5].**
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[as listed in Table 5]**.
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[as listed in Table 5]**.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.2.6 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.7 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
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.
Dependencies:	No dependencies.
Notes:	None.

5.2.8 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the **[Access Control SFP]** to restrict the ability to **[*modify, delete*]** the security attributes **[that assign user Ids to roles to only the users that are mapped]** to **[administrator role]**.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.9 FMT_MSA.3 Static attribute initialization

Hierarchical to:	No other components

FMT_MSA.3.1	The TSF shall enforce the **[Access Control 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 **[administrator role]** to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.2.10 FMT_MTD.1a Management of TSF data (Settings)

Hierarchical to:	No other components
FMT_MTD.1a.1	The TSF shall restrict the ability to **[*modify, delete, [*Create, update, assign*]*]** the **[Access Control Lists in table 5, mapping of users to user group, user ID]** to **[Administrator]**.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.11 FMT_MTD.1b Management of TSF data (Password)

Hierarchical to:	No other components
FMT_MTD.1b.1	The TSF shall restrict the ability to **[*change_default, modify, [*Update*]*]** the **[User Password]** to **[Users and Administrator]**.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.12 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[** **a) mapping user IDs to group** **b) creation of users with default passwords** **c) reset password**

	d) deletion of users/group **e) changing of passwords** **f) management of Access Control lists stated in Table 5** **g) report generation]**.
Dependencies:	No dependencies.
Notes:	None.

5.2.13 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles **[users and administrator]**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None

5.2.14 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.
Notes:	None

5.2.15 FTA_SSL.3 TSF-initiated termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_STM.1.1	The TSF shall terminate an interactive session after a **[5 minutes period of inactivity]**.
Notes:	The minimum period of inactivity can be modified by the Administrator

5.2.16 FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
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, 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 authentication*]**.
Dependencies:	No dependencies
Notes:	None.

5.3 TOE Security assurance requirements

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and a basic description of the architecture of the TOE to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to attackers with basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Table 10 – Security assurance requirements

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_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures

Assurance class	Assurance components
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	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_IND.2 Independent testing – sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4 Security requirements rationale

5.4.1 Dependency rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL2, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

Table 11 – SFR Dependencies

SFR	Dependency	Inclusion
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3

SFR	Dependency	Inclusion
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FPT_STM.1	No dependencies	N/A
FTA_SSL.3	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A

5.4.2 Mapping of SFRs to security objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.ACCESS	FDP_ACC.1	This requirement helps meet the objective by identifying the objects and users subjected to the access control policy.
	FDP_ACF.1	This requirement meets the objective by ensuring the TOE only allows access to objects based on the defined access control policy.
	FAU_GEN.1	The TOE allows specifies auditing requirements for the TOE.

Security objective	Mapped SFRs	Rationale
	FAU_SAR.1	The TOE ensures audit information can be read by the authorised users.
	FPT_STM.1	This requirement helps meet the objective by providing reliable time stamps.
	FTA_SSL.3	This requirement helps meet the objective by terminating an interactive session after a 5 minutes period of inactivity.
	FMT_MSA.3	This requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP.
O.USER	FIA_UID.2	This requirement helps meet the objective by identifying the users before any TSF mediated actions.
	FIA_UAU.2	This requirement helps meet the objective by authenticating the users before any TSF mediated actions.
	FMT_SMR.1	The TOE maintains the Administrator and manages multiple user roles.
O.MANAGE	FMT_MSA.1	The TOE allows the Administrator to determine who has access to the folder and the folder's contents, and what actions the user can perform.
	FMT_MTD.1a	This requirements helps meet the objective by allowing only the Administrator role to create, delete, modify access control lists, and mapping users to roles and user accounts to the respective organisation database.
	FMT_MTD.1b	This requirement helps meet the objective by allowing users of all roles to change their passwords.
	FMT_SMF.1	The TOE allows the mapping of user to roles, creation of users, deletion of users, changing of passwords and management of ACLs.
	FMT_SMR.1	The TOE maintains the Administrator and manages multiple user roles.
O.COMM	FTP_TRP.1	This requirement helps meet the objective by establishing a SSL secure channel from the user's browser to the TOE, thus protecting the user's data from disclosure and modification.

5.4.3 Explanation for selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). The TOE is intended to provide a number of capabilities, which are designed to support organisations to

deploy and manage DNS management systems. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with basic attack potential.

6 TOE summary specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE actually implements the claimed security functional requirements.

The TOE security functions include the following:

- **Security Audit**
- **Identification and Authentication**
- **Security Management**
- **TSF Protection**
- **Secure Communication**

6.2 Security Audit

The TOE will create audit records (which contain the date and time of the event, type of event, subject identity and outcome of the event) when the following events occur (**FAU_GEN.1**):

a) User and Administrator login

b) User and Administrator logout

c) Data modification by User and Administrator

Only the Administrator has the capability to review these audit records via the web console (**FAU_SAR.1**). Timestamps are generated for audit logs by utilising the NTP server. This time source is referred by a CMOS clock and used as the source for the timestamp recorded in each audit record.

6.3 Identification and Authentication

When a user issues a request to the TOE to access a protected resource (method), the TOE requires that the user (Users and Administrator) identify and authenticate themselves before performing any TSF mediated action (**FIA_UID.2, FIA_UAU.2**). The TOE compares the credentials by checking the information presented by the user at the login page against the authentication information stored in the database.

All users presented passwords are hashed before being used to authenticate to the TOE, or when users change their passwords (**FMT_MTD.1b**) to be written to the database.

6.4 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE (**FMT_SMF.1**):

Administrator role can modify the access control list stated in Table 5 (**FMT_MSA.1**). The TOE provides a suite of management functions to system administrator and users. These functions allow for the configuration of the TOE to suit the organisation in which it is deployed. Additionally, management roles may perform the following tasks (**FDP_ACC.1, FDP_ACF.1 and FMT_MSA.3)**:

a) mapping user IDs to a group

b) creation of users with default passwords

c) reset password

d) deletion of users/group

e) changing of passwords

f) management of Access Control lists as stated in Table 5

g) report generation

An Administrator may assign and adjust the functions available to users; and users may assign and adjust the functions based on organization's requirement(s) (**FMT_SMR.1 and FMT_MTD.1a**).

6.5 TSF Protection

The TOE maintains time internally using a CMOS clock and is synced with a NTP server. This internal time is used as the source for the timestamp recorded in each audit record, DNSSEC operation and TSIG operation (**FPT_STM.1**). The TOE also protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 5 minutes, it will automatically route users to the login page (**FTA_SSL.3**). The minimum idle time can be modified by the Administrator.

6.6 Secure Communication

When a user accesses the TOE on their browser, via typing in the website address, the TOE will initiate a SSL secure channel establishment with the user's browser (**FTP_TRP.1**). The TOE implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols.