BlueCat Networks
Adonis DNS/DHCP Appliance Version 6.7.1-P3 and Proteus IPAM Appliance Version 3.7.2-P2 Security Target

Version 2.0

August 1, 2013

Prepared For

4101 Yonge St., ste. 502, Toronto, Ontario, Canada, M2P1N6
Phone: +1.416.646.8400, +1.866.895.6931
Fax: +1.416.225.4728, +1.647.259.7317
http://www.bluecatnetworks.com

Prepared By

CYGNACOM SOLUTIONS

7925 Jones Branch Drive♦Suite 5400 ♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

Revision History

Date	Version	Author	Description
05/16/2011	0.1	Nancy Gow	First Draft
05/20/2011	0.2	Nancy Gow	Added Threats, Assumptions, Objectives, Mappings. Updated for Vendor comments.
06/14/2011	0.3	Nancy Gow	Updated for Vendor and Evaluator comments
06/17/2011	0.4	Nancy Gow	Updated for Vendor and Evaluator comments
06/30/2011	0.5	Nancy Gow	Updated for Vendor and Evaluator comments
07/01/2011	0.6	Nancy Gow	Updated for Vendor and Evaluator comments
07/01/2011	1.0	Nancy Gow	IVOR Submission Version
07/15/2011	1.1	Nancy Gow	Updated for Vendor comments
04/02/2012	1.2	Nancy Gow	Updated for IVOR Comments
06/08/2012	1.3	Nancy Gow	Updated for new component versions
06/20/2012	1.4	Nancy Gow	Dropped ALC_DVS.1 augmentation; Updates from Vendor review comments
10/11/2012	1.5	Nancy Gow	Updates from ADV work
11/01/2012	1.6	Nancy Gow	Updates from Vendor comments
01/17/2013	1.7	Nancy Gow	Updates from Vendor comments; Cleaned for TVOR submission
03/10/2013	1.8	Nancy Gow	Updated for Patches
06/25/2013	1.9	Nancy Gow	Updated for testing results and FVOR submission
08/01/2013	2.0	Nancy Gow	Updated for FVOR action items – final version

Table of Contents

Section **Page**

Figures and Tables

Figures

Tables

1 Security Target Introduction

1.1 Security Target Reference

ST Title: BlueCat Networks Adonis DNS/DHCP Appliance Version 6.7.1-P3 and Proteus IPAM Appliance Version 3.7.2-P2 Security Target

ST Version: v2.0

ST Author: CygnaCom Solutions

ST Date: August 1, 2013

Assurance level: EAL *2* augmented with ALC_FLR.1

Protection Profile: None

Keywords: IP Address Management, IPAM, DNS, DHCP, Network Management

1.1.1 *References*

Table 1-1 provides the references used to develop this Security Target.

Table 1-1: References

Reference Title	ID
Adonis 1200 DNS/DHCP Solution Installation Guide for Version 6.7.1	[A1200 INSTALL]
Adonis 1900 DNS/DHCP Solution Installation Guide for Version 6.7.1	[A1900 INSTALL]
Adonis 1950 DNS/DHCP Solution Installation Guide for Version 6.7.1	[A1950 INSTALL]
Adonis 800 DNS/DHCP Solution Installation Guide for Version 6.7.1	[A800 INSTALL]
Adonis Administration Guide Version 6.7.1	[AADMIN]
Release Notes Adonis DNS/DHCP Software Version 6.7.1	[ARELEASE]
Release Notes Adonis Appliances Hotfix KB-4606	[AREL-HF]
Release Notes Adonis v6.7.1 P1 Patch KB-3542	[AREL-P1]
Release Notes Adonis v6.7.1 P2 Patch KB-3888	[AREL-P2]
Release Notes Adonis v6.7.1 P3 Patch KB-4781	[AREL-P3]
Adonis XMB^2 Installation Guide	[AXMB2 INSTALL]
Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-002, Version 3.1, Revision 3	[CC]
DNSSEC-Secure DNS for Government, BlueCat Networks' Public Sector Practice	[DNSSEC]
Proteus 3300 IP Address Management Solution Installation Guide for Version 3.7.1	[P3300 INSTALL]
Proteus 5500 IP Address Management Solution Installation Guide for Version 3.7.1	[P5500 INSTALL]
Proteus Administration Guide Software Version 3.7.1	[PADMIN]
Release Notes Proteus v3.7.1 P1 Patch KB-3541	[PREL 3.7.1-P1]

Reference Title	ID
Release Notes Proteus™ IPAM Software Version 3.7.2	[PREL 3.7.2]
Release Notes Proteus v3.7.2 P1 Patch KB-4519	[PREL 3.7.2-P1]
Release Notes Proteus v3.7.2 P2 Patch KB-4780	[PREL 3.7.2-P2]
Release Notes Proteus IPAM Software Version 3.7.1	[PRELEASE]

1.2 TOE Reference

TOE Identification: BlueCat Networks Adonis DNS/DHCP Appliance Version 6.7.1-P3 and Proteus IPAM Appliance Version 3.7.2-P2

TOE Vendor: BlueCat Networks, Inc.

1.3 TOE Overview

The Target of Evaluation is BlueCat Networks Adonis DNS/DHCP Appliance - and Proteus IPAM Appliance, which will hereafter be referred to as the TOE throughout this document.

The TOE is an IP Address Management (IPAM) Solution, which provides network management of an organization's IP infrastructure along with DNS and DHCP core services.

The BlueCat Networks Proteus IPAM Appliance provides organizations with a scalable platform to manage their IP infrastructure. Proteus tightly integrates IP Address Management (IPAM), DNS and DHCP. The Proteus IPAM Appliance gives enterprises the ability to centrally manage, monitor and administer their entire IP address and DNS name spaces. Proteus also allows organizations to manage change and growth with support for both IPv4 and IPv6 networks and DNSSEC.

The BlueCat Networks Adonis DNS/DHCP Appliances deliver DNS and DHCP core services. The Adonis Appliances enable organizations to streamline the implementation and management of complex DNS and DHCP infrastructures in IPv4 and IPv6 networks. Adonis also supports DNSSEC.

The TOE provides the following security functionality: auditing of security relevant events; security event based alerting; audit review; protection of audit data; management of TOE user accounts; TOE user identification and authentication; security role based access to management functions; trusted communication between components; generation of reliable time and network management security functions including DNSSEC and network discovery and reconciliation.

1.3.1 *TOE Type*

The TOE is an Internet Protocol Address Management (IPAM) system, which provides DNS and DHCP services.

1.3.2 *Hardware/Firmware/Software Required by the TOE*

The evaluated configuration of the TOE requires the following Operational Environment support:

- A Web Browser to access the Proteus WebUI management interface. The Proteus WebUI supports:
  - Internet Explorer (v7 and v8)
  - Firefox (v3.5+)
  - Chrome
- Keyboard and Monitor for Adonis and Proteus CLI Access
- A protected connection between the Proteus appliance and the Adonis appliance(s)

The following Operational Environment components are optional for the evaluated configuration of the TOE although they will be included in the tested configuration.

- An external Syslog server for administrator alert notifications and external storage of audit log records
- An SNMP Trap server for administrator alert notifications
- An E-mail server to send administrator alert notifications
- An NTP server to provide reliable time for the Proteus appliance
- An external authentication server (LDAP, RADIUS, TACACS+, Microsoft Active Directory, Kerberos)

1.4 TOE Description

1.4.1 *Acronyms*

The following table defines product specific and CC specific acronyms used within this Security Target.

Table 1-2: Product and CC Acronyms

Acronym	Definition
API	Application Programming Interface
BIND	Berkeley Internet Name Domain
CC	Common Criteria [for IT Security Evaluation]
CLI	Command Line Interface
CM	Configuration Management
DDI	DNS, DHCP, and IPAM
DDNS	Dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone (a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network)
DNS	Domain Name Server / System
DNSSEC	DNS Security Extensions
EAL	Evaluation Assurance Level
ENUM	Electronic Numbering
FIPS	Federal Information Processing Standards Publication

Acronym	Definition
GSS-TSIG	Generic Security Service Algorithm for Secret Key Transaction
GUI	Graphical User Interface
HD	Host Density
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
ID	Identifier
IETF	Internet Engineering Task Force
IPAM	IP Address Management
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NIST	National Institute of Standards and Technology
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Security Layer
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSIG	Transaction Signature
TSP	TOE Security Policy
UDP	User Datagram Protocol
UI	User Interface
VPN	Virtual Private Network

1.4.2 *Terminology*

The following table defines product-specific and CC-specific terminology used within this Security Target.

Table 1-3: Product and CC Terminology

Terminology	Definition
Assets	Information or resources to be protected by the countermeasures of a TOE.

Terminology	Definition
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Audit Log (Audit Trail)	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	To establish the validity of a claimed user or object.
Authenticator	An object that contains the settings for connecting to and retrieving user data from an external authentication server.
Authoritative Server, Authoritative Name Server	An authoritative name server is a name server that only returns answers to queries about domain names that have been specifically configured by the administrator. The authoritative name server only returns the definitive versions of all records in the zone(s).
Authorized Administrator (TOE Administrator)	The authorized users that manage the TOE or a subset of its TSF data and management functions.
Availability	Assuring information and communications services will be ready for use when expected.
Berkeley Internet Name Domain (BIND)	A commonly used Domain Name System (DNS) server application on the Internet
Block	A section of a network used to manage IP address space. In the TOE, a user can set DNS restrictions, a default view, and default domains for a block.
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.
Demilitarized Zone (DMZ)	A physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network.
DHCP Zone	The assignment of a DNS server to an IP block or network to receive DDNS updates (DDNS updates can be optionally signed with TSIG or GSS-TSIG.
Discovery	The process by which Proteus uses SNMP interrogation against one or more routers and layer 3 switches to discover the IP address, hardware address, and DNS host name (if DNS is available) for hosts on a network.
DNS Zone	A portion of the global Domain Name System (DNS) namespace for which administrative responsibility has been delegated.
ENUM Zone	ENUM zones are used to allow a DNS server (managed by Proteus) to provide the e.164 phone numbers associated with client endpoints.
Evaluation	Assessment of a PP, a ST or a TOE, against defined criteria.
Incident	One or more intrusion events that are suspected of being involved in a possible violation of a security policy.

Terminology	Definition
Information Technology (IT) System	May range from a computer system to a computer network.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
IT Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Kerberos	A computer network authentication protocol that works based on "tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
Layer	An abstraction level used to represent computer network architecture.
Layer 2	The Data Link Layer of the seven-layer OSI model of computer networking. It corresponds to, or is part of the link layer of the TCP/IP reference model. The Data Link Layer is responsible for Media Access Control, Flow Control and Error Checking.
Layer 3	The Network Layer is Layer 3 of the seven-layer OSI model of computer networking. The Network Layer is responsible for routing packets delivery including routing through intermediate routers.
MAC Address	A unique identifier assigned to network interfaces for communications on the physical network segment.
Naming Policy	A collection of rules that controls the names that may be assigned to DNS resource records.
Network	Two or more machines interconnected for communications.
Override List	A specification of addresses and ranges that a reconciliation policy should ignore.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packet Sniffer	A device or program that monitors the data traveling between computers on a network.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Reconciliation	The process of reconciling MAC, IPv4, and IPv6 address information retrieved via Discovery with the content of the Proteus database.
Root (root user, root account)	The superuser, a user on Unix-like systems, usually with full administrative privileges.
Security	A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Subnet	A subnetwork; a logically visible subdivision of an IP network.
Tag (Group)	Tag groups and tags are used to create a model of an organization or process. An organization's network resources can be mapped by applying tags to objects within Proteus, such as DNS zones and networks.
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Terminology	Definition
Threat	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
Trust Anchor	To be able to prove that a signed DNS answer is correct, one needs to know at least one key or DS record that is correct from sources other than the DNS. These starting points are known as trust anchors and are typically obtained with the operating system or via some other trusted source.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

1.4.3 *Product Description*

BlueCat Network offers an IP Address Management (IPAM) Solution, which provides network management of an organization's IP and name infrastructures along with DNS and DHCP core services. The evaluation includes BlueCat Network's Proteus and Adonis appliance-based products. The Proteus IPAM Appliance gives enterprises the ability to centrally manage, monitor and administer their entire IP and name spaces while the Adonis DNS/DHCP Appliances provide core services (DNS and DHCP) in IPv4 and IPv6 network infrastructures.

The TOE consists of the following components:

- Adonis DNS/DHCP Appliance Version 6.7.1-P3
- Proteus IPAM Appliance Version 3.7.2-P2

The evaluated configuration of the TOE includes a Proteus IPAM Appliance managing two or more Adonis DNS/DHCP Appliances.

1.4.3.1 Adonis DNS/DHCP Appliance (Adonis)

Adonis is an appliance server for DNS/DHCP service provision. Adonis is a secure DNS appliance that not only protects the server, but also the DNS application and data. In addition, the DNS service runs in a jailed environment to isolate DNS threats within the system.

Adonis examines incoming DNS and DHCP requests for anomalies and provides the following functionality:

- Adonis provides secure resolution of domain names
- Adonis provides secure configuration, deployment, administration and allocation of dynamic IP addresses
- Adonis ensures the reliability and availability of DNS and DHCP services
- Adonis uses transaction signatures (TSIGs & GSS-TSIG) to provide a certificate-based authentication system for DNS from DHCP servers. This enables trusted transfers and modifications of DNS information. Adonis appliances use TSIGs to protect all transfers between them.

An Adonis appliance operates with very few open ports; ports are opened only if they are required by the network services being deployed on the appliance. Operating behind a dynamically configured packet-filtering firewall, Adonis is suited to network conditions that include hostile environments such as DMZs or the Internet. BlueCat Network's Linux™-based operating system is stripped down to its essential code, so the kernel does not load new modules during run-time. The DNS daemon (service) also runs in a chroot-jailed environment to prevent the server from being compromised in the highly unlikely event that the service is breached. The BlueCat Network's Linux operating system kernel has been hardened so that:

- All non-essential OS services and network service daemons have been removed
- The firewall and IP stack have been hardened
- The BIND daemon is started with control scripts, instead of the init daemon

Adonis offers full support for DHCPv6 to provide stateful assignment of IPv6 addresses. Full support for DNS64 provides the DNS portion of a NAT64 transition solution. These features are available only when the Adonis appliances are managed by a Proteus appliance.

Adonis is configured by Proteus to provide a masked BIND version number by default. Network administrators can configure the exact response they want returned when an Adonis appliance is queried for its BIND version. This allows the obfuscation of sensitive version information from potential attackers.

BlueCat uses ISC BIND version 9.8.3-P4. The RFC2845 (Secret Key Transaction Authentication for DNS) specifies the transaction signature (TSIG) user.

Adonis also provides the ability to secure DNS data through DNSSEC, allowing organizations to both serve and validate DNS information to ensure the authenticity and integrity of DNS records and servers being accessed.

Adonis DHCP implements a basic form of Network Access Control based on the requesting client's MAC address. A request for a dynamic IP address (and therefore access to the network) can be allowed or denied based on the client's MAC address being present in an access list.

Communications between the Proteus appliance and the Adonis appliances that it manages are secured with SSL. Secure communications is also implemented by mutual, certificate-based authentication which allows Proteus to verify the identity of an Adonis appliance (and vice versa) prior to establishing a connection with that appliance. 128-bit encrypted

communication sessions between the Proteus and Adonis appliances protect against packet snooping.

Adonis includes an Administration Console, which is a command line interface (CLI) that allows off-line installation, configuration and maintenance of the Adonis. Because the CLI is not used for run-time operation of the TOE, its functionality is not included in the scope of the evaluation.

Note: Remote login to the CLI (via SSH) can be disabled if required for the customer's security requirements.

***Warning**: BlueCat strongly advises that all network configuration changes and interface settings changes to Adonis or Proteus be made using the Administration Console only, without exception. Failure to use the Administration Console for network and interface changes may result in loss of network services, loss of the management connection, or failure of xHA functionality.*

Adonis also includes a Management Console, which provides a run-time management GUI for a stand-alone Adonis configuration. When the Adonis appliances are being managed by a Proteus appliance, the Management Console is inoperable; users will get an error message box if they try to use the Management Console. The stand-alone Adonis configuration is not being evaluated and therefore the Management Console is not in the scope of the evaluation.

The same software including the BlueCat Adonis implementation and the hardened Linux-based operating system is loaded on all Adonis appliance hardware models. All Adonis hardware models are included in the evaluation. All software installed on the Adonis appliances including the Adonis implementation, OS, and third-party software packages are included in the evaluation. The following third-party software is used on Adonis:

- Debian GNU/Linux – free operation system from Debian Project (http://www.debian.org/)
- ISC BIND – open source implementation of DNS service from ISC (Internet Systems Consortium, http://www.isc.org/)
- ISC DHCP – open source implementation of DHCP service from ISC
- MIT Kerberos-5 (no KDC, only user part) – open source Kerberos implementation from MIT (Massachusetts Institute of Technology, http://www.mit.edu/)
- SUN JRE – Java Runtime Environment previously from SUN (now Oracle, http://www.oracle.com/)
- Jetty – open source HTTP server and Servlet container (http://www.eclipse.org/jetty/about.php).

Two Adonis appliances of the same model can be configured to provide the Adonis Crossover High Availability (xHA) feature. xHA makes two Adonis appliances function as a single appliance that Proteus manages as a single virtual server. If one of the appliances fails for any reason, the other takes its place and continues providing services. The pair appears as a single server for DNS queries because both servers share a virtual IP address. Synchronization is handled within the operating system rather than at the DHCP service level.

xHA uses an enslaved master as a passive node. The passive node monitors the active node and becomes the active master if it determines that the active node is not responding. xHA performs data replication between the two nodes to ensure that the passive node always has up-to-date data and that failover occurs seamlessly. Data replication can be performed through the servers' standard network connections, or through an optional xHA Backbone Communication connection operating on the servers' eth1 ports.

The Proteus management interface can be used to force an xHA failover by an administrator. xHA failover switches the roles of the servers in the xHA pair: the passive server becomes the active node, and the formerly active server becomes the passive node. xHA failover can be used to change server roles to allow a server to be taken offline for maintenance.

1.4.3.2 Proteus IPAM Appliance (Proteus)

Proteus is a dedicated security device specifically designed for configuring and managing Adonis DNS/DHCP Appliances. Proteus provides the ability to manage DNS and DHCP services, discover IP devices, and enables tracking and management of an organization's entire IP infrastructure.

Proteus allows users to:

- Provision core network services
- Manage core DNS and DHCP services
- View the whole network's IP address and name space usage
- Make or approve changes to DHCP or DNS configurations
- Choose an appliance deployment option to match their organization's scale, budget and business continuity needs
- Manage multiple Adonis DNS and DHCP appliances
- Identify overlapping IP space during the merging of distinct networks
- Merge networks with dynamic and static IP assignments without risk of conflicts
- Move and relocate DNS, DHCP and IP network and address data while retaining metadata and configuration info
- Track all changes in detailed audit trails that show when and how an object was changed
- Clearly identify which networks are seeing the greatest and least growth
- Find available IP space in networks with a single click
- Create, resize and remove networks on demand and instantly update DNS records accordingly
- Configure recursive DNS
- Configure DNS Response Policies

The Adonis appliances, when managed by a Proteus appliance, offer full support for DHCPv6 to run stateful assignment of IPv6 addresses. Administrators are able to configure and deploy DHCPv6 providing:

- Assignment of both Global Unicast and Unique Local IPv6 addresses
- Full DHCPv6 option support to allocate configuration settings to IPv6 clients.
- IPv6 lease notifications and lease history to track all IPv6 address assignments

- Dual-stack host tracking through dynamic DNS when assigning both IPv4 and IPv6 addresses through DHCP

DHCPv6 support in Proteus includes the following limitations:

- DHCPv6 Prefix delegation is not currently supported.
- The following limitations arise from the ISC DHCP implementation:
    - IPv6 addresses that fall into DHCPv6 ranges between ::80 and ::FF with any network prefix cannot be leased
    - DHCPv6 server can only communicate with a DNS server over IPv4 for DDNS updates

Full support for DNS64 provides the DNS portion of a NAT64 transition solution for Adonis appliances managed by Proteus. NAT64 is used in IPv6-only environments to facilitate communication with IPv4-only hosts. Working in tandem with a NAT64 solution, DNS64 is used to synthesize IPv6 DNS records based on an existing IPv4 host automatically. The NAT64 gateway is then used to translate between the IPv6 synthesized IPv6 address and the real IPv4 address. Adonis supplies the DNS64 part of the solution, allowing administrators to configure DNS64 settings and options for any DNS caching server.

Proteus also provides automatic discovery and IP reconciliation. Proteus uses SNMP to talk directly to routers and layer 2 and/or layer 3 switches, enabling Proteus to find changes to IP-enabled devices across geographically dispersed networks automatically. After finding addresses that have been newly added and recently removed from the network, the discovery tool also identifies conflicts based on DNS host name and MAC address. After discovery, the IP reconciliation functionality compares the changes to identify unused IP addresses for reclamation and help uncover unauthorized IP addresses that can create security vulnerabilities. Discovery and IP reconciliation is supported for both IPv4 and IPv6 addresses.

The DNS Response Policies feature allows users to manage a recursive DNS resolver attempting to respond to the queries that might not be desirable or legal. DNS Response Policies allow customers to respond to DNS requests for domains and hosts that they do not own. DNS response policies allow customers to enforce corporate policies using DNS. By intercepting DNS requests for user-defined domains and hosts, Proteus can block or allow particular domain name queries. For example:

- To prevent employees from being connected to any harmful website, administrators can setup the response policies and block these harmful websites so that they do not return the query response.
- To follow a government regulation that mandates certain DNS blocking, the response policies can be used to implement this requirement.

There are three different types of response policies that can be set based on user requirements:

- *Blacklist*—Matching items in the list of blacklist object return a Not-existing domain (NXDomain) result.
- *Blackhole*—Matching items in this response policy object return a NOERROR result with no answers.

- *Whitelist*—Matching items in this response policy object are excluded from further processing.

Proteus includes an Administration Console, which is a command line interface (CLI) that allows off-line installation, configuration and maintenance of Proteus including database backup, and maintenance. Because the CLI is not used for run-time operation of the TOE, its functionality is not included in the scope of the evaluation.

Note: Remote login to the CLI (via SSH) can be disabled if required for the customer's security requirements.

***Warning**: BlueCat strongly advises that all network configuration changes and interface settings changes to Adonis or Proteus be made using the Administration Console only, without exception. Failure to use the Administration Console for network and interface changes may result in loss of network services, loss of the management connection, or failure of xHA functionality.*

Run-time management of the TOE is performed via the Proteus web interface (WebUI). The WebUI is accessed through a standard internet browser and is accessible over both IPv4 and IPv6. Access to the management functionality is controlled by the Proteus user's access rights, overrides, and privileges, which control how users see and work with objects and information. The WebUI may be accessed by default via any web-enabled device, however for the evaluated configuration Proteus should always be installed in a trusted part of the network (e.g. not the external or public part of the network). If remote access to Proteus outside the trusted part of the network is required, the use of a virtual private network (VPN) is recommended.

***Warning**: The Proteus appliance must be configured with HTTPS enabled and HTTP disabled.*

Proteus hardware models 5500 and 3300 are included in the evaluation. The same software including the BlueCat Proteus implementation and a hardened Linux-based operating system is loaded on all Proteus appliance hardware models. The 64-bit Linux-based operating system installed on the Proteus has been hardened in the same manner as the OS installed on the Adonis appliances:

- All non-essential OS services and network service daemons have been removed
- The IP stack has been hardened

Proteus also includes a PostgreSQL database that maintains configuration data, system data, and audit information. Passwords that are used to access the external servers in the Operational Environment are hashed using MD5 and stored in the Proteus database. In particular, each password used by SNMP to access the switches and routers in the environment are maintained in the Proteus database as an MD5 hash.

All software installed on the Proteus appliances including the Proteus implementation, OS and third-party software packages are included in the evaluation. The following third-party software is used on Proteus:

- Debian GNU/Linux – same as in Adonis
- PostgreSQL – open source object-relational database system from PostgreSQL community (http://www.postgresql.org/)
- JBoss – open source Java application server from JBoss community (http://www.jboss.org/) which also provides HTTP server functionality
- OpenSSL – open source toolkit, implementing SSL v2/v3 and TLS v1 protocols, from OpenSSL Project community (http://www.openssl.org/)
- SUN JRE – Java Runtime Environment, previously from SUN (now Oracle, http://www.oracle.com/)

1.4.4 *Data*

The data managed by the TOE can be categorized as:

- Data used to configure, manage, and operate the TOE such as: user accounts and DNS configuration data
- Audit data produced by the TOE for security significant events
- Networks IP and name structures
- Information collected from the managed network such as: IP and MAC addresses

All TOE data is considered TSF Data.

1.4.5 *Users*

The TOE maintains defined user roles, each with its own set of administrative privileges.

The defined roles for users of the Proteus WebUI are:

- "*Administrator*" Role
- "*Non-Administrator*" Role

When a new user account is created, the user must be assigned privileges and access rights to access TOE data and functionality. A user may be assigned multiple privileges and access rights individually and by being assigned to user groups, which are used to organize users and to assign and control access rights. The TOE uses access rights, overrides, and privileges to control how users see and work with objects and information. These access control settings can be configured to limit the user to specific datasets. No access is allowed to the system until a user has been authenticated. The TOE's interfaces control access to the TSF data and functions so that authenticated users have access only to the data and functions allowed by their roles, privileges and access rights. All users of the TOE have access to TSF data and management functions; therefore, they are considered administrators for the purposes of this evaluation. The terms "TOE user", "TOE administrator" and "authorized administrator" are used in this ST to refer collectively to all authorized TOE users.

Access to the Adonis and Proteus Administration Console command line interfaces is through the default "*admin*" user account. The CLI is used only for off-line installation, configuration and maintenance of the TOE; therefore, "*admin*" is not considered a TOE user role.

1.4.6 *Product Guidance*

The TOE documentation set includes both context-sensitive online help and downloadable PDF files through the Proteus WebUI. Customers may also download the documentation from the BlueCat Customer Care website. The following product guidance documents are provided with the TOE:

Table 1-4: User Guidance Documents

Adonis 1200 DNS/DHCP Solution Installation Guide for Version 6.7.1
Adonis 1900 DNS/DHCP Solution Installation Guide for Version 6.7.1
Adonis 1950 DNS/DHCP Solution Installation Guide for Version 6.7.1
Adonis 800 DNS/DHCP Solution Installation Guide for Version 6.7.1
Adonis Administration Guide Version 6.7.1
Adonis XMB^2 Installation Guide
Proteus 3300 IP Address Management Solution Installation Guide for Version 3.7.1
Proteus 5500 IP Address Management Solution Installation Guide for Version 3.7.1
Proteus Administration Guide Software Version 3.7.1
Release Notes Adonis Appliances Hotfix KB-4606
Release Notes Adonis DNS/DHCP Software Version 6.7.1
Release Notes Adonis v6.7.1 P1 Patch KB-3542
Release Notes Adonis v6.7.1 P2 Patch KB-3888
Release Notes Adonis v6.7.1 P3 Patch KB-4781
Release Notes Proteus IPAM Software Version 3.7.1
Release Notes Proteus v3.7.1 P1 Patch KB-3541
Release Notes Proteus v3.7.2 P1 Patch KB-4519
Release Notes Proteus v3.7.2 P2 Patch KB-4780
Release Notes Proteus™ IPAM Software Version 3.7.2

1.4.7 *Physical Scope of the TOE*

The TOE consists of the components described in Section 1.4.3. The physical boundary of the TOE is the Adonis and Proteus Appliances, including all hardware and all software installed on the appliances.

The TOE Boundary is depicted in the following figure.

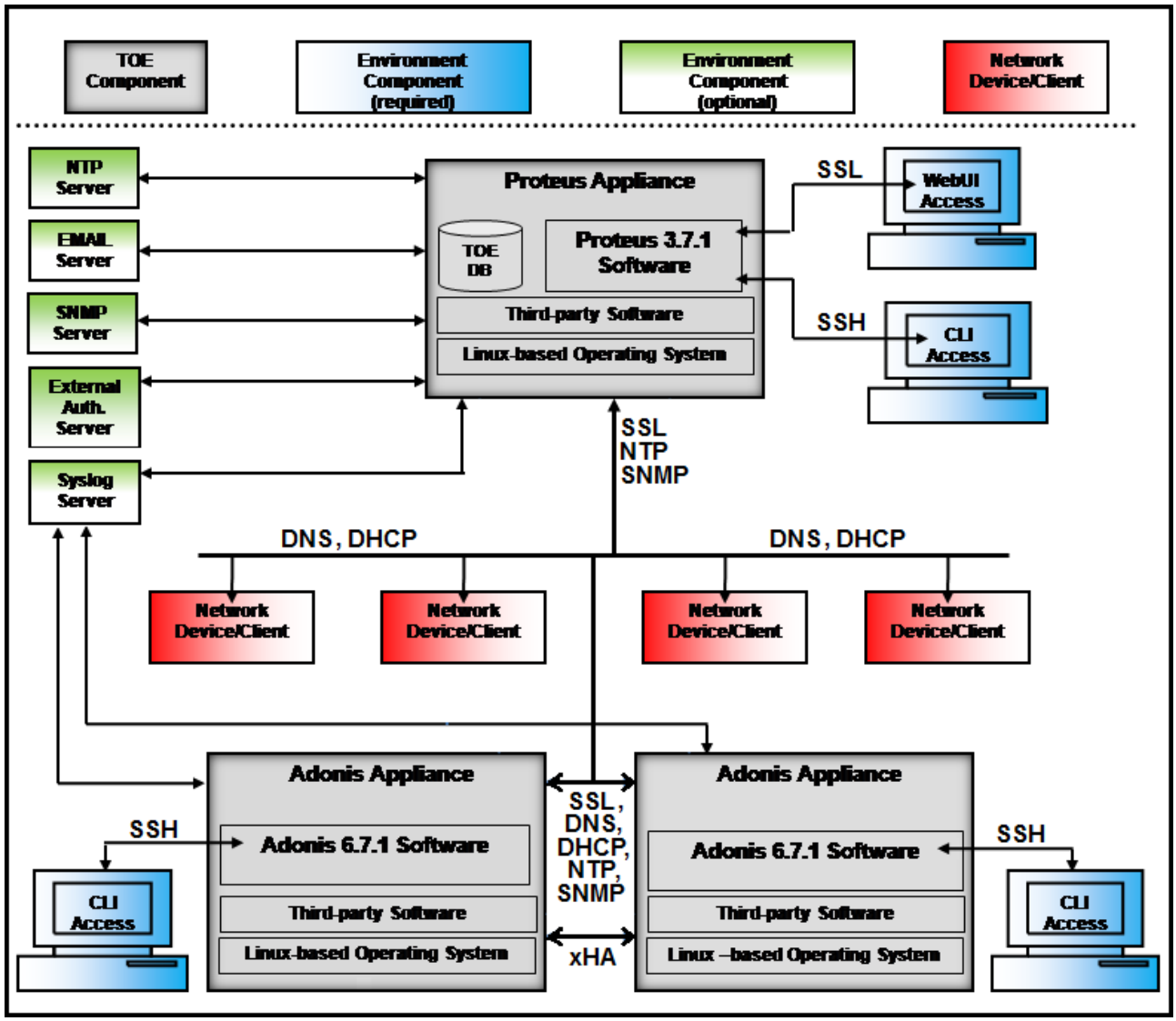

Figure 1: TOE Boundary

1.4.7.1 Included in the TOE:

The evaluated configuration includes the following:

- Adonis DNS/DHCP Appliance Version 6.7.1-P3
- Proteus IPAM Appliance Version 3.7.2-P2

All appliance hardware and the software installed on the physical and virtual appliances are included in the TOE.

The tested configuration included the following:

- The test configuration consisted of two instances of a Proteus IPAM Appliance managing two Adonis DNS/DHCP Appliances (one thread all physical appliances and one thread all virtual appliances).
- The management of the Proteus (WebUI platform) used a desktop PC running Windows 7 with Firefox, Chrome, and IE browsers installed.
- The testing environment included external authentication servers, an external SNMP server, an external SMTP (e-mail) server, an external Syslog server and an external NTP server
- The Proteus and Adonis appliances were tested in STIG-compliant configuration (running in STIG mode) and non-STIG-compliant configuration.
- The Proteus appliance had HTTPS enabled and HTTP disabled.
- A Crossover High Availability (xHA) configuration of two Adonis appliances was tested to ensure that setup and configuration procedures follow those in the vendor documentation. The xHA failover function used two Adonis appliances hardwired together.

1.4.7.2 Excluded from the TOE:

The following product components and functionality are not included in the scope of the evaluation:

- VMware supporting environment
- Stand-alone Adonis configuration (including Adonis Management Console)
- Proteus management of third-party (non-Adonis) DNS/DHCP servers (The evaluated configuration does not exclude all communications with third-party DNS/DHCP servers, only their management by the Proteus appliance. Testing scenarios will include third-party servers)
- Proteus cloud computing services
- Proteus for Windows DNS and DHCP (separate package and licensing)
- The Proteus and Adonis Administration Consoles (CLIs) used for installation, initial configuration and off-line maintenance of the appliances. (though not included in the scope of the operational TOE, the CLIs were tested during the installation of the TOE)
- A private connection between the Proteus and Adonis appliances (a dedicated management network) is not needed for secure communications because the appliances run SSL over an existing, non-management network

The following components are part of the Operational Environment of the TOE and excluded from the scope of the evaluation:

- The web browser used for the management interface of the TOE
- Keyboard and Monitor for Adonis and Proteus CLI Access (used only for initial configuration and off-line maintenance of the appliances)
- The operational network that is used for communication between the TOE components (whether separate network (i.e. a dedicated management LAN) or the same network that the TOE provides DNS/DHCP services for
- The operational network that the TOE provides DNS/DHCP services for
- An optional Syslog server for external storage of the audit records
- An optional NTP server for reliable time for the Proteus appliance

- An optional E-mail server for administrator alert notifications
- An optional SNMP Trap server for administrator alert notifications
- An optional external authentication server (LDAP, RADIUS, TACACS+, Microsoft Active Directory, Kerberos)

Note: The tested configuration included the optional Syslog, NTP, E-mail, SNMP, and external authentication servers.

1.4.8 *Logical Scope of the TOE*

The TOE provides the following security functionality:

1.4.8.1 Security Audit

The TOE is able to audit the use of the administration/management functions. This function records successful and failed authentication of TOE users, as well as the actions taken by TOE users once they are authenticated. The TOE also audits system events.

The TOE can be configured to send an alarm when a designated system event occurs. The audit data is protected by the access control mechanisms of the OS of the TOE components and by the TOE management interface. Only users with direct access to the appliances' OS have access to the audit records. Authorized users can view and sort the audit records via the TOE management interface. The TOE has the ability to offload audit records to an external Syslog server for external storage of audit data.

***Note**: If the environment requires long-term storage of audit records, then the TOE should be configured to offload audit records to an external Syslog server for external storage. The TOE also supports an administrative function that allows for the manual downloading of audit trails for off appliance long-term storage.*

1.4.8.2 Identification and Authentication

The TOE requires all users to provide unique identification and authentication data before any access to the TOE is granted. User identification and authentication is done by the TSF through username/password authentication or optionally by an external authentication server.

All authorized TOE users must have a user account with security attributes that control the user's access to TSF data and management functions. These security attributes include user name, password, and level(s) of authorization (roles, privileges, access rights) for TOE users.

Identification and Authentication depends on the Operational Environment to provide an external authentication server if that feature is configured. It also depends on the Operational Environment to provide secure communications between the TOE and the external authentication server.

1.4.8.3 Security Management

The TOE provides a web-based management interface for all run-time TOE administration. The ability to manage various security attributes, system parameters and all TSF data, and to run the administrative functions is controlled and limited to those users who have been assigned the appropriate administrative roles, permissions and access rights.

Security management relies on a platform in the Operational Environment with a properly configured Web Browser to support the web-based management interfaces.

1.4.8.4 Protection of Security Functions

The TOE ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured through various methods including encryption and mutual, certificate-based authentication.

The TOE provides NTP capabilities for its own use.

1.4.8.5 TOE Access Functions

The TOE will terminate a user's administrative session after a specified period of inactivity.

1.4.8.6 Network Management Functions

The TOE will issue alarms when a DHCP range is above or below defined watermarks.

The TOE implements DNSSEC in accordance with Internet Engineering Task Force (IETF) specifications to secure DNS data transmission.

The TOE provides automatic discovery and IP reconciliation for both IPv4 and IPv6. The TOE identifies conflicts based on DNS host names, IP addresses and MAC addresses for network devices. After discovery, the TOE compares the changes to identify unused IP addresses for reclamation and help uncover unauthorized IP addresses that can create security vulnerabilities.

The TOE implements a basic form of Network Access Control based on the requesting client's MAC address. A request for a dynamic IP address (and therefore access to the network) can be allowed or denied based on the client's MAC address being present in an access list.

1.4.8.7 Excluded Functionality

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

- The Proteus and Adonis Administration Consoles (CLIs) used for installation, initial configuration and off-line maintenance of the appliances
- Stand-alone Adonis functionality (including Adonis Management Console)
- Management of third-party DNS/DHCP servers (The evaluated configuration does not exclude all communications with third-party DNS/DHCP servers, only their

management by the Proteus appliance. Testing scenarios will include third-party servers)
- Management of TFTP servers
- Proteus API (Provides programmability to enable customer 3rd-party applications and integration with 3rd-party network management tools)
- Workflow services (separate purchase)
- Migration of data from other systems into Proteus and importation of projects into Adonis
- Proteus cloud computing services
- MAC Authentication mechanism used to authenticate client hosts to allow or deny the client host dynamic IP addresses based on authentication results

***Warning**: The software update management function is included in the TOE; however, the customer must be warned that after application of the update, the product will not be in the evaluated configuration. The customer must receive an update file and public security key file from the BlueCat Customer Care portal, before the new software can be applied. The public security key is used to verify the validity of the update file and must be checked after downloading an update file.*

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 augmented with ALC_FLR.1 from the Common Criteria Version 3.1 R3. This Security Target conforms to the Common Criteria Version 3.1 R3.

2.2 Protection Profile Claim

None

2.3 Package Claim

This ST claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.1.

3 Security Problem Definition

3.1 Threats

The following are threats identified for the TOE and its Operational Environment. The assumed level of expertise of the attacker for all the threats is unsophisticated.

Table 3-1: Threats

TOE Threats		
1	T.DATA_LOSS	An unauthorized user may attempt to disclose, modify, or destroy the data collected and produced by the TOE by bypassing a security mechanism.
2	T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to TSF data or TOE resources via the TOE's administrative interfaces.
3	T.MISMANAGE	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
4	T.PRIVILEGE	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
5	T.TRANSIT_ATTACK	An unauthorized user may attempt to disclose, modify, or destroy data produced or protected by the TOE while it is in transit between TOE components or between a TOE component and a network entity.
6	T.UNDETECT	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.
7	T.UNAUTH_CLIENT	An unauthorized client system attaches to the network and then performs malicious acts.

3.2 Organizational Security Policies (OSPs)

There are no Organizational Security Policies defined for the TOE.

3.3 Assumptions

The following are the assumptions regarding the security environment and the intended usage of the TOE.

Table 3-2: Assumptions

TOE Assumptions		
1	A.INSTALL	Those responsible for the TOE will ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with the administrative guidance.
2	A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains, who are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
3	A.PHYSICAL	The TOE hardware and software critical to security policy enforcement will be physically protected from unauthorized modification.
4	A.PROTECT_COMM	Those responsible for the TOE will ensure the communications between the TOE components and between the TOE and external IT Entities are via secure channels.
5	A.SECURE_PWD	Users will choose strong passwords and protect all authentication credentials.

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment.

4.1.1 *Security Objectives for the TOE*

The following are the TOE security objectives:

Table 4-1: TOE Security Objectives

TOE Security Objectives		
1	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
2	O.ALERTS	The TOE must be able to notify administrative personnel of security significant events.
3	O.AUDIT_PROTECT	The TOE must protect its audit data from unauthorized access and modifications.
4	O.AUDITS	The TOE must record audit records for data accesses and use of the system functions.
5	O.DNSSEC	The TOE must protect communications between the TOE components and clients using the TOE's DNS services in accordance with DNSSEC standards.
6	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
7	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
8	O.NETWORK_ACCESS	The TOE must control access to the protected network based on the attributes of the clients using the TOE's DHCP services.
9	O.NETWORK_ANALYZE	The TOE must be able to analyze collected network data to find differences in the network configuration.
10	O.PROTECT_COMM	The TOE must protect data transmitted between separate parts of the TOE.
11	O.SYSDATA	The TOE must collect data from network clients and devices to use for network management.
12	O.SYSDATA_PROTECT	The TOE must protect the data it collects from network clients and devices from unauthorized access and modifications.

4.1.2 *Security Objectives for the Operational Environment*

The TOE's operating environment must satisfy the following objectives.

Table 4-2: Security Objectives for the Operational Environment

Security Objectives for the Operational Environment		
1E	OE.ADMIN	Administrators are non-hostile, carefully selected and trained, and follow the administrator guidance when using the TOE. Administration is competent and on-going.
2E	OE.ALARMS *	The Operational Environment will provide mechanisms to notify responsible personnel of a possible problem.
3E	OE.CREDENTIALS	Those responsible for the TOE must ensure that all access credentials follow defined procedures for strong passwords, and are protected by the users in a manner that is consistent with IT security.
4E	OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
5E	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
6E	OE.PROTECT_COMM	The Operational Environment must provide a mechanism to establish a trusted communications path, which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and external entities.
7E	OE.XAUTH **	The Operational Environment must provide an authentication service that can be invoked by the TSF for user identification and authentication to control a user's logical access to the TOE and for client host authentication to control a user's logical access to the managed network.

** Note: OE.ALARMS is only applicable when the TOE is configured to use an external Syslog server, SNMP Trap server and/or E-mail server for administrator alert notification.*

*** Note: OE.XAUTH is only applicable when the TOE is configured to use an external LDAP, RADIUS, TACACS+, Microsoft Active Directory or Kerberos authentication service.*

4.2 Security Objectives Rationale

This section provides the rationale for the selection of the objectives, assumptions, and threats. In particular, it shows that the security objectives are suitable to cover all aspects of the TOE security environment.

4.2.1 *Rationale for the IT Security Objectives*

This section provides a rationale for the existence of each assumption, threat, and policy statement that comprise the Security Problem Definition of the TOE. Table 4-3: Security Objectives and Security Environment Mapping demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete.

Table 4-3: Security Objectives and Security Environment Mapping

	O.ACCESS	O.ALERTS	O.AUDIT_PROTECT	O.AUDITS	O.DNSSEC	O.EADMIN	O.IDAUTH	O.NETWORK_ACCESS	O.NETWORK_ANALYZE	O.PROTECT_COMM	O.SYSDATA	O.SYSDATA_PROTECT	OE.ADMIN	OE.ALARMS	OE.CREDENTIALS	OE.INSTALL	OE.PHYSICAL	OE.PROTECT_COMM	OE.XAUTH
A.INSTALL																X			
A.MANAGE													X						
A.PHYSICAL																	X		
A.PROTECT_COMM																		X	
A.SECURE_PWD															X				
T.DATA_LOSS			X		X					X		X						X	
T.MASQUERADE							X												X
T.MISMANAGE						X													
T.PRIVILEGE	X						X											X	X
T.TRANSIT_ATTACK					X					X								X	
T.UNDETECT		X		X					X		X			X					
T.UNAUTH_CLIENT								X	X		X								X

The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

A.INSTALL: Those responsible for the TOE will ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with the administrative guidance.

The OE.INSTALL objective provides for responsible personnel to ensure the secure delivery, installation, management and operation of the TOE.

A.MANAGE: There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains, who are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The OE.ADMIN objective provides for are non-hostile, carefully selected and trained administrators who follow the administrator guidance when using the TOE.

A.PHYSICAL: The TOE hardware and software critical to security policy enforcement will be physically protected from unauthorized modification.

The OE.PHYSICAL objective provides for the physical protection of the TOE hardware and software.

A.PROTECT_COMM: Those responsible for the TOE will ensure the communications between the TOE components and between the TOE and external IT Entities are via secure channels.

The OE.PROTECT_COMM objective ensures the protection of the data from modification or disclosure while being exchanged between TOE components and external entities.

A.SECURE_PWD: Users will choose strong passwords and protect all authentication credentials.

The OE.CREDENTIALS objective provides that administrators will ensure user access credentials follow defined procedures for strong passwords, and are protected by the users in a manner that is consistent with IT security.

T.DATA_LOSS: An unauthorized user may attempt to disclose, modify, or destroy the data collected and produced by the TOE by bypassing a security mechanism.

Audit data produced by the TOE is protected through the O.AUDIT_PROTECT objective. Data collected from network clients and devices is protected through the O.SYSDATA_PROTECT objective. The data used by the TOE's DNS services is protected by the O.DNSSEC objective. Data is protected by the TOE while in transit between TOE components by O.PROTECT_COMM. Data is protected by the Operational Environment while in transit between the TOE components and external servers by the OE.PROTECT_COMM objective. Data is also protected by the Operational Environment while in transit between the TOE components and the web browser used by the management interface by OE.PROTECT_COMM.

T.MASQUERADE: A user or process may masquerade as another entity in order to gain unauthorized access to TSF data or TOE resources via the TOE's administrative interfaces.

The O.IDAUTH provides user identification and authentication functionality by the TOE prior to any TOE data access. The OE.XAUTH objective provides user identification and authentication functionality by an external authentication server invoked by the TOE prior to any TOE data access.

T.MISMANAGE: Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.

The O.EADMIN objective provides a set of effective management functions for the TOE's administrative functions and data.

T.PRIVILEGE: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. OE.PROTECT_COMM provides for secure communications between the TOE and the external authentication server.

T.TRANSIT_ATTACK: An unauthorized user may attempt to disclose, modify, or destroy data produced or protected by the TOE while it is in transit between TOE components or between a TOE component and a network entity.

The TOE protects the data used by its DNS services while in transit by the O.DNSSEC objective. Data is protected by the TOE while in transit between TOE components by O.PROTECT_COMM. Data is protected by the Operational Environment while in transit between the TOE components and external servers by the OE.PROTECT_COMM objective. Data is also protected by the Operational Environment while in transit between the TOE components and the web browser used by the management interface by OE.PROTECT_COMM.

T.UNDETECT: Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

The O.AUDITS objective provides the recording of data accesses and the use of the system functions. The O.ALERTS objective provide for the notification of administrative personnel when security significant events occur. The O.NETWORK_ANALYZE objective provides the TOE functionality to detect changes in the managed network's configuration. O.SYSDATA objective provides for the collection of data from network clients and devices to use to detect security relevant events from the network. The OE.ALARMS objectives provide the mechanisms in the Operational Environment to issue the administrator notifications.

T.UNAUTH_CLIENT: An unauthorized client system attaches to the network and then performs malicious acts.

The O.NETWORK_ACCESS objective helps prevent attacks from network clients by controlling access to the protected network based on the attributes of the clients using the TOE's DHCP services. The O.NETWORK_ANALYZE objective provides the TOE functionality to detect changes in the network's client hosts and devices. O.SYSDATA objective provides for the collection of data from network clients and devices to use for network management. The OE.XAUTH objective provides user identification and authentication functionality by an external authentication server invoked by the TOE prior to any network access.

4.2.2 *Rationale for the Security Objectives for the Environment*

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, interoperability requirements on the TOE and for external components that support the TOE objectives. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

5 Extended Components Definition

All of the components defined below have been modeled on components from Part 2 of the CC Version 3.1 R3

The extended components are denoted by adding "_EXT" in the component name.

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	FAU_ARP_EXT.1	Event alarms
2	FIA_UAU_EXT.2	User authentication before any action
3	FNM_NEA_EXT.1	DHCP Threshold Alerts
4	FNM_SEC_EXT.1	DNSSEC Deployment
5	FNM_NDR_EXT.1	Network Discovery and Reconciliation
6	FNM_MAC_EXT.1	MAC Address Network Access Control

5.1 FAU_ARP_EXT.1 Event alarms

5.1.1 *Class FAU: Security Audit*

5.1.2 *Class and Family Information*

This extended component is part of the standard CC class "FAU: Security Audit" and the standard CC family "Security audit automatic response (FAU_ARP)". Management and audit are as shown in the CC. See Section 8 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

With regard to component leveling, FAU_ARP_EXT.1 is simply a second component, which has no hierarchical relationship with FAU_ARP.1.

5.1.3 *Definition*

FAU_ARP_EXT.1

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_ARP_EXT.1.1 The TSF shall ***[assignment: list of actions]*** upon detection of ***[assignment: type of audit event].***

5.1.4 *Rationale*

FAU_ARP_EXT.1 is modeled closely on the standard component FAU_ARP.1: Security Alarms. FAU_ARP_EXT.1 needed to be defined as an extended component because the TOE can send alarms not only upon the detection of potential security violations, but also upon detection of any designated audit event. This component was defined as extended rather than refined in Section 6, because it also has no dependency on FAU_SAA.1, which requires the definition of rules and the accumulation or combination of events to detect when to send the alarm. The TOE will send the alarm, when designated, on the simple occurrence of the event.

5.2 FIA_UAU_EXT.2 User authentication before any action

5.2.1 *Class FIA: Identification and authentication*

5.2.2 *Class and Family Information*

This extended component is part of the standard CC class “FIA: Identification and authentication” and the standard CC family “FIA: User Authentication (FIA_UAU)”. Management and audit are as shown in the CC. See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

With regard to component leveling, FIA_UAU_EXT.2 is simply an eighth component, which is hierarchical to FIA_UAU.1 (it is a sibling to FIA_UAU.2).

5.2.3 *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 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.

5.2.4 *Rationale*

FIA_UAU_EXT.2 is modeled 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 functionality of the standard component was extended by adding the text *“either by the TSF or by an authentication service in the Operational Environment invoked by the TSF”.*

5.3 New Class FNM: Network Management Security

The FNM Class was defined to cover the security functions of a Network Management TOE, including IP Address Management and DNS and DHCP functionality.

This class contains 4 families, each with a single component:

- Network Event Alarms (FNM_NEA)
- Network Security (FNM_SEC)
- Network Discovery (FNM_NDR)
- Network Access Control (FNM_MAC)

5.4 FNM_NEA_EXT.1 DHCP Threshold Alerts

5.4.1 *Class and Family Information*

This extended component is part of the class “FNM: Network Management Security” and the family “Network Event Alarms (FNM_NEA)”.

5.4.1.1 Family Behavior

This family defines the requirements for the TSF to send alerts for security-related network management events. With regard to component leveling, this family contains only a single component.

5.4.2 *Management*

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

- Management (addition, removal, or modification) of actions
- Configuration of external server to receive/display alerts

5.4.3 *Audit*

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

- Minimal: Actions taken due to detected events

5.4.4 *Definition*

FNM_NEA_EXT.1 DHCP Threshold Alerts

Hierarchical to: No other components.

Dependencies: No dependencies.

FNM_NEA_EXT.1.1 The TSF shall ***[assignment: alert actions]*** upon detection of a DHCP range above or below an administrator defined threshold.

5.4.5 *Rationale*

FNM_NEA_EXT.1 is modeled closely on the standard component FAU_ARP.1: Security Alarms. FNM_NEA_EXT.1 needed to be defined as an extended component because the TOE can send alarms upon the detection of a network event rather than on an FAU_GEN generated audit event. This component was also defined as extended because it also has no dependency on FAU_SAA.1.

5.5 FNM_SEC_EXT.1 DNSSEC Deployment

5.5.1 *Class and Family Information*

This extended component is part of the class “FNM: Network Management Security” and the family “Network Security (FNM_SEC)”.

5.5.1.1 Family Behavior

This family defines the requirements for the TSF to perform DNSSEC functionality in accordance with Internet Engineering Task Force (IETF) specifications. With regard to component leveling, this family contains only a single component.

5.5.2 *Management*

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

- Configuring the DNSSEC actions and data

5.5.3 *Audit*

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

- Minimal: Failures of the DNSSEC functions.
- Basic: All attempted uses of the DNSSEC functions.

5.5.4 *Definition*

FNM_SEC_EXT.1 DNSSEC Deployment

Hierarchical to: No other components.

Dependencies: No dependencies.

FNM_SEC_EXT.1.1 The TSF shall provide a communication path between itself and a DNSSEC enabled client (DNS resolver) that is logically distinct from other communication paths.

FNM_SEC_EXT.1.2 The TSF shall support all the required resource records needed to provide DNSSEC functionality for hosted authoritative domains.

FNM_SEC_EXT.1.3 The TSF shall sign all records hosted on the TOE's authoritative DNS server component using a cryptographic key to produce a digital signature.

FNM_SEC_EXT.1.4 The TSF shall provide support for DNSSEC Signed Zones using Zone Signing Keys (ZSK) and Key Signing Keys (KSK).

FNM_SEC_EXT.1.5 The TSF shall provide support for DNSSEC Trust Anchors.

FNM_SEC_EXT.1.6 When the DNS resolver requests a DNS record, the TSF shall also provide the DNS resolver with a digital signature of the record that was created by the cryptographic key.

FNM_SEC_EXT.1.7 The TSF shall support the use of NIST default parameter settings for zone signing.

FNM_SEC_EXT.1.8 The TSF shall support the use of administrator configured schedules and key rollover settings for automated KSK and ZSK re-signing.

FNM_SEC_EXT.1.9 When the TOE is acting as a DNS client, the TSF shall use DNSSEC standards to validate signatures from other DNSSEC servers.

5.5.5 *Rationale*

FNM_SEC_EXT.1 was modeled on sub-components of the CC Part 2 SFR FTP_TRP.1: Trusted Path. This component needed to be explicitly defined, since no standard Common Criteria SFR covers the DNSSEC functionality.

5.6 FNM_NDR_EXT.1 Network Discovery and Reconciliation

5.6.1 *Class and Family Information*

This extended component is part of the class "FNM: Network Management Security" and the family "Network Discovery (FNM_NDR)".

5.6.1.1 Family Behavior

This family defines the requirements for the TSF to perform network discovery and reconciliation functionality. With regard to component leveling, this family contains only a single component.

5.6.2 *Management*

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

- the management (addition, removal, or modification) of network discovery configuration
- the management (addition, removal, or modification) of reconciliation actions

5.6.3 *Audit*

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

- Basic: Events related to the reconciliation of IP addresses

5.6.4 *Definition*

FNM_NDR_EXT.1 Network Discovery and Reconciliation

Hierarchical to: No other components.

Dependencies: No dependencies.

FNM_NDR_EXT.1.1 The TSF shall provide the ability to run discovery scans of authorized administrator defined ranges of the managed network and collect at least the following information from each network host:

- IP address
- MAC address
- Network router connected to host
- DNS host name (if DNS is available)

FNM_NDR_EXT.1.2 The TSF shall provide the ability to run discovery scans at authorized administrator scheduled times and immediately on authorized administrator command.

FNM_NDR_EXT.1.3 TSF shall analyze all network data collected and report the following discrepancies between the scan data and the network data stored in the TOE:

- IP address exists on the physical network, but not in the TOE
- IP address exists in the TOE but not on the physical network (IPv4 only)
- IP address exists in both the TOE and on the network, but the MAC address or DNS host name information does not match (IPv4 only)

FNM_NDR_EXT.1.4 The TSF shall provide authorized users with the capability to read the discovery scan information and analysis results.

FNM_NDR_EXT.1.5 The TSF shall provide the discovery scan information and analysis results in a manner suitable for the authorized users to interpret the information.

FNM_NDR_EXT.1.6 The TSF shall provide authorized administrators the ability to perform the following reconciliation actions:

- reconcile all addresses
- reconcile selected addresses
- enable/disable automatic reconciliation (IPv4 only)
- view all addresses (IPv4 only)
- view non-reconcilable addresses (IPv4 only)
- add addresses to the override list (IPv4 only)
- delete addresses

FNM_NDR_EXT.1.7 The TSF shall be able to perform the discovery and reconciliation process for both IPv4 and IPv6.

5.6.5 *Rationale*

FNM_NDR_EXT.1 was modeled after IDS_SDC_EXT.1, IDS_ANL_EXT.1, and IDS_RCT_EXT.1 from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. (These SFRs in turn were modeled after FAU_GEN requirements from CC Part 2). This component needed to be explicitly defined, since no standard Common Criteria SFR covers the network discovery and reconciliation functionality of the TOE. The three IDS components used as models were combined into one SFR and augmented to cover the entire network discovery and reconciliation process.

5.7 FNM_MAC_EXT.1 MAC Address Network Access Control

5.7.1 *Class and Family Information*

This extended component is part of the class “FNM: Network Management Security” and the family “Network Access Control (FNM_MAC)”.

5.7.1.1 Family Behavior

This family defines the requirements for the TSF to perform basic network access control based on a client’s MAC address. With regard to component leveling, this family contains only a single component.

5.7.2 *Management*

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

- Managing the MAC addresses used to make explicit access or denial based decisions.

5.7.3 *Audit*

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

- Minimal: Successful requests to gain network access.
- Basic: All requests to perform to gain network access.

5.7.4 *Definition*

FNM_MAC_EXT.1 MAC Address Network Access Control

Hierarchical to: No other components.

Dependencies: No dependencies.

FNM_MAC_EXT.1.1 The TSF shall allow or deny a network client's request for a dynamic IP address based on the client's MAC address.

FNM_MAC_EXT.1.2 The TSF shall enforce the following rules to determine if a client's request for an IP address is allowed: ***[assignment: network access control rules].***

5.7.5 *Rationale*

FNM_MAC_EXT.1 was based on the first two sub-components of FDP_ACF.1. This component needed to be explicitly defined since the TOE performs a very limited form of network access control, based solely on the MAC address of clients requesting a dynamic IP address (and therefore, access to the network). The entire suite of FDP_ACC, FDP_ACF, FMT_MSA.1 and FMT_MSA.3 SFRs as defined in CC Part 2 is not applicable to the operation of the TOE.

6 Security Requirements

6.1 Security Functional Requirements

Conventions
The following conventions have been applied in this document:

- **Security Functional Requirements** – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter or number in parenthesis placed at the end of the component. For example, FDP_ACC.1 (1) and FDP_ACC.1 (2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, 1 and 2.
  - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., ***[assignment]).***
  - **Selection**: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., ***[selection]***).
  - **Refinement**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.

- **Application notes** provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

- **Explicitly stated Security Functional Requirements** (i.e., those not found in Part 2 of the CC) are identified "_EXT" in the component name.

The TOE security functional requirements are listed in Table 6-1. All SFRs are based on requirements defined in Part 2 of the Common Criteria and the extended components defined in Section 5 of this ST.

Table 6-1: TOE Security Functional Components

No.	Component	Component Name
1	FAU_ARP_EXT.1	Event alarms
2	FAU_GEN.1	Audit data generation
3	FAU_SAR.1	Audit review
4	FAU_SAR.2	Restricted audit review
5	FAU_SAR.3	Selectable audit review
6	FAU_STG.1	Protected audit trail storage
7	FIA_ATD.1	User attribute definition

No.	Component	Component Name
8	FIA_UAU_EXT.2	User authentication before any action
9	FIA_UID.2	User identification before any action
10	FMT_MTD.1	Management of TSF data
11	FMT_SMF.1	Specification of Management Functions
12	FMT_SMR.1	Security roles
13	FPT_ITT.1	Basic internal TSF data transfer protection
14	FPT_STM.1	Reliable time stamps
15	FTA_SSL.3	TSF-initiated termination
16	FNM_NEA_EXT.1	DHCP Threshold Alerts
17	FNM_SEC_EXT.1	DNSSEC Deployment
18	FNM_NDR_EXT.1	Network Discovery and Reconciliation
19	FNM_MAC_EXT.1	MAC Address Network Access Control (MAC Address Filtering)

6.1.1 *Class FAU: Security Audit*

6.1.1.1 FAU_ARP_EXT.1 Event alarms

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_ARP_EXT.1.1 The TSF shall ***[issue an SNMP trap, e-mail the administrator]*** upon detection of ***[an administrator selected audit event].***

6.1.1.2 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:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the ***[not specified]*** level of audit; and
c) ***[the events listed in Table 6-2].***

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 (if applicable); and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***[transaction ID or event ID]***.

Table 6-2: Auditable Events

Component	Event
FAU_ARP_EXT.1	Actions taken due to detected events
FAU_GEN.1	None
FAU_SAR.1	None
FAU_SAR.2	None
FAU_SAR.3	None
FAU_STG.1	None
FIA_ATD.1	None
FIA_UAU_EXT.2	All use of the user authentication mechanism
FIA_UID.2	All use of the user identification mechanism
FMT_MTD.1	All modifications to the values of TSF data
FMT_SMF.1	Use of the management functions
FMT_SMR.1	Modifications to users' roles, privileges and access rights Modifications to user groups'
FPT_ITT.1	None
FPT_STM.1	Changes to the system time through NTP
FTA_SSL.3	Termination of an interactive session (logout)
FNM_NEA_EXT.1	Events triggered by the DHCP Alert Settings: either HD-Ratio Low Watermark or HD-Ratio High Watermark is reached
FNM_SEC_EXT.1	Events related to the automatic generation of DNSSEC Zone Signing Keys and Key Signing Keys: DNSSEC Signing Policy applied, Key Signing Key was generated/deleted, DNSSEC Key was generated/deleted , Zone Signing Key was generated/deleted
FNM_NDR_EXT.1	Events related to the reconciliation of IP addresses: start and stop of Reconciliation Service.
FNM_MAC_EXT.1	Result of client request (allow or deny)

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 ***[user role as specified in Table 6-3]*** with the capability to read ***[audit information as specified in Table 6-3]*** from the audit records.

Table 6-3: Audit Review

User Role	Audit Information
Administrators	All Audit Trail Information
	Event List
	Transaction History
	Server Logs
	System Logs
	Database Logs

User Role	Audit Information
Non-Administrators with *View History List* History Privilege	Transaction information about allowed Proteus Objects in related Audit Trails

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.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 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 ***[sorting]*** of audit data based on ***[displayed data field].***

6.1.1.6 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 audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to ***[prevent]*** unauthorised modifications to the stored 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***
- ***Proteus authentication password***
- ***External Authenticator Assignment***
- ***E-mail Address***
- ***Lock Mode***
- ***User Type***
- ***Security Privilege***
- ***History Privilege***
- ***Access Type***
- ***Group Assignments***

].

6.1.2.2 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 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.

6.1.2.3 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_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[perform the operations specified in Table 6-4]*** the ***[TSF data as specified in Table 6-4]*** to ***[user security role as specified in Table 6-4].***

Table 6-4: Management of TSF data

User Security Roles	Operations	TSF Data
Administrator Role	Create	Acceptance Criteria (for automatic reconciliation of network discovery data)
	Add, edit, delete, view, assign user to	Authenticator (external authentication)
	Download, view, delete	Database logs
	Configure	DHCP Alerts
	Configure, apply, view	DNSSEC signing policy
	View	Event list
	Enable, disable	IP overlap detection
	Add, edit, delete	IPv4 reconciliation policy (includes discovery)
	Add, edit, delete	IPv6 reconciliation policy (includes discovery)
	Add, edit, delete, view	Notification groups (includes alert configuration)
	Download, view	Proteus server logs
	Add, edit, delete, view	Proteus user accounts
	Configure	Session time-out
	Download, Apply	Software Updates *
	Download, view	Syslogs
	View	System information
	Add, edit, delete, view, assign user to	User groups
	View	User session details
	Lock, unlock	User sessions
	Reconcile	IPv4 addresses
	View, run	IPv4 reconciliation policy (includes discovery)
	Reconcile	IPv6 addresses
	View, run	IPv6 reconciliation policy (includes discovery)
	Perform xHA failover	xHA pair
Administrator Role **or** **Non-Administrator (with applicable access rights and privileges for object)**	Update	IP address state
	Assign	IPv4 addresses
	View	IPv4 addresses
	Manage	IPv4 blocks
	Manage	IPv4 networks
	Assign	IPv6 addresses
	View	IPv6 addresses
	Manage	IPv6 blocks

User Security Roles	Operations	TSF Data
	Manage	IPv6 networks
	View	Transaction history
	Add, edit, delete, view	User access rights
	Configure, view	xHA details
	View	xHA server logs
	View, configure, enable	Adonis monitoring
	Add, edit, delete, view, connect to, issue commands to, configure services for, disable, enable, replace	Adonis server
	Add, edit, delete, view	Adonis server deployment options
	Add, edit, delete, view	Adonis server interfaces
	View	Adonis server logs, performance metrics, running services status
	View	Adonis statistics
	View	Audit trail
	Add, edit, delete, view, add DHCP options to	Configurations (network implementation)
	Configure, enable	Data checking feature
	Configure	DDNS between Adonis appliances
	View	Deployment status
	Enable, disable	Deployment validation options
	Add, assign	Device type
	Add, edit, delete, view	DHCP deployment roles (DHCPv6 and DHCPv4)
	View	DHCP lease history
	Add, edit, delete, view, merge, resize	DHCP range
	Configure	DHCP settings (DHCPv6 and DHCPv4)
	Add, edit, delete, view	IPv4 Network Templates
	Add, edit, delete, view	DHCP zone groups
	Add, edit, delete, view	DHCP zones
	Add, edit, delete, view, add options	DNS deployment options
	Add, edit, delete, view	DNS deployment roles
	Add, edit, delete, view	DNS response policies
	Add, edit, delete, view	DNS view
	Add, edit, delete, view	DNS zones
	Configure	DNS64 settings
	Add, edit, delete, view	ENUM zones
	Add, edit, delete, view	External host objects
	Add, edit, delete, view	Internal root zone
	Add, edit, delete, view	MAC pools
	Deploy manually	Managed server data
	Add, edit, delete, view	Naming restrictions
	Add, assign	Object tag
	Change	Own password

User Security Roles	Operations	TSF Data
	View, configure, enable	Proteus monitoring
	Add, edit, delete, view	Reports
	Add, edit, delete, view	Resource records
	Add, edit, delete, view	Scheduled deployments
	Modify	Start of Authority (SOA) deployment option
	Add	Tag group
	Add, edit, delete, view	Tasks
	Define	TSIG key
	Configure	Zone Transfers between Adonis appliances

**Application Note: The software update management function is included in the TOE; however, the customer must be warned that after application of the update, the product will not be in the evaluated configuration. The customer must receive an update file and public security key file from the BlueCat Customer Care portal, before the new software can be applied. The public security key is used to verify the validity of the update file and must be checked after downloading an update file.*

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: ***[as specified in Table6-4].***

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***
- ***Non-Administrator***

].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: In addition to user roles, the TOE maintains privileges and access rights for each user, which controls the user's access to TSF data and management functions.

6.1.4 *Class FPT: Protection of the TSF*

6.1.4.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT.1.1 The TSF shall protect TSF data from ***[disclosure, modification]*** when it is transmitted between separate parts of the TOE.

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.

Application Note: The TSF can provide reliable time for its own use when Proteus NTP services are configured.

6.1.5 *Class FTA: TOE Access*

6.1.5.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a ***[administrator assigned time interval of user inactivity].***

6.1.6 *Class FNM: Network Management Security*

6.1.6.1 FNM_NEA_EXT.1 DHCP Threshold Alerts

Hierarchical to: No other components.

Dependencies: No dependencies.

FNM_NEA_EXT.1.1 The TSF shall ***[issue an SNMP trap, e-mail a designated user]*** upon detection of a DHCP range above or below an administrator defined threshold.

6.1.6.2 FNM_SEC_EXT.1 DNSSEC Deployment

Hierarchical to: No other components.

Dependencies: No dependencies.

FNM_SEC_EXT.1.1 The TSF shall provide a communication path between itself and a DNSSEC enabled client (DNS resolver) that is logically distinct from other communication paths.

FNM_SEC_EXT.1.2 The TSF shall support all the required resource records needed to provide DNSSEC functionality for hosted authoritative domains

FNM_SEC_EXT.1.3 The TSF shall sign all records hosted on the TOE's authoritative DNS server component using a cryptographic key to produce a digital signature.

FNM_SEC_EXT.1.4 The TSF shall provide support for DNSSEC Signed Zones using Zone Signing Keys (ZSK) and Key Signing Keys (KSK).

FNM_SEC_EXT.1.5 The TSF shall provide support for DNSSEC Trust Anchors

FNM_SEC_EXT.1.6 When the DNS resolver requests a DNS record, the TSF shall also provide the DNS resolver with a digital signature of the record that was created by the cryptographic key.

FNM_SEC_EXT.1.7 The TSF shall support the use of NIST default parameter settings for zone signing.

FNM_SEC_EXT.1.8 The TSF shall support the use of administrator configured schedules and key rollover settings for automated KSK and ZSK re-signing.

FNM_SEC_EXT.1.9 When the TOE is acting as a DNS client, the TSF shall use DNSSEC standards to validate signatures from other DNSSEC servers.

6.1.6.3 FNM_NDR_EXT.1 Network Discovery and Reconciliation

Hierarchical to: No other components.

Dependencies: No dependencies.

FNM_NDR_EXT.1.1 The TSF shall provide the ability to run discovery scans of authorized administrator defined ranges of the managed network and collect at least the following information from each network host:

- IP address
- MAC address
- Network router connected to host
- DNS host name (if DNS is available)

FNM_NDR_EXT.1.2 The TSF shall provide the ability to run discovery scans at authorized administrator scheduled times and immediately on authorized administrator command.

FNM_NDR_EXT.1.3 TSF shall analyze all network data collected and report the following discrepancies between the scan data and the network data stored in the TOE:

- IP address exists on the physical network, but not in the TOE
- IP address exists in the TOE but not on the physical network (IPv4 only)
- IP address exists in both the TOE and on the network, but the MAC address or DNS host name information does not match (IPv4 only)

FNM_NDR_EXT.1.4 The TSF shall provide authorized users with the capability to read the discovery scan information and analysis results.

FNM_NDR_EXT.1.5 The TSF shall provide the discovery scan information and analysis results in a manner suitable for the authorized users to interpret the information.

FNM_NDR_EXT.1.6 The TSF shall provide authorized administrators the ability to perform the following reconciliation actions:

- reconcile all addresses
- reconcile selected addresses
- delete addresses
- enable/disable automatic reconciliation (IPv4 only)
- view all addresses (IPv4 only)
- view non-reconcilable addresses (IPv4 only)
- add addresses to the override list (IPv4 only)

FNM_NDR_EXT.1.7 The TSF shall be able to perform the discovery and reconciliation process for both IPv4 and IPv6.

6.1.6.4 FNM_MAC_EXT.1 MAC Address Network Access Control (MAC Address Filtering)

Hierarchical to: No other components.

Dependencies: No dependencies.

FNM_MAC_EXT.1.1 The TSF shall allow or deny a network client's request for a dynamic IP address based on the client's MAC address.

FNM_MAC_EXT.1.2 The TSF shall enforce the following rules to determine if a client's request for an IP address is allowed: ***[***

CASE Allow:

If the 'Allow MAC Pools' option is set, and the client's MAC address matches an entry in an Allow MAC Pool, the request is allowed, otherwise the request is denied.

CASE Deny:

If the 'Deny MAC Pools' option is set, and the client's MAC address matches an entry in a Deny MAC Pool, the request is denied, otherwise the request is allowed.

CASE Deny Unknown:

If the 'Deny Unknown MAC Addresses' option is set, and the client's MAC address is unknown to the TSF (i.e. not DHCP Reserved status), the request is denied, otherwise the request is allowed.

Default:

All requests allowed (no MAC pool defined)

].

Application Note: The three cases are mutually exclusive. If none of the three apply, all requests are allowed.

6.2 Security Assurance Requirements for the TOE

This Section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL 2 augmented with ALC_FLR.1. None of the assurance components is refined. Table 6-5 summarizes the components.

Table 6-5: EAL2+ Assurance Components

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Architectural Design with Domain Separation and non-bypassability
	ADV_FSP.2	Security enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability Analysis

6.3 Security Requirements Rationale

6.3.1 *Dependencies Satisfied*

Table 6-6 shows the dependencies between the functional requirements including the extended components defined in Section 5. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. All dependencies have been satisfied.

Table 6-6: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_ARP_EXT.1	Event alarms	FAU_GEN.1	2
2	FAU_GEN.1	Audit data generation	FPT_STM.1	14
3	FAU_SAR.1	Audit review	FAU_GEN.1	2
4	FAU_SAR.2	Restricted audit review	FAU_SAR.1	3
5	FAU_SAR.3	Selectable audit review	FAU_SAR.1	3
6	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	2
7	FIA_ATD.1	User attribute definition	None	N/A
8	FIA_UAU_EXT.2	User authentication before any action	FIA_UID.1	9 (H)
9	FIA_UID.2	User identification before any action	None	N/A
10	FMT_MTD.1	Management of TSF data	FMT_SMF.1	11
11	FMT_SMF.1	Specification of Management Functions	None	N/A
12	FMT_SMR.1	Security roles	FIA_UID.1	9 (H)
13	FPT_ITT.1	Basic internal TSF data transfer protection	None	N/A
14	FPT_STM.1	Reliable time stamps	None	N/A
15	FTA_SSL.3	TSF-initiated termination	None	N/A
16	FNM_NEA_EXT.1	DHCP Threshold Alerts	None	N/A
17	FNM_SEC_EXT.1	DNSSEC Deployment	None	N/A
18	FNM_NDR_EXT.1	Network Discovery and Reconciliation	None	N/A
19	FNM_MAC_EXT.1	MAC Address Network Access Control (MAC Address Filtering)	None	N/A

6.3.2 *Functional Requirements*

Table 6-7 traces each SFR back to the security objectives for the TOE.

Table 6-7: Requirements vs. Objectives Mapping

	O.ACCESS	O.ALERTS	O.AUDIT_PROTECT	O.AUDITS	O.DNSSEC	O.EADMIN	O.IDAUTH	O.NETWORK_ACCESS	O.NETOWRK_ANALYZE	O.PROTECT_COMM	O.SYSDATA	O.SYSDATA_PROTECT
FAU_ARP_EXT.1		X										
FAU_GEN.1				X								
FAU_SAR.1						X						
FAU_SAR.2	X		X									X
FAU_SAR.3						X						
FAU_STG.1			X									X
FIA_ATD.1	X						X					
FIA_UAU_EXT.2							X					
FIA_UID.2							X					
FMT_MTD.1	X					X						
FMT_SMF.1						X						
FMT_SMR.1	X											
FPT_ITT.1										X		
FPT_STM.1				X								
FTA_SSL.3							X					
FNM_NEA_EXT.1		X										
FNM_SEC_EXT.1					X					X		X
FNM_NDR_EXT.1						X			X		X	
FNM_MAC_EXT.1						X		X			X	

The following discussion provides detailed evidence of coverage for each security objective:

O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data.

This objective is covered by the role-based access to the administrative functions and TSF data enforced by the TOE. The administrative functions supplied by the TOE are restricted to the user roles, permissions and access rights as specified in FMT_MTD.1. FAU_SAR.2 restricts access to the audit records through the TOE's interfaces. The

user roles as specified in FMT_SMR.1 are maintained by the TOE along with other user attributes that restrict access as defined in FIA_ATD.1.

O.ALERTS: The TOE must be able to notify administrative personnel of security significant events.

This objective is covered by FAU_ARP_EXT.1, which specifies that an administrator can enable alerts when a security relevant event occurs, and FNM_NEA_EXT.1, which can send an alert when a DHCP Threshold is met.

O.AUDIT_PROTECT: The TOE must protect its audit data from unauthorized access and modifications.

The audit information that is stored in the TOE is protected by the FAU_STG.1 functionality. FAU_SAR.2 protects the audit information from being viewed by unauthorized personnel.

O.AUDITS: The TOE must record audit records for data accesses and use of the system functions.

Audit information is generated by the TOE as described in FAU_GEN.1. The TOE supports the generation of audit records by being able to supply reliable time for its own use as specified in FPT_STM.1.

O.DNSSEC: The TOE must protect communications between the TOE components and clients using the TOE's DNS services in accordance with DNSSEC standards.

The TOE's support of DNSSEC specifications is defined in FNM_SEC_EXT.1.

O.EADMIN: The TOE must include a set of functions that allow effective management of its functions and data.

The administrative functions of the TOE are specified in FMT_SMF.1 and FMT_MTD.1. More information about the audit review functions of the TOE are given in FAU_SAR.1 and FAU_SAR.3. FNM_NDR_EXT.1 specifies administrator functionality that applies to the TOE's discovery and reconciliation functionality. While FNM_MAC_EXT.1 supplies more details about the management functions used in the MAC address network access control functionality of the TOE.

O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

User attributes, including those used for identification and authentication are defined in FIA_ATD.1. FIA_UAU_EXT.2 and FIA_UID.2 define the identification and authentication functionality supplied by the TOE. Finally, FTA_SSL.3 protects the TOE from unauthorized access by terminating a user session after a defined period of inactivity.

O.NETWORK_ACCESS: The TOE must control access to the protected network based on the attributes of the clients using the TOE's DHCP services.

The two types of basic network access control performed by the TOE and based on a client's MAC address are specified in FNM_MAC_EXT.1.

O.NETWORK_ANALYZE: The TOE must be able to analyze collected network data to find differences in the network configuration.

The TOE's network discovery and reconciliation process, which finds changes to the managed network's configuration, is defined in FNM_NDR_EXT.1.

O.PROTECT_COMM: The TOE must protect data transmitted between separate parts of the TOE.

Communications between TOE components (between the Proteus and Adonis appliances, and between two Adonis appliances) is protected by the functionality of FPT_ITT.1. DNS information is protected when in transit between the Proteus and Adonis by the DNSSEC functionality of FNM_SEC_EXT.1.

O.SYSDATA: The TOE must collect data from network clients and devices to use for network management.

The data collected and used for the TOE's network discovery and reconciliation functionality is specified as in FNM_NDR_EXT.1. The data used for network access control is described in FNM_MAC_EXT.1.

O.SYSDATA_PROTECT: The TOE must protect the data it collects from network clients and devices from unauthorized access and modifications.

The collected data stored in the various logs maintained by the TOE is protected by the same mechanisms used for the audit data generated by the TOE. This functionality is defined in FAU_STG.1 and FAU_SAR.2. In addition, DNS data is protected by the DNSSEC support procedures defined in FNM_SEC_EXT.1.

6.3.3 *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. At EAL *2*, the TOE will have incurred a search for obvious flaws to support its introduction to the non-hostile environment.

7 TOE Summary Specification

7.1 IT Security Functions

Section 7 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 1.4.8 Logical Scope of the TOE. The following sub-sections describe how the TOE meets each SFR listed in Section 6.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Functions	Sub-Functions	SFRs
Security Audit	AU-1 Event Alarms	FAU_ARP_EXT.1
	AU-2 Audit Generation	FAU_GEN.1
	AU-3 Audit Review	FAU_SAR.1
		FAU_SAR.2
		FAU_SAR.3
	AU-4 Audit Protection	FAU_STG.1
User I&A	IA-1 User Security Attributes	FIA_ATD.1
	IA-2 User Identification & Authentication	FIA_UAU_EXT.2
		FIA_UID.2
Security Management	SM-1 Management Functions	FMT_MTD.1
		FMT_SMF.1
	SM-2 Management Security Roles	FMT_SMR.1
Protection of Security	PT-1 Internal Data Transfer Protection	FTP_ITT.1
	PT-2 Time Stamps	FTP_STM.1
TOE Access	TA-1 Session Time-Out	FTA_SSL.3
Network Management	NM-1 DHCP Threshold Alerts	FNM_NEA_EXT.1
	NM-2 DNSSEC Deployment	FNM_SEC_EXT.1
	NM-3 Network Discovery and Reconciliation	FNM_NDR_EXT.1
	NM-4 MAC Address Network Access Control	FNM_MAC_EXT.1

7.1.1 *Security Audit Functions*

7.1.1.1 AU-1: Event Alarms

(FAU_ARP_EXT.1)

The Event List provides a record of system events and is available only to users with the Administrator Role on the Administration page of the Proteus WebUI. The Event List logs events generated by TOE services, as well as events generated by the Proteus application itself.

Proteus administrators can be notified of events through the configuration of Notification Groups and Event Level Subscriptions. An SNMP trap can be triggered by an event, or users can be notified by e-mail message when certain events occur. Adonis can send SNMP traps over both IPv4 and IPv6. Proteus only supports SNMP traps over IPv4.

The Event List includes the following types of events:

- *Application*—events related to the operation of the Proteus software.
- *Deployment Service*—events related to deploying data to Adonis servers managed by Proteus.
- *Data Check Service*—events related to the Data Checker service as it reviews data within configurations.
- *DHCP Alert Service*—events triggered by the DHCP Alert Settings.
- *Database Maintenance Service*—events related to the Database Replication, History reflected Archive and Purge, Database Cleaner, and Database Re-index functions.
- *IP Reconciliation Service*—events related to the reconciliation of IP addresses through the IP Reconciliation function.
- *Monitoring Service*—events related to the Proteus-managed servers through the service.
- *DNSSEC Auto Generate Key Service*—events related to the automatic generation of DNSSEC Zone Signing Keys and Key Signing Keys.
- *xHA*—events related to the function of servers in an xHA pair.

Note: The Event List can also include events related to features that are not included in the scope of the evaluation such as Proteus managed Window servers or workflow events.

Alarms can be set for any of these events.

AU-1: Event Alarms require an SNMP and/or SMTP server in the Operational Environment to send the alarms.

7.1.1.2 AU-2: Audit Generation

(FAU_GEN.1)

The TOE maintains several logs of audit information about security relevant events.

The *Event List* provides a record of system events. The Event List logs events generated by the TOE services, as well as events generated by the Proteus application itself. Events logged in the list include a unique tracking ID, the message issued, the user's name, and the date and time the event occurred. The events included in the Event List are stored in the Proteus database.

The *Transaction History* / *Audit Trail* records transaction details. Audit Trail Information is part of Transaction History and is related to a particular Proteus object. Each record contains the following fields:

- *Operation*—a descriptive phrase describing the transaction.
- *User*—the name of the user who performed the transaction.
- *Time*—the date and time that the transaction occurred.
- *Transaction Number*—a unique identification number for the transaction.
- *Details*— transactions details which can be viewed on a separate web page and include:
    - A *General* section that provides general information about the transaction:
        - *Operation*—a description of the operation performed
        - *Comment*—the change control comments entered for the transaction
        - *Time*—the date and time of the transaction
        - *Transaction Number*—the unique identification number for the transaction
    - A *History Details* section that lists details for each object affected by the transaction:
        - *Action*—the action performed
        - *Object Type*—the type of object or objects affected by the transaction
        - *Details*—details describing the affected object
        - *Object ID*—the unique identification number for the object

The events included in the Audit Trail are also stored in the Proteus database.

Other Proteus logfiles include:

- *Server Logs* - event logs for the Proteus application. Administrators can set the logging levels for the Proteus server
- *System Logs* - Proteus operating system events, Proteus database events, and, when it is enabled, the replication service (syslog)

Adonis logfiles include:

- *Server Logs* - event logs for the Adonis application
- *System Logs* - event logs for Adonis operating system events (syslog)

These logfiles are stored on the file system of the appliances' OS.

On both Adonis and Proteus, the syslog can be redirected to an external syslog server via the CLI. The audit data that is redirected to the external server can be configured with user created filters.

Note: This redirection functionality is necessary for many potential DOD/NSA customers and therefore will be included in the tested configuration.

Startup / Shutdown of Auditing

The Event List and Transaction History / Audit Trail become available / unavailable when the Proteus Server service starts up /shuts down. There are messages in the Proteus Server Logs that are specific for startups and shutdowns of the Proteus Server service and therefore can be considered equivalent to logging the startup and shutdown of the audit logging functionality.

The shutdown of Proteus Server service is reflected with the following messages in the log file '/opt/jboss/server/proteus/log/server.log' (also reachable through link '/var/log/jboss.log'):

> <timestamp> INFO [com.arjuna.ats.jbossatx.jta.TransactionManagerService] Stopping transaction recovery manager
>
> <timestamp> INFO [com.arjuna.ats.jbossatx.jta.TransactionManagerService] Destroying TransactionManagerService

The startup of Proteus Server service is reflected with the following messages in same log file ('/opt/jboss/server/proteus/log/server.log'):

> <timestamp> INFO [com.arjuna.ats.jbossatx.jta.TransactionManagerService] Binding TransactionManager JNDI Reference
>
> <timestamp> INFO [com.arjuna.ats.jbossatx.jta.TransactionManagerService] Starting transaction recovery manager

When the Auditd daemon is enabled, the TOE also generates a specific audit.log file, which contains messages related to startups and shutdowns of the Proteus Server. Every startup and shutdown of the Proteus Server creates numerous related messages in the /var/log/audit/audit.log file. The Proteus Server service has hundreds of sub-processes and each sub-process' startup and shutdown is reflected with log messages. However, these messages:

- are in RAW format (exactly as the kernel sends them);
- are almost not human readable;
- only correspond to particular sub-processes, i.e. there are no separate messages explicitly saying that entire Proteus Server service has started up or shut down.

Example of the log messages generated by shutdown of sub-process 'RenameResourceRecord.page':

> type=SYSCALL msg=audit(<timestamp>): arch=40000003 syscall=10 per=400000 success=yes exit=0 a0=9fb9a48 a1=9bdad10 a2=b8007ff4 a3=9fb9a48 items=2 ppid=2865 pid=3105 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="java" exe="/usr/lib/jvm/java-6-sun-1.6.0.20/jre/bin/java" key=(null)

type=CWD msg=audit((<timestamp>): cwd="/"
type=PATH msg=audit((<timestamp>): item=0 name="/opt/jboss-5.1.0.GA/server/proteus/tmp/4su1c37-jvlekw-gvwndbhq-1-gvwnemh3-1l/proteus-html-HEAD.war/WEB-INF/page/dns/resource/" inode=188340 dev=08:02 mode=040755 ouid=0 ogid=0 rdev=00:00
type=PATH msg=audit((<timestamp>): item=1 name="/opt/jboss-5.1.0.GA/server/proteus/tmp/4su1c37-jvlekw-gvwndbhq-1-gvwnemh3-1l/proteus-html-HEAD.war/WEB-INF/page/dns/resource/RenameResourceRecord.page" inode=190019 dev=08:02 mode=0100644 ouid=0 ogid=0 rdev=00:00

AU-2: Audit Generation may depend on an NTP server in the Operational Environment to provide reliable time stamps if Proteus NTP services are not configured.

7.1.1.3 AU-3: Audit Review

(FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

The management interfaces of the TOE allow only users who have the appropriate authorizations to view security audit data for the system.

The Proteus Audit Trail displays transactions that have occurred within the context being viewed in the WebUI. This means that if a page is used at the configuration level, it displays transactions that have occurred within the context of that configuration. If a particular subnet is being modified, the Audit Trail page for that object lists only transactions that have occurred within the context of that particular subnet. The Transaction History / Audit Trail fields displayed on the WebUI are described in Section 7.1.1.2: AU-2: Audit Generation. Only users with the “Administrator” role or users with the “Non-Administrator” role plus the “History” privilege may view the Audit Trail.

The Event List can be viewed by users with the “Administrator” role on the Administrator page of the WebUI. Besides a display of the Event Log data fields, icons indicate the status of items in the Event List (a successfully completed event, an informational item, or a warning or error condition).

Proteus users with the “Administrator” role or the “Non-Administrator” role with the “View” privileges for the Adonis Audit object can view the Adonis Audit Logs from the Proteus WebUI.

On the Log Management page of the WebUI, users with the appropriate roles and permissions can download and view the TOE audit data. The permission necessary to review the audit data varies with the type of log in which that data is recorded (Proteus server log, syslog, database log …).

All logs are displayed in a tabular format. Users can sort the logs by clicking on the column header for any field.

7.1.1.4 AU-4: Audit Protection

(FAU_STG.1)

The audit records are protected by the access control functionality of the Proteus' PostgreSQL database and the hardened Linux-based operating system installed on the Proteus and Adonis appliances. The only way to access the audit data (logfiles) directly is through the appliances' OS (the Linux shell) and having 'root' privileges. The TOE provides protection for the security audit records primarily by role based access control enforced on the WebUI and requiring successful identification and authentication prior to providing any functionality to the user. The WebUI provides no functionality to modify or delete the audit trail.

For logfiles generated by Proteus services, the following rules are implemented in the TOE:

- Each logfile has a maximum default size of 10 Mb
- Once this size limit is exceeded, the current logfile is closed, compressed, and stored on the OS file system and a new logfile is created
- The default number of backup logfiles allowed for each log type is 4. Once the fifth backup logfile is created, the oldest file is deleted.

Both Proteus and Adonis logfiles can be redirected to an external Syslog Server for protection of the audit information.

To prevent loss of audit data, the customer should use the TOE's ability to offload audit records to an external Syslog server in the Operational Environment. The TOE also supports an administrative function that allows for the manual downloading of audit trails for off appliance long-term storage.

Note: There is no automatic warning for the deletion of logfiles currently implemented in the TOE. There is a SNMP based Monitoring Service implemented in Proteus that allows monitoring of the disk utilization percentage in both Proteus and attached Adonis servers. Administrators are allowed to add and manage shell scripts that generate e-mail alerts or SNMP traps in case of low disk space.

7.1.2 *User I&A Functions*

7.1.2.1 IA-1: User Security Attributes

(FIA_ATD.1)

User account information is stored in the TOE and contains the following attributes:

- *Username*
- *Proteus Password* – used for user authentication by the TOE

  Note: A hash of the Proteus Password is stored. The TOE does not store passwords in the clear.

- *External Authenticator Assignment* - Default uses the native password based authenticator. An administrator can assign an external authenticator to each individual

user. When the user account is created or modified, the administrator selects the "Other" checkbox under Authentication subsection and then selects the appropriate authenticator from the dropdown list to the right of the checkbox to assign the authenticator. The dropdown list only reflects those authenticators that have been configured into Proteus already.

- *E-mail Address* – E-mail address Proteus uses for notifications to this particular user account.

- *Lock Mode* – flag that allows the administrator to lock or unlock a user from gaining access to Proteus without having to remove the user. A locked user cannot gain access. If the user is logged in when their account is locked, they are logged out of Proteus. If there is active session with the user whose account has just been locked, Proteus will terminate that session (log that user out) immediately and block any further login attempts until the account is unlocked by an administrator.

- *User Type* – the user role, which determines the functions to which a Proteus user has access. Values:
    - *Administrator*
    - *Non-Administrator*

- *Security Privilege* – controls users' ability to view and set access rights (All privileges are cumulative, meaning that each more permissive privilege includes the abilities of the less permissive levels.) Values:
    - *No Access* – users cannot view or change access rights or overrides
    - *View My Access Rights* – users can view only their own access rights and overrides
    - *View Other's Access Rights* – users can view all access rights and overrides
    - *Change Access Rights* – users can modify existing access rights and overrides within the scope of their own access rights
    - *Add Access Rights* – users can add new access rights and overrides
    - *Delete Access Rights* – users can delete access rights and overrides
    - *Administrator* – users can perform any security privilege action, including adding and deleting users, as well as changing security privileges and audit trail privileges. Administrators are the only users that can view the "Administration" WebUI page.

- *History Privilege* – controls users' access to the transaction history in the Audit Trail. Values:
    - *Hide* – users cannot see the audit trail information
    - *View History List* – users can see the audit trail information

- *Access Type* - determines how the Proteus user can access Proteus. Values:
    - *GUI* – user can access the system only through the Proteus WebUI: these users cannot log in to the Proteus API (Application Programming Interface)
    - *API* – user can access the system only through the Proteus API: these users cannot log in to the Proteus WebUI

Note: The Proteus API is not included in the scope of the evaluation; therefore, the only access type that can be used is "GUI".

- *Group Assignments* – a list of groups to which the user is assigned

Proteus access rights can be assigned to both users and groups, and multiple rights can exist for the same object. A single user may have both an access right and multiple overrides on an object, while multiple users could also have access rights and overrides on the same object. Three rules determine a user's access rights for any object within Proteus:

- Administrators always have full control over any system object.
- The child object's access right takes precedence over any other rights assigned to any parent level object within the Proteus object hierarchy.
- In the case of conflicting access rights for an object, the most permissive access right always takes precedence.

See Section 7.1.3.2 SM-2: Management Security Roles for more information on object access rights.

7.1.2.2 IA-2: User Identification & Authentication

(FIA_UAU_EXT.2, FIA_UID.2)

Each individual must be successfully identified and authenticated with a username and password by the TSF before access is allowed to the TOE.

User identification and authentication by the TSF uses the security attributes of the user account described in Section 7.1.2.1 above. When identification and authentication data is entered, the TOE attempts to identify the applicable user account from the provided identity and if a match is found, the password provided is compared against that stored with the user account information. (*Note: The password stored is encoded; the TOE does not store passwords in the clear.*) If a user account cannot be associated with the provided identity or the provided password does not match that stored with the user account information, identification and authentication will fail. No access to the WebUI is allowed until successful identification and authentication of the user.

Proteus comes with a password based authentication subsystem. The password complexity must be administratively enforced, as the password complexity has no requirements enforced by the TOE (i.e. password length can be 1 character). The vendor highly recommends using the external authentication mechanism for the primary means of authenticating and using the native password authentication mechanism for an Administrator role user to allow for emergency access to the TOE if the external authentication mechanism is not available.

Alternately, the TOE can be configured to use an external authentication service for user identification and authentication.

Proteus also supports mixed-mode authentication through RADIUS, LDAP, TACACS+, Microsoft Active Directory, or Kerberos. (Different users can be authenticated by different authentication mechanisms.)

Before Proteus can exchange authentication information with a remote system, the authenticator must be defined and associated with a Proteus user. An Authenticator is a type of system object in Proteus that represents a connection to an external authentication system. That system's native safeguards apply for communications between it and Proteus. Proteus acts as a proxy client for the authentication system, validating the identity of a Proteus user without managing or validating the user's password or credentials. After the external authenticator validates the user, Proteus considers the user valid until the session closes or times out.

More than one authenticator can be added to a user, so that a secondary authenticator can be used if the primary authenticator is not available. Authenticators can be tested to confirm that Proteus can communicate with the external service.

The Authenticators page of the WebUI lets administrators add external authenticators to the Proteus system. Depending on the type of authenticator chosen, the Authenticators interface displays different text fields.

Proteus LDAP/TACACS+ Groups allow users from Lightweight Directory Access Protocol (LDAP) systems, such as Microsoft Active Directory or OpenLDAP, or from a TACACS+ authentication server to log in to Proteus. LDAP/TACACS+ Groups may be used when users are defined in another system without having to re-define those users in Proteus. When a user from an LDAP/TACACS+ group logs in to Proteus, the user is automatically added to the Proteus Users list with the default role of "non-administrator" assigned, and the LDAP/TACACS+ User column indicates that the user was created from an LDAP or a TACACS+ group. An administrator would have to edit the user to increase their privileges or roles.

IA-2: User Identification & Authentication relies on the Operational Environment to provide an external authentication service if this form of user authentication is configured. IA-2 also relies on the Operational Environment to provide secure communications between the TOE and the authentication server.

7.1.3 *Security Management Functions*

7.1.3.1 SM-1: Management Functions

(FMT_MTD.1, FMT_SMF.1)

The TOE requires user authentication before any actions can be performed through the TOE interfaces. Access to TSF data and management functions of the Proteus WebUI are restricted by a user's assigned role, privileges, and access rights, as specified in FMT_MTD.1 (see Section 6.1.3.1 FMT_MTD.1 Management of TSF data).

A detailed list of the menu options of the Proteus WebUI and the user account privileges (roles, privileges, access rights) needed to access each option is provided in the Proteus Administrator guidance [PADMIN].

Note: Both Proteus and Adonis appliances have an Administration Console which is a command line interface. These CLIs are used only for installation, initial configuration of the appliances and off-line maintenance and are therefore not included in the scope of the evaluation.

SM-1: Management Functions depends on the Operational Environment for a properly configured Web Browser to support the TOE's management interface.

7.1.3.2 SM-2: Management Security Roles

(FMT_SMR.1)

All users of the TOE have access to TSF data and management functions; therefore, they are considered administrators for the purposes of this evaluation. The terms "TOE user", "TOE administrator" and "authorized administrator" are used in this ST to refer collectively to all authorized TOE users.

The defined roles for TOE users are "Administrator" and "Non-Administrator".

Although there are only two defined user roles, access to the TSF data and functionality of the Proteus management functionality through the WebUI is fine-grained. Access is controlled not only by the users' roles, but also by their access rights and the privileges specified in Section 7.1.2.1 IA-1: User Security Attributes. Users also obtain access rights from the user groups to which they are assigned. Access rights assigned to the user group apply to all users in the group. Administrators can also assign access rights to users individually, if needed.

Proteus uses access rights, overrides, and privileges to control how users see and work with objects and information.

Information and settings in Proteus are handled as individual objects. An object contains information that describes the options and parameters defined for a setting or a managed IP or DNS item. Object types contain individual fields. Fields hold information about an object, such as display names, data values, and other attributes. Objects are arranged in a hierarchy, with parent objects grouping together child objects. Child objects may or may not inherit fields from their parent objects. Administrators can create user-defined fields for each object type to capture and track information associated with the object. Examples of objects include policies, groups, addresses, and zones.

Access rights and overrides control access to Proteus objects. Privileges control how users see and work with user access rights and object transaction histories.

- *Default Access Rights* are global access rights for a user or user group. Default access rights are used to set the general access policy for a user or group. Administrators can set overrides within the access right to fine tune access to different types of objects.

- *Object Access Rights* are local access rights for a particular Proteus object. Object access rights are used to control access to a specific object and any child objects it contains. For objects that contain child objects, administrators can set overrides within the access right to control access to the child objects. For example, an access right granting access to an IPv4 Block may have an override that prevents access to IPv4 Networks within the block.

- *Overrides* are part of a default access right or an object access right that controls access to child objects within an object. For example, an access right granting access to a DNS zone may have overrides that prevent access to resource records within the zone.

The following access rights and override levels can be applied to users and groups:

- *Hide* – users cannot see objects of this type
- *View* – users can see objects of this type but cannot make changes
- *Change* – users can see objects of this type and can make changes
- *Add* – users can see objects of this type and can make changes, add object of this type, and copy these objects
- *Full Access* – users have all available rights, including all those above plus the ability to delete objects

Note: If no access rights are selected for a user, the user is assigned the default right of Hide.

Access rights may be assigned to the LDAP group and to individual LDAP users. If there are multiple LDAP groups with differing access rights, and a user belongs to multiple groups, or if access rights are applied to a user in addition to those that the user inherits from the LDAP group, the user receives the most permissive access rights.

Note: The customer is advised to read the administrator guidance carefully to gain a full understanding of user roles, privileges, and access rights and how they interact with object access rights.

7.1.4 *Protection of Security Functions*

7.1.4.1 PT-1: Internal Data Transfer Protection

(FPT_ITT.1)

The TSF ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification.

Communications between the Proteus appliance and the Adonis appliances that it manages are secured with SSL. Administrators are able to specify an optional IPv6 address when communicating with Adonis for zone delegation and DNS. IPv6 support also includes SNMP and syslog services on both Proteus and Adonis.

The TOE includes support for SNMP v1, v2c, and v3 for monitoring. Adonis and Proteus appliances both default to SNMP v2c. The Adonis appliances and their managing Proteus appliance must use the same version of SNMP. Mismatched SNMP versions cause a Failed to connect status message to appear in Proteus.

These communications are configured during installation of the TOE. Secure communications is also implemented by mutual, certificate-based authentication which allows Proteus to verify the identity of an Adonis appliance (and vice versa) prior to establishing a connection with that appliance. The certificates are self-signed and generated within the TOE each time that the Proteus – Adonis connection is established; they are not hard-coded into the appliances. 128-bit encrypted communication sessions between the Proteus and Adonis appliances protect against packet snooping. A private connection between the Proteus and Adonis appliances (a dedicated management network) is not needed for secure communications. Although this configuration can be used, normally, the appliances run SSL over an existing, non-management network.

Communications between Adonis appliances for data replication between the two nodes of an xHA pair of Adonis appliances is secured by the following combination of TOE hardware and Operational Environment support:

- The dedicated port ETH1 is used on each Adonis to connect with sibling node;
- The two nodes are connected by direct cable in xHA;
- Both xHA nodes are installed in the same secure server room (See assumptions A.INSTALL and A.PHYSICAL).

The following table summarizes the cryptographic functions used by the TOE for protection of data transfers to and from the TOE appliances.

Table 7-2: Data Transfer Protection

Data Transmission Path	Cryptographic Protection
Proteus <-> Adonis	TLS v1.0 RSA with RC4-128-SHA encryption and RSA key exchange mechanism
SNMPv3 access to Adonis SNMPv3 access to Proteus	Authentication Type: SHA-1 (recommended) or MD5 Privacy Type: AES-128 (recommended) or DES
Browser <-> Proteus (Proteus WebUI)	TLS 1.0 (HTTPS) encryption; AES-256 with SHA1 message authentication and RSA key exchange mechanism

The following data transfers between Adonis:

- DNS Zone Transfers – transferring contents of DNS zones between Adonis appliances
- Dynamic DNS Updates – when an Adonis DHCP server sends updates to dynamic DNS data on another Adonis DNS server
- DNS query forwarding – DNS queries and DNS records returned in response

are implemented the same as the DNS and DHCP services the TOE provides for any external DNS Server. These are not considered internal communications between TOE components. These data transfers are covered by the DNS services that are managed by the administrative functions described in FMT_MTD.1 and protected by the TOE's DNSSEC functionality. See Section 7.1.6.2 for the details of DNSSEC algorithms.

PT-1: Internal Data Transfer Protection depends on the Operational Environment to secure the communications between Adonis appliances in an xHA pair.

7.1.4.2 PT-2: Time Stamps

(FPT_STM.1)

The Proteus appliance serves as an NTP (Network Time Protocol) server for time synchronization of the Adonis appliances. The Proteus appliance can be used as the sole timeserver for the TOE or an external NTP server may be used in the TOE configuration. When using an external NTP server, the Proteus appliance is a client of that server and the Adonis appliances are still clients of the Proteus for time synchronization.

Time synchronization between Adonis and Proteus is very critical for TOE to run properly, therefore direct connections between an external NTP server and the Adonis appliances is excluded from the TOE configuration. NTP services are also critical for synchronization of data between an xHA pair of Adonis appliances.

CLI commands allow an administrator to enable and disable the NTP service and configure the external NTP service. The administrators can also specify logging of the NTP service events.

The Adonis appliances that are managed by the Proteus server automatically obtain the time sync services of that Proteus server regardless of whether the Proteus server is configured to use an external NTP server or not.

7.1.5 *TOE Access Functions*

7.1.5.1 TA-1 Session Time-Out

(FTA_SSL.3)

Administrators can set a user session timeout value on the Global Settings pages of the Proteus WebUI. This is a global setting that will apply to all users of the Proteus WebUI. After a user session is inactive for the specified period of time, Proteus closes the user session (logs out the user). The default setting is 20 minutes.

7.1.6 *Network Management Functions*

7.1.6.1 NM-1: DHCP Threshold Alerts

(FNM_NEA_EXT.1)

DHCP Alerts notify an administrator that a DHCP range is above or below the defined watermarks. That is, when either too few or too many addresses contained in a range of addresses are being used (when compared to a defined value). If the number of free addresses in the range passes one of the thresholds or watermarks, Proteus can e-mail the administrator or issue an SNMP trap. DHCP Alert settings are configured globally. These settings are inherited by all IP blocks, networks, and DHCP ranges in any configuration. For DHCP alerts to be forwarded to users, the Event Notification Service must be configured. DHCP Alerts are configured through the Proteus WebUI.

NM-1: DHCP Threshold Alerts requires an SNMP and/or SMTP server in the Operational Environment to send the alarms.

7.1.6.2 NM-2: DNSSEC Deployment

(FNM_SEC_EXT.1)

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications 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 extensions to DNS, which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

DNSSEC is designed to protect DNS resolvers (clients) from forged DNS data, which occurs as the result of a DNS attack. DNSSEC secures DNS by signing all records hosted on the authoritative server using a cryptographic key to produce a digital signature. When a DNS resolver requests a DNS record, it also receives a digital signature of the record that was created by the cryptographic key. The resolver decrypts the signature using the associated public key to verify that the record it received is identical to the record on the authoritative server.

Please see NIST Special Publication (SP) 800-81, Secure Domain Name System (DNS) Deployment Guide, May 2006, for the details of DNSSEC specification.

Note: DNSSEC does not provide confidentiality of data. It provides a means to authenticate DNS responses, but does not encrypt the information.

The TOE supports all the required resource records needed to provide DNSSEC functionality for hosted authoritative domains including Resource Record Signatures (RRSIGs), DNSKEY, Next Secure (NSEC) Records, and Next Secure 3 Records (NSEC3).

The TOE provides the ability to configure Trust Anchors, which are used to validate responses from other authoritative name servers running DNSSEC signed zones. The TOE also supports

the configuration of DLVs (Designated-Lookaside-Validators), allowing administrators to configure a single address of a server, which contains many Trust Anchors.

The TOE provides full support for DNSSEC Signed Zones using Zone Signing Keys (ZSK) and Key Signing Keys (KSK). Zone Signing Keys are used to sign the record within a zone. Key Signing Keys are used to sign the keys themselves typically used outside the zone as the Trust Anchor. Within Proteus, both ZSKs and KSKs can be generated automatically using zone policies.

Administrators can configure a zone signing policy through the Proteus WebUI and apply it to any number of DNS zones. These policies allow the administrator to use Industry Standard National Institute of Standards and Technology (NIST) defaults for zone signing, or choose their own schedules to automate KSK and ZSK re-signing, and key rollover settings. Automated zone signing ensures that the zones are always signed and valid.

The TOE can also act as a DNS client, in which case DNSSEC is used to validate responses from other DNSSEC servers. The integrity and authenticity of returned DNS records are protected with DNSSEC. Every returned DNS record, including DS and DNSKEY records, is accompanied with unique RRSIG record, which is a digital signature for the DNS record. Every RRSIG record is created by security algorithm assigned in the DNSSEC policy. The following algorithms are available in DNSSEC policies:

- RSA/SHA1 (key lengths - 512, 1024, 1536, 2048, 2560, 3072, 3584, 4096)
- DSA/SHA1 (key lengths - 512, 1024)
- RSA/MD5 (key lengths - 512, 1024, 1536, 2048, 2560, 3072, 3584, 4096)
- RSASHA1-NSEC3-SHA1 (key lengths - 512, 1024, 1536, 2048, 2560, 3072, 3584, 4096)
- DSA-NSEC3-SHA1 (key lengths - 512, 1024)
- RSA/SHA256 (key lengths - 512, 1024, 1536, 2048, 2560, 3072, 3584, 4096) (both with and without NSEC3)
- RSA/SHA512 (key lengths - 1024, 1536, 2048, 2560, 3072, 3584, 4096) (both with and without NSEC3)

7.1.6.3 NM-3: Network Discovery & Reconciliation

(FNM_NDR_EXT.1)

IP address discovery and reconciliation discovers IPv4 and IPv6 addresses on the network and returns their host information to Proteus. After discovering the addresses on the network, administrators can add them to the Proteus configuration.

The discovery functionality can detect new devices on the network and MAC, IP, or name clashes. After finding addresses that have been newly added and recently removed from the network, the discovery tool also identifies conflicts based on DNS host name and MAC address. After discovery, the IP reconciliation functionality compares the changes to identify unused IP addresses for reclamation and help uncover unauthorized IP addresses that can create security vulnerabilities.

Proteus uses SNMP v1, v2c or encrypted SNMP v3 interrogation against one or more layer 2 or layer 3 routers and switches to discover the IP address, hardware address, and DNS host name (if DNS is available) for hosts on the network. The SNMP credentials are encoded and maintained in the Proteus database.

The TOE supports discovery for any router or switch that supports SNMP access and MIBs as follows:

- RFC1213 “MIB-II”
- RFC2863 “IF MIB”,
- RFC4188 “BRIDGE MIB”,
- RFC4292 “IP Forwarding Table MIB”
- RFC4293 “IP MIB”

Proteus displays the results on the Reconciliation Policy page on the Proteus WebUI. From this page, administrators can reconcile the IP addresses in Proteus with the discovered IP addresses. IP address discovery is controlled through an IP Reconciliation Policy. The policy includes address and SNMP information for a router, scheduling parameters to determine when and how often the discovery process runs, and other parameters. The discovery can run at scheduled intervals and on demand.

The steps for creating IP reconciliation processes, running them, and working with the results are similar for both IPv4 and IPv6 policies. However, there are minor differences in the options available and the information returned for IPv4 and IPv6 networks.

IPv4 Discovery and Reconciliation Process

IPv4 reconciliation policies can be created at the configuration, IPv4 block, or IPv4 network levels. When set and run at the configuration level, Proteus automatically creates blocks and networks based on the results of the network discovery, unless they are in conflict with existing blocks. A policy set at the configuration level requires specification of one or more network boundaries (ranges).

IPv4 reconciliation policies can be configured to enable (or disable) the automatic reconciliation process, which places any IP addresses found by the discovery process into the Proteus database automatically. Automatic reconciliation starts immediately after the discovery process returns all discovered IP addresses.

IPv4 reconciliation policies can also return layer 2 information for switches that use Cisco IOS version 10.3 or higher with Cisco Discovery Protocol (CDP). Link Layer Discovery Protocol (LLDP) is also supported. Layer-2 Discovery is not supported with SNMP v3.

Between discovery sessions, IP addresses on the physical network may be added or removed, resulting in addresses on the network differing from addresses in Proteus. In IPv4 Reconciliation, Proteus lists such addresses as one of three types:

- *Reclaimable IP Address*—an IP address that exists in Proteus, but not on the physical network. This may represent a device that was turned off at the time of the discovery, or the address may no longer exist on the network.

- *Unknown IP Address*—an IP address that exists on the physical network, but not in Proteus. This likely represents an address that has been added to the network since the last discovery.
- *Mismatched IP Address*—an IP address that exists in both Proteus and on the network, but where the MAC address or DNS host name information does not match.

After an IPv4 reconciliation policy discovery scan has been run, the following information can be viewed by the administrator:

- *IP Address*—lists the IP address.
- *Type*—an IP address may be of one of the following types:
    - *Mismatch*—an address that exists in both Proteus and on the network, but where the MAC address or DNS host name information does not match.
    - *Reclaimable*—an address that exists in Proteus, but it is not found on the physical network. This may represent a device that was turned off at the time of the discovery, or the address may no longer exist on the network.
    - *Unknown*—an address that exists on the physical network, but that is not in Proteus. This likely represents an address that has been added to the network after the last discovery.
- *Network*—the parent IP network object for the IP address.
- *FQDN*—the fully qualified domain name for the IP address.
- *MAC Address*—the MAC address of the IP address.
- *Overridden*—indicates if the address is exempt from the reconciliation process.
    - *No* indicates that the IP address is not added to the override list
    - *Yes* indicates that it is added to the override list.

  Overridden addresses are not affected by the Reconcile All and Reconcile functions.
- *Time Since First Detection*—the time since the address was first discovered by the IP reconciliation policy.

After viewing the discovery data, the administrator can perform the following reconciliation actions:

- Reconcile all addresses
- Reconcile selected addresses
- Delete addresses
- View all addresses
- View non-reconcilable addresses
- Add addresses to the override list

The reconciliation action performs the following:

- Unknown IP addresses are added to the Proteus database.
- Reclaimable IP addresses are removed from the Proteus database. The status of Reclaimable IP addresses are changed to “available” in the Proteus database
- Mismatched IP addresses are updated with the information from the most recent discovery operation, overwriting the mismatched data in Proteus. The only exception to this rule is if an IP address discovered on the network has a different DNS host name from the host name listed in Proteus. In this situation, Proteus creates a new host record for the IP address, resulting in multiple host records for the IP address.

Proteus may not be able to reconcile an address for one of the following reasons:

- There is a conflict between the size of the physical network and the size of the equivalent IP network object in Proteus. As a result, Proteus cannot add the address.
- The IP state between two discovery sessions does not match. For example, an earlier discovery session reported the address as Static; before the next discovery session, another user changes its state to Reserved.

The result of the reconciliation process can be viewed on the Reconciliation Summary page of the Proteus WebUI.

IPv6 Discovery and Reconciliation Process

IPv6 reconciliation policies are created at the IPv6 block or IPv6 network levels. When an IPv6 reconciliation policy is run, Proteus automatically builds IPv6 blocks and networks based on their physical size as represented on the interrogated routers or switches.

Between discovery sessions, IP addresses on the physical network may be added or removed, resulting in addresses on the network differing from addresses in Proteus. In IPv6 Reconciliation, Proteus lists such addresses as one of two types:

- *Unknown IP Address*—an IP address that exists on the physical network, but not in Proteus. This likely represents an address that has been added to the network since the last discovery.

After an IPv6 reconciliation policy discovery scan has been run, the following information can be viewed by the administrator:

- *IP Address*—lists the IP address.
- *Type*—an IP address may be of one of the following types:
    - *Unknown*—an address that exists on the physical network, but that is not in Proteus. This likely represents an address that has been added to the network after the last discovery.
- *Network*—the parent IP network object for the IP address.
- *FQDN*—the fully qualified domain name for the IP address.
- *MAC Address*—the MAC address of the IP address.
- *Time Since First Detection*—the time since the address was first discovered by the IP reconciliation policy.

After viewing the discovery data, the administrator can perform the following reconciliation actions:

- Reconcile all addresses
- Reconcile selected addresses
- Delete addresses

The reconciliation action performs the following

- Unknown IP addresses are added to the Proteus database.

Proteus may not be able to reconcile an address for one of the following reasons:

- There is a conflict between the size of the physical network and the size of the equivalent IP network object in Proteus. As a result, Proteus cannot add the address.
- The IP state between two discovery sessions does not match. For example, an earlier discovery session reported the address as Static; before the next discovery session, another user changes its state to Reserved.

The result of the reconciliation process can be viewed on the Reconciliation Summary page of the Proteus WebUI.

7.1.6.4 NM-4: MAC Address Network Access Control

(FNM_MAC_EXT.1)

The TOE implements a basic form of Network Access Control in the Adonis component. This consists of a function based on the MAC address of the client requesting access to the managed network: MAC Address Filtering (MAC Pools). This function is configurable through the Proteus WebUI (configuration changes are applied to Adonis from Proteus through the deployment mechanism).

Adonis can filter client requests based on the originating MAC address of the workstation hardware that makes the request. When a client requests an IP address, Adonis checks the MAC address of the network interface from which the request originated.

MAC pools are lists of MAC addresses. MAC pools:

- are created manually by administrators
- can contain only individual MAC addresses
- cannot include either MAC address wildcards or ranges
- are used by the Adonis DHCP service to define whether hosts can receive a dynamic IP address and hence access to network
- can be set at the configuration, IP block, IP network, or DHCP range levels

When Adonis is under Proteus control, the administrator can configure three MAC pool options:

- *Allow MAC Pools*—this option explicitly allows hosts with MAC addresses contained in the MAC pool or pools access to DHCP services wherever it is set. It also denies all other MAC addresses from receiving an IP address from DHCP
- *Deny MAC Pools*—this option denies DHCP services to hosts with the specific MAC addresses contained in the MAC pool(s)
- *Deny Unknown MAC Addresses*—by default, unknown MAC addresses are allowed access to DHCP services. By setting this option, unknown MAC addresses are denied. Only MAC addresses that have been added as DHCP reserved addresses or MAC addresses that are members of allowed MAC pools are allowed access to DHCP if this option is set.

These three options are mutually exclusive. Each defined MAC pool (set at the configuration, IP block, IP network, or DHCP range level) can have a difference option applied to it; i.e. MAC addresses in Pool-1 can be allowed access while the MAC addresses in Pool-2 can be denied.

By default, MAC pools are not defined and all MAC addresses are allowed to obtain an IP address from Adonis DHCP.