National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

BlueCat Networks

Adonis DNS/DHCP Appliance Version 6.7.1-P3

and

Proteus IPAM Appliance Version 3.7.2-P2

Report Number: CCEVS-VR-VID10480-2013
Dated: August 9, 2013
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

List of Figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product BlueCat Networks Adonis DNS/DHCP Appliance Version 6.7.1-P3 and Proteus IPAM Appliance Version 3.7.2-P2.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

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.

The TOE is intended for use in computing environments where there is a low level threat of malicious attacks. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in August 2013. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 3.1 R3 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.1 from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, [CEM]. This Security Target does not claim conformance to a protection profile.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security

Target (ST) is contained within the document *BlueCat Networks Adonis DNS/DHCP Appliance Version 6.7.1-P3) and Proteus IPAM Appliance Version 3.7.2-P2 Security Target.*

2. Identification

Target of Evaluation:	BlueCat Networks Adonis DNS/DHCP Appliance Version 6.7.1-P3 and Proteus IPAM Appliance Version 3.7.2-P2
Evaluated Software and Hardware:	
	Adonis DNS/DHCP Appliance Version 6.7.1-P3
	Proteus IPAM Appliance Version 3.7.2-P2
Developer:	BlueCat Networks, Inc.
CCTL:	CygnaCom Solutions
	7925 Jones Branch Dr., Suite 5400
	McLean, VA 22102-3321
Evaluator:	Mr. Herb Markle
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Mr. Bradford O'Neill, Dr. Patrick Mallett
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, July 2009
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, July 2009

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in Section 6.1 of the ST. Potential customers of this product should confirm that functionality implemented is suitable to meet the customers' requirements.

The following sections describe the TOE's security features.

3.1. Security Audit Functions

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.

NOTE: If the environment requires long-term storage of audit records, then the TOE should be configured to send 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.

3.2. Identification and Authentication Functions

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.

3.3. Security Management Functions

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.

3.4. 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.

3.5. TOE Access Functions

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

3.6. 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.

3.7. Summary

3.7.1. Security functional Requirements

A list of the SFRs for the TOE follows.

***Note**: "_EXP" in the SFR ID indicates extended requirements. The ST must be consulted for the specifics of the _EXP requirements and the completions of the SFRs drawn from the CC.*

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
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)

3.7.2. Operational Environment Objectives

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

1 Administrators are non-hostile, carefully selected and trained, and follow the administrator guidance when using the TOE. Administration is competent and on-going.

2 The Operational Environment will provide mechanisms to notify responsible personnel of a possible problem.

Note: This objective 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.

3 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.

4 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.

5 Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

6 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.

7 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: This Objective is only applicable when the TOE is configured to use an external LDAP, RADIUS, TACACS+, Microsoft Active Directory or Kerberos authentication service.

4. Assumptions and Clarification of Scope

The ST provides additional information on the assumptions made and the threats countered.

4.1. Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL 2 assurance requirements.

a) AGD_OPE.1 Operational user guidance

b) AGD_PRE.1 Preparative procedures

c) ALC_DEL.1 Delivery procedures

4.2. Assumptions

The ST identifies the following assumptions about the use of the product:

- It is assumed that 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.
- It is assumed that 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.
- It is assumed that the TOE hardware and software critical to security policy enforcement will be physically protected from unauthorized modification.
- It is assumed that 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.
- It is assumed that TOE users will choose strong passwords and protect all authentication credentials.

4.3. Clarification of Scope

This section covers the limitations and clarifications of this evaluation. Note that:

4.3.

1. This evaluated configuration satisfies the security claims made with the EAL2 level of assurance.

4.3.

4.3.

4.3.

2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.

3. As with EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

4. The following are not included in the Evaluation Scope:

   TOE functionality considered out of scope

   - 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 to authenticate client hosts by an external authentication server to allow or deny them dynamic IP addresses based on authentication results

   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.

5. The IT environment needs to provide the following capabilities:
   - 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

- 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 for which the TOE provides DNS/DHCP services
- The operational network for which the TOE provides DNS/DHCP services
- 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)

5. Architectural Information

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

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

The evaluated configuration of the TOE includes a Proteus IPAM Appliance managing two or more Adonis DNS/DHCP Appliances. Figure 1 shows the TOE boundary and the typical environment in which the TOE would operate.

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.

A hardened Linux-based operating system is loaded on all Proteus and Adonis 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

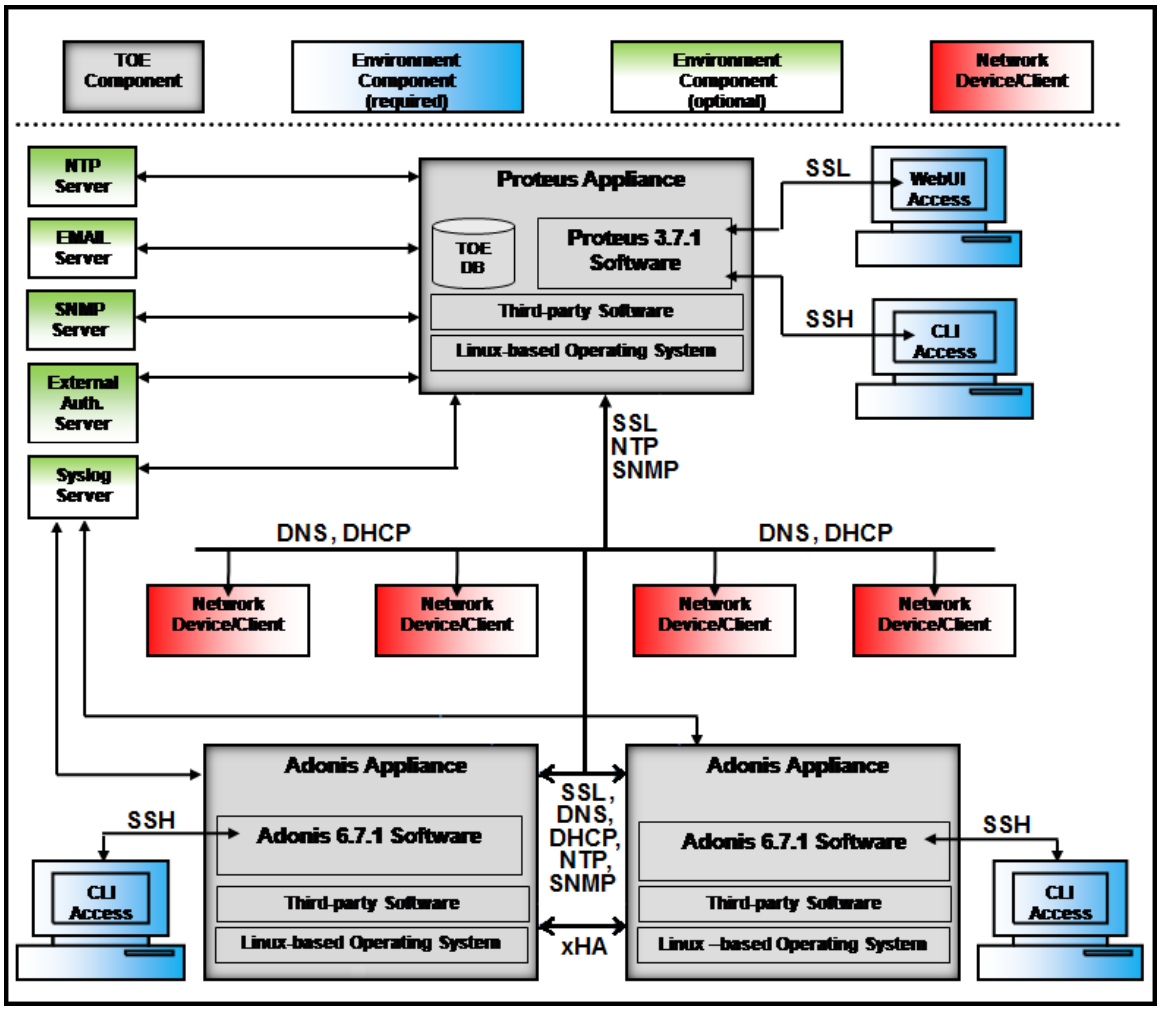

Figure 1: TOE Boundary

Adonis DNS/DHCP Appliance

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.

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.

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.

Proteus IPAM Appliance

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

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.

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.

6. Documentation

The TOE is physically delivered to the End-User or downloaded from the vendor's website. The guidance is part of the TOE and is delivered on the installation media.

The following guidance documents are developed and maintained by EiQ Networks and delivered to the end user of the TOE:

- **Adonis 1200 DNS/DHCP Solution Installation Guide for Version 6.7.1**, April 20, 2012
- **Adonis 1900 DNS/DHCP Solution Installation Guide for Version 6.7.1**, April 20, 2012
- **Adonis 1950 DNS/DHCP Solution Installation Guide for Version 6.7.1**, April 20, 2012
- **Adonis 800 DNS/DHCP Solution Installation Guide for Version 6.7.1**, April 20, 20121
- **Adonis Administration Guide Version 6.7.1**, April 20, 2012
- **Adonis XMB2 Installation Guide**, April 25, 2012
- **Proteus 3300 IP Address Management Solution Installation Guide for Version 3.7.1**, April 20, 2012
- **Proteus 5500 IP Address Management Solution Installation Guide for Version 3.7.1**, April 20, 2012
- **Proteus Administration Guide Software Version 3.7.1**, April 23, 2012
- **Release Notes Adonis Appliances Hotfix KB-4606**, December 4, 2012
- **Release Notes Adonis DNS/DHCP Software Version 6.7.1**, April 2 2012
- **Release Notes Adonis v6.7.1 P1 Patch KB-3542**, June 19, 2012
- **Release Notes Adonis v6.7.1 P2 Patch KB-3888**, October 30, 2012
- **Release Notes Adonis v6.7.1 P3 Patch KB-4781**, April 26, 2013
- **Release Notes Proteus Appliances Proteus v3.7.2 P2 Hotfix KB-4983**, May 28, 2013
- **Release Notes Proteus IPAM Software Version 3.7.1**, April 3, 2012
- **Release Notes Proteus v3.7.1 P1 Patch KB-3541**, June 19, 2012
- **Release Notes Proteus v3.7.2 P1 Patch KB-4519**, December 11, 2012
- **Release Notes Proteus v3.7.2 P2 Patch KB-4780**, April 23, 2013
- **Release Notes Proteus™ IPAM Software Version 3.7.2**, October 30, 2012

7. IT Product Testing

At EAL 2, the overall purpose of the testing activity is “independently testing a subset of the TSF, whether the TOE behaves as specified in the design documentation, and to gain confidence in the developer's test results by performing a sample of the developer's tests” (ATE_IND.2, 14.6.2.1 [CEM])

At EAL 2, the developer’s test evidence must “show the correspondence between the tests provided as evaluation evidence and the functional specification. However, the coverage analysis need not demonstrate that all TSFI have been tested, or that all externally-visible interfaces to the TOE have been tested. Such shortcomings are considered by the evaluator during the independent testing.” (ATE_COV.1, 14.3.1.3 [CEM])

This section describes the testing efforts of the vendor and the evaluation team.

The objective of the evaluator’s independent testing sub-activity is “to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests” (ATE_IND.2, Independent testing – sample [CC]).

7.1. Developer Testing

The developer testing effort that is described in detail in the Developer Test Plan involved executing the test sets in the test configurations as described in Section 8: Evaluated Configuration.

7.1.1. Overall Test Approach and Results

The developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. These test cases were mapped to the SFRs and TSFIs, listed in the ST, Functional Specification [FSP], and Common Criteria Test Coverage Document. After the test cases were defined, test procedures were written by the vendor’s development team to exercise each test case.

All of the developer test cases are manual, i.e. all test steps including setup and cleanup steps were performed by a user entering commands a terminal running the Proteus web interface (WebUI). The tests were written to use the WebUI to exercise the functions of the TOE.

7.1.2. Depth and Coverage

All developer test cases test TOE security functions by stimulating an external interface.

Although the developer tests are performed using the WebUI, the evaluator determined that, the test cases as described in the test documentation adequately exercise the internal interfaces.

The developer provided a test plan, test procedures and test evidence consisting of screen shots of the actual results from the execution of the tests:

- The developer's test plan covered all of the security relevant behavior of each Security Function in the ST.
- The developer wrote test procedures for 100% of the cases identified in the Common Criteria Test Coverage Document.
- The Developer executed all of their test procedures and provided the actual results.
- The developer's test procedures covered 100% of the TOE SFRs claimed in the Security Target.
- The developer's test procedures covered all of the External TSF Interfaces.
- The developer's test procedures covered all of the Internal Subsystem Interfaces.

7.1.3. Results

The evaluator checked the developer’s test procedures and the test evidence and found that the expected test results are consistent with the actual test results provided. For each test case examined, the evaluator checked the expected results in the test procedures with the actual results provided in the test evidence and found that the actual results were consistent with the expected results.

Given the Evaluation Assurance level (EAL 2), the evaluator determined that the vendor’s development team TOE testing is adequate. The vendor’s TOE testing exercises all security functions identified in the Functional Specification.

7.2. Evaluator Independent Testing

The evaluator performed the following activities during independent testing:

- Installation of the TOE in its evaluated configuration (AGD_PRE.1)
- Execution the Developer’s Functional Tests (ATE_IND.2)
- Evaluator-Defined Functional Testing (ATE_IND.2)
- Vulnerability/Penetration Testing (AVA_VAN.2)

The evaluator’s testing was performed at the vendor’s facility. The evaluator confirmed that the operational environment for the test platforms conformed to the configuration specified in the ST and the vendor’s test plan. (See Section 8: Evaluated Configuration.)

Installation was successful and the TOE was installed in the evaluated configuration as specified in the ST. At the end of the installation the evaluator identified the TOE components reference numbers (i.e. version numbers) using the procedures outlined in the CM documentation and found that they matched the evaluated versions of the TOE components.

7.2.1. Execution of the Developer's Functional Tests

The developer's functional test cases were executed after the TOE was installed in the evaluated configuration consistent with the Security Target.

Almost all (98%) of the developer's functional tests were rerun during the on-site testing on both the physical and virtual appliances.

During the running of the developer's functional test cases:

- All SFRs were tested
- All TSFI were tested

During testing, the parameter values used in commands were changed on an ad-hoc basis from the values documented in the developer's functional test steps to ensure the full functionality of each interface. The evaluator took notes and screenshots during the entire testing process.

All developer tests performed as expected with the following exceptions:

- The version numbers of the Adonis and Proteus were changed to incorporate necessary patches. The ST was updated for the new version numbers
- E-mail Address is mandatory when adding a user. The ST was updated to reflect the email address as being a required field.
- MAC address based access control functioned differently than the rules documented in the ST. The ST was updated.

7.2.2. Evaluator-Defined Functional Testing

The evaluator-defined tests were devised to augment the developer's functional tests in order to exercise functionality in greater depth than the developer tests provided. Because of the extensive coverage of the vendor tests, the following evaluator-defined tests were defined and run to cover functionality not exercised in the vendor tests.

1. **DNSSEC Test (tests DNSSEC functionality of the TOE)**
    - Sign DNS Zone
    - Distribute a Trust Anchor
    - Verify Trust Anchor
    - Configure DNS forwarding with DNSSEC enabled on Adonis
    - Query a signed zone without DNSSEC validation required
    - Query a signed zone with DNSSEC validation required

2. **Test Adonis DHCP to an external 3rd Party DNS Server**
    - Demonstration to satisfy test requirements outside the normal mode of operation
    - Shows the GSS-TSIG based dynamic DNS updates from Adonis DHCP server to MS DNS server

3. **Test SNMP traps over IPv4 and IPv6**
    - Verify SNMP Trap can be sent over IPv4 from Adonis
    - Verify SNMP Trap can be sent over IPv4 from Proteus
    - Verify SNMP Trap can be sent over IPv6 from Adonis
    - Verify error handling when IPv4 SNMP parameters are wrong
    - Verify error handling when IPv6 SNMP parameters are wrong

4. **Syslog Testing**
    - Syslog was tested on the Proteus and Adonis machines.
    - The Adonis was stopped and started to force an event. The Syslog of Adonis shows that the SNMP trap being sent for going DOWN and being UP.

In addition to these tests, throughout the running of the vendor tests the evaluator used input parameters (names, policy parameters …) other than those specified in the vendor's test procedure documentation on an ad-hoc basis.

The test environment and configuration were the same as for the developer's functional testing. No special tools were used for the evaluator-defined functional testing.

All evaluator-defined tests passed with no comments. All vendor tests run with input other than that documented by the vendor ran as expected.

7.2.3. Vulnerability/Penetration Testing

The Vulnerability / Penetration tests covered hypothesized vulnerabilities and potential misuse of guidance.

The evaluator considered the following while performing the vulnerability analysis and developing the penetration tests:

- All Evidence Deliverables: All evidence deliverables were considered for identifying potential vulnerabilities.
    - An analysis of the design documentation identified no specific vulnerabilities.
    - Vulnerabilities based on the various protocols that are used by the TOE were considered.
- Public Sources: The Evaluator performed an independent search for vulnerabilities available from the public domain including the NVD database, CVE and Security Focus.
    - The search for publicly known vulnerabilities included a search for vulnerabilities that affected the class of products that could potentially be applicable to the TOE.
- TSF based analysis: All Security Functions, Security Functional Requirements and External interfaces were considered.
- Subject to Threats: Including Bypass, Tampering, Direct Attacks and Misuse.

During the vulnerability search, the evaluator found publicly known vulnerabilities that affected the vendor product line or product. The Evaluator worked with the Developer to find a rationale for why each of the vulnerabilities found was either valid or invalid for the TOE.

As a result of the Evaluator's Vulnerability search, patches were developed for both the Adonis and Proteus software and were incorporated into the evaluated version of the TOE that will be distributed to customers.

The following Vulnerability / Penetration tests were developed by the evaluator:

1. **Data Transfer Protection Tests**
    - Verify interface from the Browser (Firefox and Chrome) to the Proteus servers (check cypher suite)
    - Verify DNSSEC Handshaking
    - Verify SSH to Proteus interface
    - Verify SSH to Adonis interface

2. **Data Transfer between Proteus and Adonis Test**
    - Shows how the communication between Proteus and Adonis is secured using Wireshark

3. **MAC Authentication vs Regular Authentication**
    - Created to prove that MAC authentication has no influence on the Proteus authentication mechanism
    - Tests that a user cannot gain administrator privileges to Proteus even if the same user is in the authentication server used for both MAC Authentication and TOE Authentication

The test environment and configuration were the same as for the developer's functional testing. The test results and screenshots for the test cases were recorded during the Penetration testing.

All Penetration tests passed with no comments.

8. Evaluated Configuration

The tested configuration of the TOE consisted of 2 instances of one Proteus and managing two Adonis appliances. One thread (X.X.48.20X) consisted of all physical appliances. The other instance consisted of virtual appliances (X.X.48.11X).

The management of both forms of Proteus appliances was accomplished using a desktop PC running Windows 7 with Firefox, Chrome, and IE browsers installed.

Both types of Proteus appliances were configured to use the supporting servers (NTP, EMAIL, SNMP, Syslog, external authentication servers).

The physical Adonis appliances were hardwired together for the cross-over high availability feature.

The virtual appliances were configured to mimic a physical connection between the Adonis Appliance as well. Network Device Clients (red) were virtual hosts.

The Proteus appliance had HTTPS enabled and HTTP disabled.

The following interfaces were tested in both instances of the test bed.

- NTP, SMTP, SNMP, External Authentication Servers --> Proteus
- Syslog Server --> Proteus and Adonis Servers
- Administrative SSH--> Proteus and Adonis
- Administrative SSL --> Proteus
- Proteus --> Adonis trusted communication
- Adonis--> Adonis xHA
- Device Client DNS, DHCP requests --> Adonis

The evaluated configuration of the TOE is depicted in the following figure:

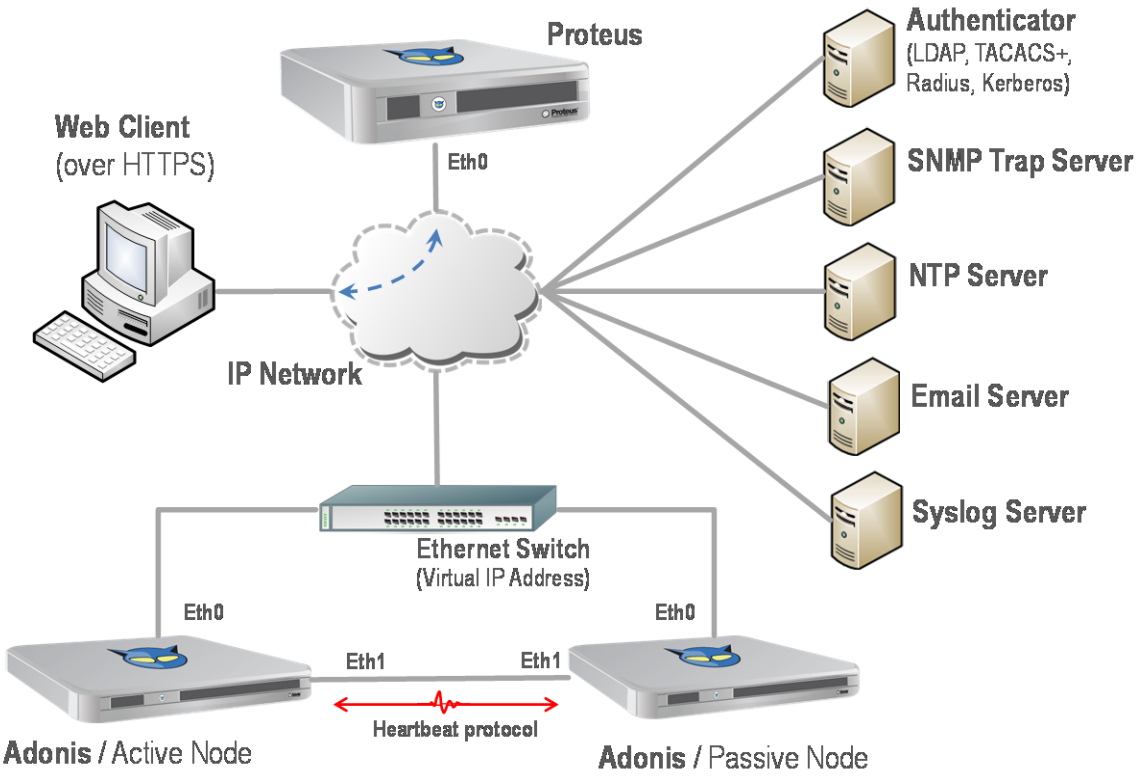

Figure 2: Evaluated Configuration of TOE.

9. Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 augmented with ALC_FLR.2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 2 augmented with ALC_FLR.1. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted.

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.1 Basic design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- 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
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.2 Security objectives
- ASE_REQ.2 Derived security requirements
- ASE_SPD.1 Security problem definition
- ASE_TSS.1 TOE summary specification
- ATE_COV.1 Evidence of coverage
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing – sample

- AVA_VAN.2 Vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached Pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.
- The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

10. Validators Comments/Recommendations

While SSH is not part of the evaluated TOE configuration and should be disabled during normal operations, SSH was enabled during evaluation testing because it was needed for initial setup and reconfiguration of system. SSH use was limited only to those functions.

Internal communications between Proteus and the Adonis appliances are protected from disclosure (FPT_ITT.1) via TLS connections which are encrypted with RC4 (128 bits). RC4 is not a FIPS approved algorithm. A bug report (CES-2974) was submitted to address this issue in future releases of the product.

Security Target

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 is compliant with the Specification of Security Targets requirements found within Annex B of Part 1of the CC.

11. Glossary

11.1. Product Specific Acronyms and Terminology

The following are product specific acronyms and terms. Not all are used in this document.

API	Application Programming Interface
Assets	Information or resources to be protected by the countermeasures of a TOE.
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 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.
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).
Availability	Assuring information and communications services will be ready for use when expected.
Berkeley Internet Name Domain (BIND)	Berkeley Internet Name Domain: 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.
CLI	Command Line Interface
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.
DDI	DNS, DHCP, and IPAM

DDNS	Dynamic DNS
Demilitarized Zone (DMZ)	A physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network.
DHCP	Dynamic Host Configuration Protocol
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	Domain Name Server / System
DNS Zone	A portion of the global Domain Name System (DNS) namespace for which administrative responsibility has been delegated.
DNSSEC	DNS Security Extensions
ENUM	Electronic Numbering
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.
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
Incident	One or more intrusion events that are suspected of being involved in a possible violation of a security policy.
IPAM	IP Address Management
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
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.
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
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.
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.
RADIUS	Remote Authentication Dial In User Service
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.
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
Subnet	A subnetwork; a logically visible subdivision of an IP network.
TACACS+	Terminal Access Controller Access-Control System Plus
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.
TCP/IP	Transmission Control Protocol/Internet Protocol

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.
TLS	Transport Security Layer
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.
TSIG	Transaction Signature
UDP	User Datagram Protocol
UI	User Interface
VPN	Virtual Private Network

11.2. CC Specific Acronyms and Terminology

This section defines the CC-specific acronyms and terms. Not all of these are used in this document.

Assurance	Grounds for confidence that an entity meets its security objectives.
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of a threat agent's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) to a package.
Authentication data	Information used to verify the claimed identity of a user.
Authorised user	A user who may, in accordance with the SFR, perform an operation.
CC	Common Criteria [for IT Security Evaluation]
CEM	Common Methodology for Information Technology Security Evaluation
Class	A grouping of families that share a common focus.
Component	The smallest selectable set of elements on which requirements may be based.
Connectivity	The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency	A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package..
EAL	Evaluation Assurance Level
Element	An indivisible security requirement.
Evaluation	Assessment of a PP, an ST, or a TOE against defined criteria.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted community.
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
External entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Family	A grouping of components that share security objectives but may differ in emphasis or rigor.
Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.
Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Internal communication channel	A communication channel between separated parts of TOE.
Internal TOE transfer	Communicating data between separated parts of the TOE.
Inter-TSF transfers	Communicating data between the TOE and the security functions of other trusted IT products.
IT	Information Technology

Iteration	The use of the same component to express two or more distinct requirements.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Organizational security policies	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.
OSP	Organizational Security Policy
Package	A named set of either functional or assurance requirements (e.g. EAL 3).
PP	Protection Profile
Protection Profile (PP)	An implementation-independent statement of security needs for a TOE type.
Prove	This term refers to a formal analysis in its mathematical sense. It is completely rigorous in all ways. Typically, “prove” is used when there is a desire to show correspondence between two TSF representations at a high level of rigor.
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
SAR	Security Assurance Requirement
Secure state	A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
Security attribute	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.
Security Function Policy (SFP)	A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions.
Security Target (ST)	An implementation-dependent statement of security needs for a specific identified TOE.
Selection	The specification of one or more items from a list in a component.
Semiformal	Expressed in a restricted syntax language with defined semantics.
SFP	Security Function Policy

SFR	Security Functional Requirement
ST	Security Target
Subject	An active entity in the TOE that performs operations on objects.
Target of Evaluation (TOE)	A set of software, firmware and/or hardware possibly accompanied by guidance.
TOE	Target of Evaluation
TOE resource	Anything useable or consumable in the TOE.
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.
Transfers outside TSF	TSF mediated communication of data to entities not under control of the TSF.
Transfers outside TSF	TSF mediated communication of data to entities not under control of the TSF.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.
Trusted path	A means by which a user and a TSF can communicate with necessary confidence.
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF interface (TSFI)	A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
User	See external entity
User data	Data created by and for the user that does not affect the operation of the TSF

12. Bibliography

URLs

1. Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).
2. CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-001.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-002.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-003.
4. Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-004