National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Infoblox Trinzic Appliances with NIOS 7.1

Report Number: CCEVS-VR-VID10624-2015

Dated: December 21, 2015

Version: 1.0

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

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul A. Bicknell

Patrick Mallett

Brad O’Neill

Jay Vora

Evaluation Team

Cheryl Dugan

Eve Pierre

Common Criteria Testing Laboratory

Computer Sciences Corporation
7459A Candlewood Road
Hanover, Maryland 21076

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Infoblox Trinzic Appliances with NIOS 7.1, the Target of Evaluation (TOE), performed by Computer Sciences Corporation. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC) of Hanover, MD in accordance with the United States evaluation scheme and completed on December 21, 2015. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated September 2012 at Evaluation Assurance Level 1, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 4, September 2012.

The TOE is a network appliance that provides delivery of IP network services and management including: DNS, DHCP, IPAM, FTP, TFTP and HTTP.

The Evaluation Team performed an analysis of the international interpretations of the CC, CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before September 19, 2011.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Infoblox Trinzic Appliances with NIOS 7.1
Protection Profile	NIAP Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 3.0, February 13, 2015
Security Target	Infoblox Trinzic Appliances with NIOS 7.1, version 2.3, December, 2015
Dates of evaluation	August 31, 2015 – December 21, 2015
Evaluation Technical Report	Infoblox Trinzic Appliances with NIOS 7.1 Assurance Activity Report, v1.0
Conformance Result	1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012. 2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012. 3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012. 4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012. The following CC conformance: • Part 2 extended • Part 3 conformant 5. Protection Profile for Network Devices, version 1.1, 08 June 2012 6. Security Requirements for Network Devices Errata #3, 03 November 2014.
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012
Common Evaluation Methodology (CEM) version	CEM version 3.1R4, September 2012
Sponsor	Infoblox
Developer	Infoblox
Evaluators	Cheryl Dugan, Eve Pierre
Validation Team	Paul A. Bicknell, Patrick Mallett, Brad O’Neill, Jay Vora

3. SECURITY POLICY

The TOE is intended to be used in a range of security settings (i.e. computers coupled to a single TOE can vary from non-classified Internet connected to those protected in accordance with national security policy). Any data leakage across the TOE may cause severe damage to the organization and therefore must be prevented.

4. SECURITY PROBLEM DEFINITION

4.1. Assumptions

The ST identified the following security assumptions:

Table: Secure Usage Assumptions

Assumption	**Definition**
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.

4.2. Threats

The ST identified the following threats addressed by the TOE:

Table: Threats

Threat	**Definition**
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may

	masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

4.3. Organizational Security Policies

The Security Target identifies the following Organizational Security Policies (OSPs) to which the TOE must comply.

Table 2: Organizational Security Policies

OSP	**Definition**
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

5. ARCHITECTURAL INFORMATION

5.1. Physical Scope and Boundary

This section provides an overview of the Infoblox Trinzic Appliances running NIOS 7.1 Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following: ND-800, TE-810, TE-820, TE-1410, TE-1420, PT-1400, ND-1400, TE-2210, TE- 2220, PT-2200, ND-2200, IB-4010, IB-4020, PT-4000, PT-4000-10G, IB-4030, IB-4030-10G, ND-4000. The software is comprised of the NIOS 7.1.

Common hardware characteristics of all models listed above are as follows:

- The TE and IB versions are identical in terms of hardware, but based on a software license, the CPU clock may be throttled to a lower performance level.
- The ND versions have additional memory, additional disk storage and an additional processor socket compared to the Base Appliance.
- The TR versions have additional disk storage compared to the Base Appliance.

Figure 2 below depicts the typical physical aspects of the Infoblox Trinzic Appliances.

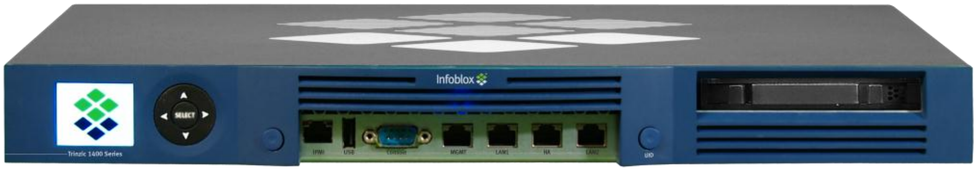

Figure 1: Infoblox Trinzic Appliance

5.1.1. Required Non-TOE Hardware, Software, and Firmware

The TOE incorporates all hardware, software and firmware of the appliances listed in Table 1 of the ST. Depending on the administrator defined configuration, the TOE may require the following services to be present in the environment:

- Active Directory when the TOE is configured to use an external authentication source
- NTP server when the TOE is configured to use an NTP server
- Kerberos server where GSS-TSIG or external authentication is enabled

5.1.2. Evaluated Configuration

In the evaluated configuration the TOE is deployed as described in the guidance documents which are delivered with the TOE. The TOE is evaluated using the following configuration settings:

- TSIG is configured for dynamic DNS updates from ISC DHCP servers and DNS clients (if applicable to the environment)
- GSS-TSIG is configured for dynamic DNS updates from Microsoft DHCP servers and DNS servers and clients (if applicable to the environment)
- bloxTools is disabled
- SSH is disabled (CLI access is performed via the local console port)
- RADIUS authentication is disabled
- TACACS+ authentication is disabled
- Secure Copy (SCP) is disabled / not used
- Grid must NOT be configured

5.2.Logical Scope and Boundary

The TOE logical boundary is comprised of the following security functions:

- Security Audit
- Cryptographic Support
- Full Residual Information Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all SFRs of the NDPP v1.1 as necessary to satisfy testing/assurance measures prescribed therein.

Given that this Security Target conforms to the NDPP, the security claims focus on the TOE as a secure network infrastructure device and do not focus on other key functions provided by the TOE, such as Secure DNS. However, those functions can be freely used without affecting the claimed and evaluated security functions; they simply have not been evaluated to work correctly themselves.

5.2.1. Security Audit

The TOE generates audit records associated with use of the administrative functions. Audit records may be stored locally and sent to a syslog server. The TOE deletes the oldest records if the audit trail exceeds a defined maximum. A local time source supports reliable time stamps for the audit function. Auditable events include those requirements stated in Table 1 of the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) ver. 1.1, dated June 8, 2012.

Note: if the TOE is configured to transmit its audit logs to an external syslog server then that

5.2.2. Cryptographic Support

The TOE provides cryptography in support of Infoblox Trinzic security functionality. All algorithms have been validated against CAVP requirements (http://csrc.nist.gov/groups/STM/cavp/). See table 2 below for certificate references.

Table 3: FIPS References

Algorithm	Support Mode	CAVP Cert. #
SHS	Intel Xeon, Intel Pentium	1839
RSA/ rDSA	Intel Xeon, Intel Pentium	1085
AES	Intel Xeon, Intel Pentium	2115
HMAC	Intel Xeon, Intel Pentium	1287
RNG	Intel Xeon, Intel Pentium	1086
DRBG	Intel Xeon, Intel Pentium	835

The cryptographic services provided by the TOE are described in Table 3 below.

Table 4: TOE Provided Cryptography

Cryptographic Method	Use within the TOE
SHS	Used to provide TLS traffic integrity verification
RSA/ rDSA	Used in TLS session establishment, trusted update signature verification
AES	Used to encrypt TLS session traffic
RNG	Used in TLS session establishment
DRBG	Used in random number Generation

5.2.3. Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Residual data is never transmitted from the TOE. The TOE ensures that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects by clearing the residual information before network packets are sent from the TOE.

5.2.4. Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password based authentication can be performed on the serial console

5.2.5. Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure TLS session or via a local console connection. The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE; and
- TOE configuration file storage and retrieval.

A user must have an admin account to log in to the TOE. Each admin account belongs to an admin group, which contains roles and permissions that determine the tasks a user can perform.

The TOE provides a default superuser admin group, called admin-group, with one superuser administrator, admin. The default superuser admin can log in to the TOE, using the default user name admin and password infoblox.Superuser admins are the security admins and have full access and control of all the operations of a TOE. Note that you must change the default user name and password of the default superuser admin to prevent unauthorized access to the TOE.

Only superusers can do the following:

- Create admin accounts and groups.
- Set password parameters.
- Create the login banner.
- Set the session timeout

Limited-access admin groups provide their members with read-only or read/write access to specific resources. These admin groups can access the appliance through the GUI, API, or both. They cannot access the appliance through the console. In addition, limited-access admins are not allowed to perform the following tasks:

- Download the support bundle.
- Enable SNMP on Grid members.
- Upload files that are larger than 100 MB.

If the file size is greater than the maximum size allowed, the Upload dialog box closes and an error message is displayed in the feedback panel. The attempt to upload a file that exceeded the maximum will be logged to syslog. non-superusers only are able to upload files for file distribution and do CSV import.

5.2.6. Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords.

5.2.7. TOE Access

The TOE provides administrative access via a console port (local) and HTTPS (remote). The TOE provides a password-based logon mechanism for local and remote access and enforces a defined password complexity and expiration policy. The TOE optionally supports authentication against an Active Directory server.

The TOE enforces Role Based Access Control (RBAC), session timeouts and displays an advisory banner at login.

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

5.2.8. Trusted Path/Channels

The TOE initiates outbound TLS tunnels to transmit audit logs to remote syslog servers. In addition, TLS is used to secure the session between the TOE and the authentication servers.

6. DOCUMENTATION

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- Infoblox 800 Series Installation Guide
- Infoblox 1400 Series Installation Guide
- Infoblox NIOS Administrator Guide, Release 7

All documentation delivered with the product is relevant to and within the scope of the TOE.

7. IT PRODUCT TESTING

This section describes the testing efforts of the evaluation team.

7.1. Evaluation team independent testing

The evaluation team conducted independent testing at the Infoblox facilities in Santa Clara, California. The evaluation team configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Protection Profile test procedures as a basis for creating each of the Independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profiles and the evaluation team verified that each test passed.

7.2.Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

8. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R4.

Computer Sciences Corporation (CSC) has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Protection Profile for Network Devices, version 1.1, June 8, 2012 and the Security Requirements for Network Devices Errata #3, November 3, 2014. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on December 21, 2015.

VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the Infoblox Trinzic Appliances with NIOS 7.1 meets the claims stated in the Security Target.

9. ANNEXES

None

10. SECURITY TARGET

Infoblox Trinzic Appliances with NIOS 7.1 Security Target, version 2.3, December 2015.

11. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) 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.

12. BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
5. Infoblox Trinzic Appliances with NIOS 7.1, version 2.3
6. Computer Sciences Corporation (CSC): Infoblox Trinzic Appliances with NIOS 7.1 Assurance Activity Report, v1.0