# C089 Certification Report

## Infoblox Trinzic Appliances with NIOS v8.2.6

File name: ISCB-3-RPT-C089-CR-v1
Version: v1
Date of document: 14 June 2018
Document classification: PUBLIC


For general inquiry about us or our services,
please email: mycc@cybersecurity.my



CyberSecurity Malaysia
(720830-U)
Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

# C089 Certification Report

## Infoblox Trinzic Appliances with NIOS v8.2.6

14 June 2018

ISCB Department

**CyberSecurity Malaysia**

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 □ Fax: +603 8992 6841
http://www.cybersecurity.my

***DISTRIBUTION:*** UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

# Copyright Statement



Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

*Printed in Malaysia*

# Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 22th June 2018, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

# Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# Document Change Log

| RELEASE | DATE | PAGES AFFECTED | REMARKS/CHANGE REFERENCE |
|---|---|---|---|
| d1 | 13 June 2018 | All | Initial draft |
| v1 | 14 June 2018 | All | Changes and reviewed by sponsor, developer and BAE System |

# Executive Summary

The Target of Evaluation (TOE) is the Infoblox Trinzic Appliances with NIOS v8.2.6 that includes the NIOS v8.2.6 software, hardware and virtual appliances. The TOE is a network device that consolidates the delivery and management of core IP network services including DNS, DHCP, IPAM, FTP, TFTP and HTTP.

In addition, the TOE also provides Secure Grid functionality which allows Infoblox appliances to work cooperatively in an enterprise deployment. One appliance is designated as a Master which distributes configuration information to all other Grid devices. Communication between the appliances is secured with OpenVPN.

The TOE NIOS operating system is a hardened version of the Fedora Linux distribution optimised for security and network performance. The appliance models are differentiated by performance, capacity and availability to support various deployment scenarios.

The TOE also provides cryptography in support of Infoblox Trinzic security functionality and all algorithms implemented have been validated against CAVP requirements.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented ALC_FLR.2. This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 12 June 2018.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that Infoblox Trinzic Appliances with NIOS v8.2.6 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

# Table of Contents

# Index of Tables

# 1 Target of Evaluation

## 1.1 TOE Description

1 Infoblox Trinzic Appliances with NIOS v8.2.6 is the Target of Evaluation (TOE). It is a network device that consolidates the delivery and management of core IP network services including DNS, DHCP, IPAM, FTP, TFTP and HTTP and provides Secure Grid functionality. Secure Grid is the capability of Infoblox appliances to work cooperatively in an enterprise deployment. One appliance is designated as Master which distributes configuration information to all other Grid devices. Communication between the appliances is secured with OpenVPN.

2 The TOE NIOS operating system is a hardened version of Fedora Linux distribution optimised for security and network performance. The appliance models are differentiated by performance, capacity and availability to support various deployment scenarios.

3 In addition, the TOE also provides cryptography in support of its security functionality and all algorithms implemented in TLS/HTTPS have been validated against CAVP requirements (http://csrc.nist.gov/groups/STM/cavp/). Infoblox supports both CC Mode and FIPS Mode, and either is allowed in the evaluated configuration.

4 The functionality defined in the Security Target (Ref [6]) that was subsequently evaluated is as follows:

- **Security Audit**
- **Cryptographic Support**
- **Identification & Authentication**
- **Security Management**
- **Protection of the TSF**
- **TOE Access**
- **Trusted Path/Channel**

## 1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

| | |
|---|---|
| **Evaluation Scheme** | Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme |
| **Project Identifier** | C089 |
| **TOE Name** | Infoblox Trinzic Appliances with NIOS v8.2.6 |
| **TOE Version** | v8.2.6 |
| **Security Target Title** | Infoblox Trinzic Appliances with NIOS v8.2.6 Security Target |
| **Security Target Version** | 1.0 |
| **Security Target Date** | 30 May 2018 |
| **Assurance Level** | Evaluation Assurance Level 2 Augmented ALC_FLR.2 |
| **Criteria** | Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2]) |
| **Methodology** | Common Methodology for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3]) |
| **Protection Profile Conformance** | None |
| **Common Criteria Conformance** | CC Part 2 Extended<br>CC Part 3 Conformant<br>Package conformant to EAL 2 with Augmented ALC_FLR.2 |
| **Sponsor** | Leidos Inc.<br>6841 Benjamin Franklin Drive<br>Columbia, Maryland 21046 |
| **Developer** | Infoblox Inc.<br>3111 Coronado Drive<br>Santa Clara, CA 95954 |
| **Evaluation Facility** | BAE Systems Applied Intelligence – MySEF (Malaysia Security Evaluation Facility)<br>Level 28, Menara Binjai,<br>2 Jalan Binjai, 50450 Kuala Lumpur, Malaysia |

## 1.3 Security Policy

6 There is one organisational security policy that has been defined regarding the use of the TOE. Section 3.3 of the Security Target (Ref [6]) defines that 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.

## 1.4 TOE Architecture

7 The TOE includes both physical and logical boundaries which are described in Section 2.3 and 2.4 of the Security Target (Ref [6]).

### 1.4.1 Logical Boundaries

8 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

Table 2: Logical Boundaries

| Security Function | Description |
|---|---|
| Security Audit | The TOE generates audit records for security relevant events and includes the date and time of the event, subject identity, outcome for the security events, and additional content for particular event types. For audit events resulting from actions of identified users, the TOE associates each auditable event with the identity of the user that caused the event.<br><br>The TOE protects the stored audit records in the audit trail from unauthorised deletion and prevents unauthorised modifications to the stored audit records in the audit trail. The TOE overwrites the oldest stored audit records when the audit trail is full. |
| Cryptographic Support | The TOE includes cryptographic functionality that provides random bit-generation, encryption/decryption, digital signature, secure hashing and key-hashing features. These features support cryptographic protocols including SSH, TLS |

| | |
|---|---|
| | and HTTPS.<br><br>SSH and Transport Layer Security protocol (HTTP over TLS) are used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from undetected modification. Communication between the TOE and trusted external entities (syslog and authentication servers) is over TLS. Finally, the TOE uses a TLS protected channel to distribute configuration data when it is transmitted between distributed parts of the TOE.<br><br>The TOE supports TLS v1.0, v1.1, and v1.2. The TOE uses OpenSSL and OpenSSH cryptography and has obtained CAVP certificates for all supporting cryptographic algorithms. |
| Identification & Authentication | The TOE requires all users to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user. The TOE supports user authentication using a local password mechanism and can be configured to use Active Directory (AD), LDAP, RADIUS or TACACS+ authentication. The TOE provides a mechanism to verify that passwords meet a defined quality metric and provides only obscured feedback to the user while the authentication is in progress. |
| Security Management | The security functions of the TOE are managed by an authorised administrator using a web-based GUI, SSH protected remote access to CLI, local CLI console port, or using an API. The ST defines the security role of 'superuser'. The superuser is the authorised administrator of the TOE and performs all security functions of the TOE including (but not limited to) managing audit configuration, password and authentication policies, and TOE updates. |
| Protection of the TSF | When Grid is enabled, communications between the TOE instances utilise TLS VPN to protect against the disclosure and modification of data exchanged |

| | |
|---|---|
| | between the TOE appliances.<br><br>The TOE provides reliable time stamps; and executes self-tests, during initial startup, to determine whether the TOE is operating correctly.<br><br>The TOE provides authorised administrators the ability to query the current version of; initiate updates to TOE firmware/software; and provides a digital signature mechanism to verify firmware/software updates to the TOE prior to installing those updates. |
| TOE Access | The TOE terminates local and remote interactive sessions after an administrator configurable time interval and allows user-initiated termination of the user's own interactive session.<br><br>Before establishing a user/administrator session, the TOE displays an administrator configured advisory banner warning message regarding unauthorized use of the TOE. |
| Trusted Path/Channel | The TOE communicates with authorised remote administrators via a web based GUI that is protected using HTTPS/TLS.<br><br>The TOE uses TLS to protect all communications with active directory and LDAP external authentication servers and syslog servers. |

### 1.4.2 Physical Boundaries

9 The TOE consist of the following appliance models stated in Table 3: TOE Appliance Models, Table 4: TOE Hardware Models and Table 5: Resource Requirements for Virtual Appliances as below:

Table 3: TOE Appliance Models

| Hardware Appliance Model | Virtual Appliance Model |
|---|---|
| IB-4015 | IB-V4015 |

| | |
|---|---|
| IB-2225 | IB-V2225 |
| IB-1425 | IB-V1425 |
| IB-825 | IB-V825 |

Table 4: TOE Hardware Models

| Infoblox Model | CPU | CPU Speed | Memory | Storage | Network Connectivity |
|---|---|---|---|---|---|
| IB-4015 | Intel Xeon E5-2680 | 2.4 Ghz | 64GB | 1.8TB | 4x1Gbe Ethernet, nonaccelerated |
| IB-2225 | Intel Xeon E5-2620 | 2.1 Ghz | 64GB | 1.8TB | 4x1Gbe Ethernet, nonaccelerated |
| IB-1425 | Intel Xeon be E3-1275 | 3.6 Ghz | 32GB | 900GB | 4x1Gbe Ethernet, nonaccelerated |
| IB-825 | Intel Xeon Core i3-6100TE | 3.6 Ghz | 32GB | 1TB | 4x1Gbe Ethernet, nonaccelerated |

Table 5: Resource Requirements for Virtual Appliances

| NIOS Virtual Appliance | Primary Disk (GB) | # of CPU Cores | Memory Allocation (GB) |
|---|---|---|---|
| IB-V4015 | 250 | 14 | 128 |
| IB-V2225 | 250 | 8 | 64 |
| IB-V1425 | 250 | 4 | 32 |
| IB-V825 | 250 | 2 | 16 |

10 The TOE can be deployed on a single machine ("stand alone" machine) or as a distributed environment of multiple machines (referred to as a "grid"). Each TOE appliance instance is a hardened Linux system running NIOS v8.2.6. In a distributed environment, the TOE provides Secure Grid functionality, protecting communication between the appliances by using OpenVPN.

11 Depending on the administrator defined configuration, the TOE may require the following services to be present in the environment such as:

- The following browsers to access the GUI:
  - Firefox on Windows, Linux and Mac OS;
  - Safari on Mac OS;
  - Internet Explorer on Windows; and
  - Chrome on Windows, Linux and Mac OS.
- SSHv2 client when accessing the CLI remotely across an Ethernet network.
- NTP server when the TOE is configured to use an NTP server.
- Active Directory, LDAP, RADIUS, TACACS+ servers when the TOE is configured to use an external authentication source.
- An external log server when the TOE is configured to use an external syslog server.

12 The Infoblox virtual appliance models includes virtual images for VMWare and runs on ESXi servers that have DAS (Direct Attached Storage), or iSCSI (Internet Small Computer System Interface) or FC (Fibre Channel) SAN (Storage Area Network) attached. The TOE software package for virtual appliances is installed on a host with VMWare ESXi 6.5 or 5.5 and then configured as a virtual appliance. The host appliance and VMWare are part of the operational environment and are not part of the TOE. However, the required memory, CPU, and disk allocation for the virtual appliances is as stated in Table 5.

## 1.5 Clarification of Scope

13 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

14 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

15 Potential consumers of the TOE are advised that some functions and services of the overall product have not have been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

16 The scope of the evaluation does not include the system-defined admin roles that can be assigned to the Limited-Access group since all of the security management functions are performed by the superuser admin role which belongs to the superuser group. The TOE construct of an Authorised Administrator equates to a TOE administrative user with the superuser admin role. All security management functions are performed by the superuser admin.

## 1.6 Assumptions

17 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

### 1.6.1 Usage assumptions

18 Assumptions for the intended usage of the TOE, as described in the Security Target (Ref [6]):

a) The authorised administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organisation. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

b) The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).

c) The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

### 1.6.2 Environment assumptions

19 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

a) The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

b) A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the TOE.

c) The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.

## 1.7 Evaluated Configuration

20 The TOE can be deployed on a single machine ("stand alone" machine) or as a distributed environment of multiple machines (referred to as a "grid"). Each TOE appliance instance is hardened Linux system running NIOS v8.2.6. The functionality is the same across all appliances and processor families. The appliances all run the same code and only differ by performance and capacity.

21 The TOE presents a graphical user interface (GUI), a command line interface (CLI), and application programming interfaces (APIs). Authorised administrators manage the TOE via a TLS protected web GUI, HTTPS/TLS protected API, SSH protected remote access to CLI, or via the local CLI console port.

22 The evaluated configuration supports both CC Mode and FIPS mode. FIPS Mode also complies with FIPS certification standard to include required additional startup steps.

## 1.8 Delivery Procedures

23 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

24 The delivery procedure requirement should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

### 1.8.1 Pre-Delivery

25 The TOE NIOS is developed in-house. Before the TOE may be delivered, it must first be approved for release. In order to be approved, the TOE must undergo acceptance testing until it successfully meets the defined acceptance criteria. The release package is tested on all supported hardware platforms to ensure it meets the functionality requirements for that specific release version of the TOE. Once testing has been completed successfully, the product is then approved for release.

### 1.8.2 Appliance Delivery

26 Third party contractors are used to assemble the hardware appliances upon which the TOE operates and to install the software components. The TOE is tested according to the Contract Manufacturer's procedures prior to being shipped to customers via a secure courier.

27 In some cases the appliances are shipped from the Contract Manufacturer’s to a Infoblox reseller/partner which handles the actual delivery to the customer. The delivery to the reseller/partner will use the same process as direct customer delivery.

### 1.8.3 Online Delivery

28 All general releases are made available to existing customers for On-line delivery. The NIOS release image can only be used for upgrades of appliances that have

previously gone through the Appliance Delivery model described above or that have previously deployed via the Virtual Image Format in VMWare.

29 It is not possible for the administrator to upgrade to a release package which does not validate as correct. The customer can verify the TOE by the version number included in the file name as well as through the administrative interface both before and after upgrade.

# 2 Evaluation

30 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2+ Augmented (ALC_FLR.2). The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

## 2.1 Evaluation Analysis Activities

31 The evaluation activities involved a structured evaluation of the TOE, including the following components:

### 2.1.1 Life-cycle support

#### 2.1.1.1 Configuration Management Capability

32 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

33 The evaluators confirmed that the TOE references used are consistent.

34 The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

35 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

#### 2.1.1.2 Configuration Management Scope

36 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;
- the parts that comprise the TOE; and
- the evaluation evidence required by the SARs in the ST.

37 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

38 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

#### 2.1.1.3 TOE Delivery

39 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

#### 2.1.1.4 Flaw Reporting Procedures

40 The evaluators examined the flaw remediation procedures documentation and determined that it describes the procedures used to track all reported security flaws in each release of the TOE which would produce a description of each security flaw in terms of its nature and effects.

41 The evaluators examined the flaw remediation procedures and determined that the application of the procedures would identify the status of finding a correction to each security flaw and identify the corrective action for each security flaw.

42 The evaluators examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information on each security flaw.

43 The evaluators examined the flaw remediation procedures and determined that it describes procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.

44 The evaluators examined the flaw remediation procedures and determined that the application of the procedures would help to ensure every reported flaw is corrected and that TOE users are issued remediation procedures for each security flaw.

45 The evaluators examined the flaw remediation procedures and determined that the application of the procedures would result in safeguards that the potential correction contains no adverse effects.

46 The evaluators examined the flaw remediation guidance and determined that the application of the procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

### 2.1.2 Development

#### 2.1.2.1 Architecture

47 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail

commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

48 The security architecture description describes the security domains maintained by the TSF.

49 The initialisation process described in the security architecture description preserves security.

50 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

#### 2.1.2.2 Functional Specification

51 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given.

52 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

53 The evaluators also confirmed that the developer supplied tracing that links the SFRs to the corresponding TSFIs.

#### 2.1.2.3 TOE Design Specification

54 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

55 The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

56 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

57 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

58 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

59 The evaluators determined that all SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

### 2.1.3 Guidance documents

#### 2.1.3.1 Operational Guidance

60 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

61 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

62 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

63 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

64 The evaluators found that the operational user guidance is clear and reasonable.

#### 2.1.3.2 Preparation Guidance

65 The evaluators examined the provided delivery acceptance documentation and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

66 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

67 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

### 2.1.4 IT Product Testing

68 Testing at EAL2+ Augmented (ALC_FLR.2) consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by evaluators from BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

#### 2.1.4.1 Assessment of Developer Tests

69 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

#### 2.1.4.2 Independent Functional Testing

70 At EAL2+ Augmented (ALC_FLR.2), independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

71 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 6: Independent Functional Test

| Identifier | Description | Results |
|---|---|---|
| TEST-IND-001-GUI | • Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions.<br>• Verify that authorised users are able to perform management of TSF data functions.<br>• Verify that authorised users are able to determine and modify the behaviour of security management functions.<br>• Verify that the TSF shall maintain security roles.<br>• Verify that the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels.<br>• Verify cryptographic keys used by the TOE are as specified in the ST.<br>• Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs. | Passed. Result as expected. |

| Identifier | Description | Results |
|---|---|---|
| TEST-IND-002-GUI | • Verify that the TSF performs TOE access functions such as inactive session termination and display of TOE access banner.<br>• Verify that authorised users are able to determine and modify the behaviour of security management functions.<br>• Verify that the TSF restricts access to audit record and prevents audit records from unauthorised deletion and modification.<br>• Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs. | Passed. Result as expected. |

| Identifier | Description | Results |
|---|---|---|
| TEST-IND-003-CLI | • Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions.<br>• Verify that authorised users are able to perform management of TSF data functions.<br>• Verify that authorised users are able to determine and modify the behaviour of security management functions.<br>• Verify that the TSF performs TOE access functions such as inactive session termination and display of TOE access banner.<br>• Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.<br>• Verify that authorised users are able to query the current version of the TOE firmware/software. | Passed. Result as expected. |

| Identifier | Description | Results |
|---|---|---|
| TEST-IND-004-API | • Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions.<br>• Verify that authorised users are able to perform management of TSF data functions.<br>• Verify that authorised users are able to determine and modify the behaviour of security management functions.<br>• Verify that the TSF allows the configuration of authentication failure handling and TOE access banner.<br>• Verify that the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels.<br>• Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs. | Passed. Result as expected. |

72 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

### 2.1.4.3 Penetration Testing

73 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

74 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation.

75 The penetration tests focused on:

a) Unnecessary Open Ports

b) Common Web Vulnerability Scan

c) Input and Data Validation

d) Unrestricted File Upload

e) Secure Communication

f) Perl API Injection

76 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a basic attack potential. However, it is important to ensure that the TOE is use only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

#### 2.1.4.4 Testing Results

77 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. In addition, the documentation supplied as evidence for the EAL2+ Augmented (ALC_FLR.2) Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

# 3 Result of the Evaluation

78 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Infoblox Trinzic Appliances with NIOS v8.2.6 performed by BAE Systems Applied Intelligence MySEF.

79 BAE Systems Applied Intelligence MySEF found that Infoblox Trinzic Appliances with NIOS v8.2.6 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2+) Augmented (ALC_FLR.2).

80 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

## 3.1 Assurance Level Information

81 EAL2+ Augmented (ALC_FLR.2) provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a basic description of the design and architecture of the TOE, to understand the security behaviours of the TOE.

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

83 EAL2+ Augmented (ALC_FLR.2) also provides assurance through use of a configuration management system, evidence of secure delivery procedures and flaw remediation procedures.

## 3.2 Recommendation

84 The following recommendations are made:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) Potential purchasers of the TOE should ensure that the administrators responsible for the TOE are provided sufficient training and are familiar with the guidance supplements prior to configuring and administering the TOE.

# Annex A References

## A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] ISCB Product Certification Schemes Policy (Product_SP), v1a, CyberSecurity Malaysia, June 2017.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1, June 2017.

[6] Infoblox Trinzic Appliances with NIOS V8.2.6 Security Target, Version 1.0, 30 May 2018

[7] Infoblox Trinzic Appliances with NIOS V8.2.6 Evaluation Technical Report, Version 1.0, 12 June 2018

## A.2 Terminology

### A.2.1 Acronyms

Table 7: List of Acronyms

| Acronym | Expanded Term |
|---|---|
| CB | Certification Body |
| CC | Common Criteria (ISO/IEC15408) |
| CEM | Common Evaluation Methodology (ISO/IEC 18045) |
| CCRA | Common Criteria Recognition Arrangement |
| IEC | International Electrotechnical Commission |
| ISO | International Organisation for Standardization |
| ISCB | Information Security Certification Body |
| MyCB | Malaysian Common Criteria Certification Body |
| MyCC | Malaysian Common Criteria Evaluation and Certification Scheme |
| MyCPR | MyCC Scheme Certified Products Register |
| MySEF | Malaysian Security Evaluation Facility |
| PP | Protection Profile |

| Acronym | Expanded Term |
|---|---|
| ST | Security Target |
| TOE | Target of Evaluation |

### A.2.2 Glossary of Terms

Table 8: Glossary of Terms

| Term | Definition and Source |
|---|---|
| CC International Interpretation | An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants. |
| Certificate | The official representation from the CB of the certification of a specific version of a product to the Common Criteria. |
| Certification Body | An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA |
| Consumer | The organisation that uses the certified product within their infrastructure. |
| Developer | The organisation that develops the product submitted for CC evaluation and certification. |
| Evaluation | The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65 |
| Evaluation and Certification Scheme | The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA. |
| Interpretation | Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**. |
| Certifier | The certifier responsible for managing a specific certification task. |
| Evaluator | The evaluator responsible for managing the technical aspects of a specific evaluation task. |
| Maintenance Certificate | The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme. |

| Term | Definition and Source |
|---|---|
| National Interpretation | An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only. |
| Security Evaluation Facility | An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy |
| Sponsor | The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer. |

--- END OF DOCUMENT ---