MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C118 Certification Report

INFOBLOX TRINZIC APPLIANCES WITH NIOS V8.5.2

File name: ISCB-5-RPT-C118-CR-v1
Version: v1
Date of document: 5 August 2021
Document classification : PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

C118 Certification Report

Infoblox Trinzic Appliances with NIOS v8.5.2

5 August 2021

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C118 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C118-CR-v1
ISSUE:	v1
DATE:	5 August 2021
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

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 13 Aug 2021, 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 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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	16 July 2021	All	Initial draft
v1	5 August 2021	All	Final version

Executive Summary

The Target of Evaluation (TOE) is Infoblox Trinzic Appliances with NIOS v8.5.2. Infoblox Trinzic Appliances with NIOS v8.5.2 is a family of network appliances that provide core network services including DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), IPAM (Internet Protocol Address Management), FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol) and HTTP (Hypertext Transfer Protocol), and Network Insight Discovery Services; Threat Insight and Response Policy Zone capabilities. It also provides Secure Grid functionality, which is the capability to work co-operatively in an enterprise deployment.

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 with 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 Lab – MySEF and the evaluation was completed on 11 June 2021.

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 v8.5.2 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

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 Infoblox Trinzic Appliances with NIOS v8.5.2 is a family of network appliances that provide core network services including DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), IPAM (Internet Protocol Address Management), FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol) and HTTP (Hypertext Transfer Protocol), and Network Insight Discovery Services; Threat Insight and Response Policy Zone capabilities. It also provides Secure Grid functionality, which is the capability to work co-operatively in an enterprise deployment.

2 The TOE includes the following security functions:

- Security Audit
- Cryptographic Support
- DNS Traffic Control (extended)
- Identification & Authentication
- Asset Discovery (extended)
- Resource Utilization
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

1.2 TOE Identification

3 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	C118
TOE Name	Infoblox Trinzic Appliances with NIOS v8.5.2 (Infoblox)
TOE Version	8.5.2

Security Target Title	Infoblox Trinzic Appliances with NIOS v8.5.2 Security Target
Security Target Version	V1.0
Security Target Date	15 June 2021
Assurance Level	Evaluation Assurance Level 2 Augmented with ALC_FLR.2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 2 Augmented with ALC_FLR.2
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046, United States of America
Developer	Infoblox 2390 Mission College Blvd, Suite 501, Santa Clara, CA 95054 United States of America
Evaluation Facility	BAE Systems Applied Intelligence Malaysia Lab - MySEF

1.3 Security Policy

4 There is organisational security policies defined regarding the use of TOE.

OSPs	Statements
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.

1.4 TOE Architecture

5 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

6 The TOE consists of the following security functions identified in the Security Target (Ref [6]).

Table 2: Infoblox Logical Boundaries

Security Audit	The TOE generates audit records for security relevant events and include date and time of the event, subject identity, outcome for 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. The TOE protects the stored audit records in the audit trail from unauthorized deletion and prevents unauthorized 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 Secure Shell (SSH), Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS). 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. 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. The TOE implements the DNSSEC Protocol for authenticating the source of DNS data and ensuring its integrity. It protects DNS data from certain attacks, such as man-in the middle attacks and cache poisoning.
DNS Traffic Control (extended)	The TOE analyzes incoming DNS data and applies algorithms to detect security threats. Once security threats are detected, the TOE blacklists the domain, its traffic is blocked, and an SNMP trap is sent. The extensible service includes a whitelist that contains trusted domains on which the TOE allows DNS traffic that carry legitimate DNS tunneling traffic. The TOE employs DNS RPZs (Response Policy Zones), for allowing reputable sources to dynamically communicate domain name reputation and allows administrators to implement policy controls for DNS lookups. An RPZ feed receives response policies from external sources and also allows administrators to define multiple response policies locally (local RPZs).
Identification and 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 Two-factor authentication, Active Directory (AD), LDAP, RADIUS, SAML, 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. The TOE implements a RADIUS client

	protocol to support authentication with external RADIUS servers.
Asset Discovery (extended)	The TOE can detect networks and assets and collect data about them utilizing collection methods: SNMP; CLI device querying; ICMP Ping Sweep and Smart Subnet Ping Sweep; TCP Port Scanning; NetBIOS Queries; and vDiscovery. The protocols can be used to discover and catalogue device types: routers, enterprise switches, firewalls and security appliances, load balancers, enterprise printers, wireless access points, VoIP concentrators, application servers, VRF-based virtual networks, and end hosts. The TOE can be configured to send SNMP and email notifications when it detects particular events.
Security Management	The security functions of the TOE are managed by an authorized 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' and 'Limited-Access Group role with Cloud API permission'. The superuser performs all security functions of the TOE including (but not limited to) managing audit configuration, password and authentication policies, and TOE updates. The Limited-Access Group user only has access to the Cloud API Service.
Protection of the TSF	Communications between the TOE instances (The Infoblox Grid) utilize a TLS secured VPN to protect against the disclosure and modification of data exchanged between the TOE appliances. High Availability (HA) configuration provides hardware redundancy and degraded fault tolerance to minimize service outages. The TOE provides reliable time stamps and can optionally be set to receive clock updates from a Network Time Protocol (NTP) server. The TOE executes self-tests during initial startup to determine whether the TOE is operating correctly.

	The TOE provides authorized 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. Before establishing a user/administrator session, the TOE displays an administrator configured advisory banner warning message regarding unauthorized use of the TOE.
Trusted Path/Channels	The TOE communicates with authorized remote administrators via a web based GUI that is protected using HTTPS/TLS. Administrators can also use a CLI over SSH. The TOE uses TLS to protect all communications with external authentication servers, syslog servers, and backup/restore servers. The TOE uses HTTPS to communicate with the Advisor Service. The Advisor assists TOE administrators in monitoring and maintaining network and security infrastructure based on Common Vulnerabilities and Exposures (CVEs) as well as vendor product lifecycle announcements.

1.4.2 Physical Boundaries

Table 3: TOE hardware models

Series	Physical Appliance	Virtual Appliance
Infoblox 805 Series	TE-815, TE-825, ND-805, TR-805	ND-V805, IB-V815, IB-V825
Infoblox 1405 Series	TE-1415, TE-1425, ND-1405, TR-1405	ND-V1405, IB-V1415, IB-V1425
Infoblox 2205 Series	TE-2215, TE-2225, ND-2205, TR-2205	ND-V2205, IB-V2215, IB-V2225

Series	Physical Appliance	Virtual Appliance
Infoblox 4005 Series	TE-4015, TE-4025, ND-4005, TR-4005	IB-V4005, ND-V4005, IB-V4015, IB-V4025
Infoblox 5005 Series	N/A	IB-V5005

7 The TOE consists of the appliances and NIOS v8.5.2 software. See Table 3 for hardware and virtual appliance models in the TOE. See Table 4 for hardware appliance model specifications. The resource requirements for the virtual appliances are specified in Table 5.

8 The TOE is deployed as a distributed environment of multiple machines (hereinafter referred to as a "grid"). In a distributed environment, the TOE provides Secure Grid functionality, protecting communication between the appliances using OpenVPN and HA functionality.

9 The TOE hardware appliances include the NIOS v8.5.2 software and the hardware listed in Table 4.

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

- an external log server when the TOE is configured to use an external syslog server Decoder
- Active Directory, LDAP, RADIUS, SAML, TACACS+ servers when the TOE is configured to use an external authentication source
- An OCSP Server when X509 certificates are used for 2-factor authentication
- NTP server when the TOE is configured to use an NTP server
- Backup Server
- Source(s) for Advisor Service
- SSHv2 client when accessing the CLI remotely across an Ethernet network
- The GUI can be accessed using the following browsers: Firefox, Internet Explorer, or Chrome.
    - Firefox on Windows, Linux and Mac OS
    - Safari on Mac OS
    - Internet Explorer on Windows

- Chrome on Windows, Linux and Mac OS.

11 The Infoblox NIOS on VMware software runs on VMWare ESX/ESXi; KVM Hypervisor (RHEL); and Nutanix AHV platforms. The servers 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 one of the hosts and then configured as a virtual appliance. The host appliance and VM OS are part of the operational environment and not part of the TOE. The following table lists the required memory, CPU, and disk allocation for each supported Infoblox virtual appliance model

Table 4: TOE hardware models

Infoblox Model	CPU	CPU Speed	Memory	Storage
TR/ND-805	IntelCorei36100TE (2.7Ghz Dual)	2.7GHz	32GB DDR4	1TB single fixed 7200rpm
TE-815	IntelCorei3-6100TE (2.7Ghz Dual)	1.10GHz	16gb DDR4	1TB single fixed 7200rpm
TE-825	Intel Core i3-6100TE	3.6 GHz	32GB	1TB
TR-1405	IntelXeonE31275v5 (3.6Ghz Quad)	3.6GHz	32GB DDR4	1.2TB RAID-1 FRU 2@10k
ND-1405	IntelXeonE31275v5 (3.6Ghz Quad) IntelXeonE31275v6 (3.6Ghz Quad)	3.6GHz	32GB DDR4	1.2TB RAID-1 FRU 2@10k
TE-1415	IntelXeonE31275v5 (3.6Ghz Quad)	1.2GHz	32GB DDR4	900GB single FRU 10k
TE-1425	Intel Xeon E3-1275	3.6 GHz	32GB	900GB
TR/ND-2205	IntelXeonE52620v4 (2.1Ghz 8)	performance governor	64GB DDR4	2.4TB RAID-10 FRU 4@10k
TE-2215	IntelXeonE52620v4 (2.1Ghz 8)	powersave governor	64GB DDR4	1.8TB RAID-10 FRU 4@10k
TE-2225	Intel Xeon E5-2620	2.1 GHz	64GB	1.8TB
TR/ND-4005	IntelXeonE52680v4 (2.4Ghz 14)	performance governor	128GB DDR4	3.6TB RAID-10 FRU 4@10k
TE-4015	Intel Xeon E5-2680	2.4 GHz	64GB	1.8TB
TE-4025	IntelXeonE52680v4 (2.4Ghz 14)	performance governor	128GB DDR4	1.8TB RAID-10 FRU 4@10k

Table 5: Resource Requirement for Virtual Appliances

NIOS Virtual Appliance	Primary Disk (GB)	# of CPU Cores	Memory Allocation (GB)
ND-V805	250	2	32
IB-V815	250	2	16
IB-V825	250	2	16
ND-V1405	250	4	32
IB-V1415	250	4	32
IB-V1425	250	4	32
ND-V2205	250	8	32
IB-V2215	250	8	64
IB-V2225	250	8	64
IB-V4005	250 (+ 1500 GB reporting storage)	14	128
ND-V4005	250	14	128
IB-V4015	250	14	128
IB-V4025	250	14	128
IB-V5005	User defined	User defined	User defined

1.5 Clarification of Scope

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

13 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]).

14 Potential consumers of the TOE are advised that some functions and services of the overall product have not 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.

1.6 Assumptions

15 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 Operational Environment Assumptions

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

Table 6: Assumptions for the TOE environment

Assumption	Statements
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.LIMITED_FUNCTIONALITY	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).
A.NO_THRU-TRAFFIC_PROTECTION	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.
A.PHYSICAL_PROTECTION	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.

Assumption	Statements
	This protection is assumed to be sufficient to protect the device and the data it contains.
A.TRUSTED_ADMINISTRATORS	The authorized administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. 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.
A.REGULAR_UPDATES	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.

1.7 Evaluated Configuration

17 The TOE may be deployed in a number of configurations consistent with the requirements identified in this Security Target (Ref [6]).

18 The evaluated configuration consists of the following appliances:

- HA Pair consisting of two Trinzic appliances: a Grid Master Appliance and a Grid Member - 'TE' or 'IB' appliances.
- Two Network Insight Appliances- one probe and one consolidator – 'ND' or 'IB' appliances.
- Threat Insight (streaming analytics) - 'TE' or 'IB' appliance.
- One Reporting and Analytics Grid Member appliance – 'TR' or 'IB' appliance.

19 During the testing activities, the TOE components were deployed in a multi-server configuration, which consists of all components listed above deployed in a combination of physical and virtual environments.

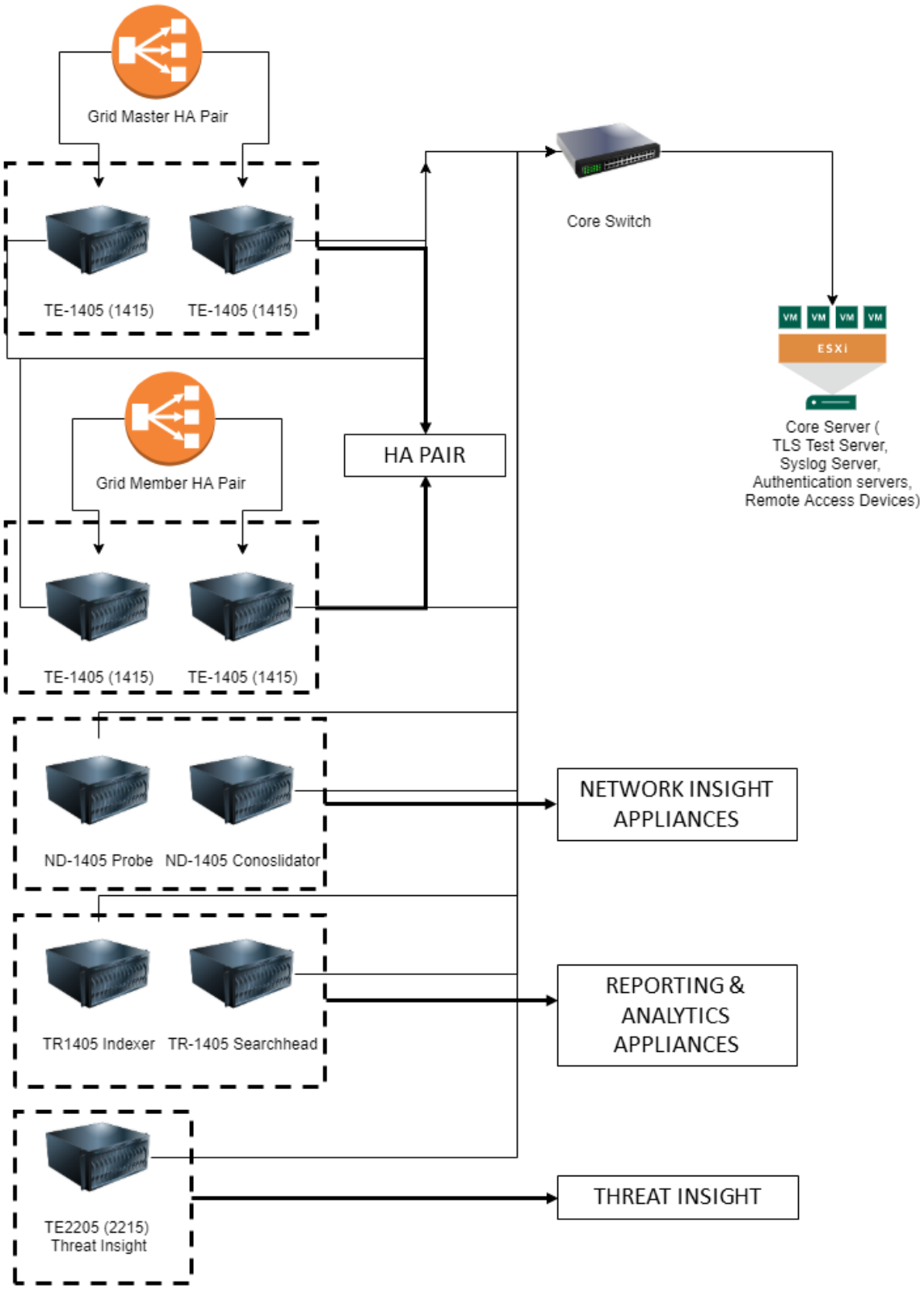

Figure 1: Test Environment Specifics

1.8 Delivery Procedures

20 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.

21 The delivery procedures 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 TOE Delivery

1.8.1.1 Software Delivery

22 Release engineering will notify Operations through email that the release is available.

23 Operations will download the release package from the release archive server, validate the checksum and install the release in the Manufacturing Test Lab on their network boot server. Operations will perform some basic tests on all supported hardware to validate that the release installs correctly and validate the TOE labelling.

24 Infoblox contracts Flextronics International Limited, Milpitas, CA and Avnet, San Jose, CA, to assemble the hardware appliances upon which the TOE operates and to install the software components. Only one of these will be used for a particular customer's delivery. The contractor used for particular delivery is hereafter referred to as the Contract Manufacturer. Which Contract Manufacturer is used for a particular customer delivery depends on which hardware and software versions are involved.

25 When the TOE has been validated by Operations internally Operations will hand carry a copy of the release package to the Contract Manufacturer. Operations will validate the checksum and install and test the release package in the same way as described

above for the Manufacturing Test Lab, there is a functionally identical setup at the Contract Manufacturer.

1.8.1.2 Hardware Delivery

26 There are two types of hardware delivery offered by Infoblox. They are Appliance Delivery and On-line Delivery.

27 **APPLIANCE DELIVERY**. Operations will get the sales order through the Oracle system and will enter/validate the software and hardware information and license data. After Operations has validated the order it is entered into the License Generator.

28 The Contract Manufacturer has access to the License Generator system through a secure VPN. The order is sent to the Contract Manufacturer via e-mail, this specifies the hardware model and software licenses required. The Oracle system also generates a shipping label which contains customer name and address, serial numbers of hardware and licenses and all TOE Labels.

29 Once an appliance (composed of no user-serviceable parts) has been assembled together with mechanical fastenings and tested, it is protected from tampering with a tamper-evident seal labels affixed on key locations to protect unauthorized access.

30 The Contract Manufacturer packages the TOE together with the shipping slip and included documentation in the shipping container.

31 Prior to receiving a customer order and initiating the software licensing process to fulfil a customer order the TOE is stored in its shipping carton which is placed on a standard warehouse rack within a secured warehouse. The secured warehouse is maintained by the Contract Manufacturer. The warehouse employs a security alarm and surveillance system. Entry by non-Contract Manufacturer personnel into the warehouse is controlled through one point of entry by a guard and requires individuals to sign-in with identification.

32 Upon receipt of the customer order, the TOE contained in its shipping carton is picked from the warehouse rack and then the software license is installed per the customer order. The TOE is then sealed within its shipping carton and shipping labels are applied to the outside of the carton. The TOE is shipped to customers via secure courier from the Contract Manufacturer using FedEx to provide delivery (unless another carrier is specifically requested by the customer). Customers are provided with tracking numbers for their order, and are able to review the status of their shipment from the courier's website using these numbers.

33 Infoblox stock replacement units at Flash Global depots. These are used to replace defective units. All handling/shipping of these units are handled by FedEx.

34 In some cases, the appliances are shipped from the Contract Manufacturers 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.

35 All Infoblox manufacturing and logistics partners are TAA compliant and ISO 9001 certified.

36 Customers are able to track the current location of the package en route using the tracking options of the common carrier. Once the package arrives, the customer can verify the product by comparing the shipping slip to the invoice.

37 The customer should also inspect the tamper-evident seals for any potential tampering.

38 **ON-LINE DELIVERY**. All general releases are made available to existing customers for On-line delivery. On-line delivery comes in two approaches, the first format is in "Virtual Image Format" initial deployment image for virtual platforms (OVA images for VM-Ware) and the second format is the NIOS release image (*.bin2). The Virtual Image Format is an industry standard delivery mechanism for virtual "systems", it is the initial delivery mechanism for Infoblox virtual platforms (in lieu of the above-described physical delivery model). 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 VM-Ware.

39 Release Engineering will copy the release package (except the Preboot Execution Environment (PXE) boot components) to a file server reachable from the Internet. Release Engineering is the only entity with write access to the file server.

40 Support controls all external access (read-only) to the file server and only gives access to registered customers with active maintenance agreements. Customers are notified of the existence of a release through email from Support. If the customer decides to upgrade, they will download the release package and store it locally. There are no assumptions about the security of file server; the customers file server client/local storage or the communication channel between them. The integrity of the whole delivery procedure is handled by the decryption and signature validation described below.

41 The file server is access through HTTP for general releases and FTP for limited releases.

42 The TOE administration interface contains an option for upgrading the system. The upgrade option is only available to security administrators. After the downloaded release package has been provided to the TOE, it will be uploaded to the TOE and the signature will be verified. If the package validates correctly the security administrator will be given the option to proceed with the upgrade of the TOE to the new version. It is not possible for the administrator to upgrade to a release package which does not validate as a correct package.

43 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.

1.9 Flaw Reporting Procedures

44 The evaluator 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.

45 The evaluator 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.

46 The evaluator 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.

47 The evaluator 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.

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

49 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.

50 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.

51 Therefore, the evaluator confirms that the information provided meets all requirements for content and presentation of evidence.

2 Evaluation

53 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 Augmented with 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

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

2.1.1 Life-cycle support

55 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the TOE provided for evaluation is labelled with its reference and the TOE references used are consistent.

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

57 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 ALC Life Cycle Support: Configuration Management version 0.3.

2.1.2 Development

Architecture

58 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.

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

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

61 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.

Functional Specification

62 The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

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

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

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

TOE Design Specification

65 The evaluators examined the TOE design (contained in [[8]]) and determined that the structure of the entire TOE is described in terms of subsystems.

66 The evaluators also determined that all subsystems of the TSF are identified.

67 The evaluators determined that interactions between the subsystems of the TSF were described.

68 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.

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

70 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.

71 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.

72 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

73 The evaluators examined the operational user guidance 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.

74 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.

75 The evaluators examined the operational user guidance in conjunction with other evaluation evidences 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.

76 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.

77 The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

78 Testing at EAL 2 Augmented with ALC_FLR.2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by BAE Systems Applied Intelligence Malaysia Lab – 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

79 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, 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). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

80 At EAL 2 Augmented with 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.

81 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 7: Independent Functional Test

TEST ID	DESCRIPTIONS	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 and provide only minimal feedback during the authentication process • Verify that authorised users are able to perform management of TSF data functions. • Verify that authorised users are able to determine and modify the behaviour of security management	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	functions and terminate their own interactive sessions. • Verify that the TSF shall maintain security roles. • 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. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs and associate them with the identity of the user that caused the event. • Very that the TSF provides a mechanism that provide password limitations.	
TEST-IND-002-GUI	• Verify that the TSF performs TOE access functions such as inactive session termination and display of TOE access banner. • Verify that authorised users are able to determine and modify the behaviour of security management functions. • Verify that the TSF restricts access to audit record and prevents audit	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	records from unauthorised deletion and modification. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs. • Verify that the TSF shall restrict ability to manage the TSF data to authorised administrators.	
TEST-IND-003-GUI	• Verify that the TSF implements DNSSEC protocol. • Verify that the TSF is able to send audit record to a trusted IT device such as a remote audit server. • Verify that the TSF shall overwrite the oldest audit log records first if the audit trail is full.	Passed. Result as expected.
TEST-IND-004-GUI	• Verify that core operation services remain active and the secure state is preserved in case of a hardware or device failover scenario. • Verify that the TSF can perform DNS Traffic analysis.	Passed. Result as expected.
TEST-IND-005-CLI	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that authorised users are able to perform management of TSF data functions.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	• Verify that authorised users are able to determine and modify the behaviour of security management functions. • Verify that the TSF performs TOE access functions such as inactive session termination and display of TOE access banner. • 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. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.	
TEST-IND-006-API	• To test the identification and authentication process of the TOE, security management function behaviours, and verify that the TSF shall maintain security roles and security attributes belonging to individual users. • To test the authentication failure handling process of the TOE and advisory warning message function.	Passed. Result as expected.

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

2.1.4.3 Penetration testing

83 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.

84 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack 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 (elapsed 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

85 The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched:

a) CVE (Common Vulnerabilities & Exposures) Details - https://www.cvedetails.com/vendor/1511/Infoblox.html

b) Infoblox Community Page - https://community.infoblox.com/

c) OWASP (Open Web Application Security Project) Testing Project - https://wiki.owasp.org/index.php/Category:OWASP_Testing_Project

86 The penetration tests focused on:

a) General vulnerability scan;

b) Web application vulnerability scan;

c) Input and data validation;

d) Unrestricted file upload;

e) Secure Communication.

87 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated

configuration and in a secure environment as specified in Section 2 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

88 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. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

3 Result of the Evaluation

89 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 v8.5.2 performed by BAE Systems Applied Intelligence Malaysia Lab – MySEF.

90 BAE Systems Lab – MySEF found that Infoblox Trinzic Appliances with NIOS v8.5.2 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 Augmented with ALC_FLR.2.

91 Certification is not a guarantee that a TOE is completely free from 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

92 EAL 2 Augmented with ALC_FLR.2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE to understand the security behaviours.

93 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 penetration attackers with a basic attack potential.

94 EAL 2 Augmented with ALC_FLR.2 also provides assurance through use of a configuration management system, the secure delivery procedures, and evidence of flaw remediation procedures.

3.2 Recommendation

95 The Malaysian Certification Body (MyCB) is strongly recommending that:

a) Potential purchasers of the TOE should consider the use of a CA (Certificate Authority) signed-certificate, as opposed to a self-signed certificate to fully secure the access to the TOE environment.

b) Potential purchasers of the TOE should consider using alternative ciphers and security measures to secure inter-network communications, to ensure that the operational environment provides mechanisms to protect all data communicated between remote users from disclosure and modification.

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

d) Potential purchasers of the TOE should ensure there are appropriate security controls in the TOE operational environment to ensure protection of the database and its stored data.

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 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v11, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2018.

[6] Infoblox Trinzic Appliances with NIOS v8.5.2 Security Target, Version 1.0, 15 June 2021.

[7] Infoblox Trinzic Appliances with NIOS v8.5.2, Evaluation Technical Report, Version 1.0, 6 March 2020.

[8] Infoblox Trinzic Appliances with NIOS v8.5.2 Design Specification, Version 0.3, 8 January 2021

A.2 Terminology

A.2.1 Acronyms

Table 8: 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

Acronym	Expanded Term
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 9: 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.

Term	Definition and Source
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.
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 ---