CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

C045 Certification Report

iDeras Unified Threat Management (UTM) v5.02

File name: ISCB-5-RPT-C045-CR-v1a
Version: v1a
Date of document: 4 November 2013
Document classification: PUBLIC

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

Securing Our Cyberspace

CyberSecurity Malaysia
(726630-U)

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C045 Certification Report

iDeras Unified Threat Management (UTM) v5.02

4 November 2013

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

Document Authorisation

DOCUMENT TITLE:	C045 Certification Report – iDeras Unified Threat Management (UTM) v5.02
DOCUMENT REFERENCE:	ISCB-5-RPT-C045-CR-v1a
ISSUE:	v1a
DATE:	4 November 2013

DISTRIBUTION:	UNCONTROLLED COPY – FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2013

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 4 November 2013, 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 at www.commoncriteriaportal.org).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

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 (Ref [4]) 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
v1	24 October 2013	All	Final Released.
v1a	4 November 2013	Page iv	Add the date of the certificate.

Executive Summary

iDeras Unified Threat Management (UTM) v5.02 (hereafter referred as iDeras) from Infosys Gateway Sdn Bhd is the Target of Evaluation (TOE) for the Evaluation Assurance Level 2 (EAL2) evaluation.

iDeras is a Unified Threat Management (UTM) or hybrid solution consists of firewall packet filtering technology, offering server hosting services, network security with management features, and gateway security management within a single appliance. The scope of the evaluation only covers network gateway functions that are responsible to manage the enterprise network traffic flow. iDeras includes other supporting features that are not part of TOE scope such as Intrusion Detection/Prevention, antimalware, content filtering, VPN, network management, hosting server, and other features specified in Section 2.6.3 of the Security Target (Ref [6]).

The scope of evaluation covers major security features as follow:

a) Identification and Authentication – TOE administrator can access TOE by providing username and password in the Webconfig interface and CLI interface. TOE administrator will be granted role based on built-in Groups, access to services and pages within Webconfig. Password for each administrator account is governed by password policy. TOE administrator is able to modify the existing configurable settings as per required by the organisational security policies implemented or enforced.

b) User Data Protection – The TOE has capabilities of protecting internal network from external network intrusion by using information flow controls between internal and external network. The TOE will check the inbound and outbound IP network protocols, contents and ports before allowing or rejecting the IP network and packets. TOE Administrator can configure packet filter rules and policies based on the subject and information security attributes. By default, all external (internet) traffic will be blocked. TOE administrator can configure any services, ports and protocols that are accessible between Internet and internal networks.

c) Security Management – TOE features can be managed through Webconfig and CLI by the TOE administrator. User of TOE, whom is assigned with TOE administrator roles, is configurable using built-in feature by assigning to administrator account “admin”. TOE administrator could enable, disable, modify the behaviour of services controlled by TOE packet filtering rules, user attributes values, network setting, time-of-day web access, NTP Time server, backup and restore configuration setting, restart and shutdown functions, password policies, and related functions of TOE.

d) Security Audit – The TOE will generate audit records for selected security events in several log files and categories. Each audited events will be recorded along with date and time of event, account user who performed the event, event name, system filename related to event and other event details. Audit record can be viewed by TOE administrator but it cannot be edited. TOE Administrator could select and filter the logs for easy viewing. TOE will create a new log file to store the audit records if the size limit is reached for a single log file. Limitation of the log storage is based on the internal hard disk equipped within the TOE appliance.

e) Protection of the TSF – The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. TOE prevents modification of date and time manually.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for TOE, the security function 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). 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 MySEF CyberSecurity Malaysia evaluation facility and completed on 21 October 2013.

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 www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of user to ensure that iDeras meet their requirements. It is recommended that a potential user of iDeras to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

1 Target of Evaluation 1

1.1 TOE Description 1

1.2 TOE Identification 2

1.3 Security Policy 3

1.4 TOE Architecture 3

1.4.1 Logical Boundaries 3

1.4.2 Physical Boundaries 6

1.5 Clarification of Scope 7

1.6 Assumptions 7

1.6.1 Usage assumptions 8

1.6.2 Environment assumptions 8

1.7 Evaluated Configuration 8

1.8 Delivery Procedures 8

1.9 Documentation 9

2 Evaluation 10

2.1 Evaluation Analysis Activities 10

2.1.1 Life-cycle support 10

2.1.2 Development 10

2.1.3 Guidance documents 10

2.1.4 IT Product Testing 11

3 Result of the Evaluation 15

3.1 Assurance Level Information 15

3.2 Recommendation 15

Annex A References 17

A.1 References 17

A.2 Terminology 17

A.2.1 Acronyms 17

A.2.2 Glossary of Terms 18

Index of Tables

Table 1: TOE identification 2
Table 2: Independent Functional Testing 11
Table 3: List of Acronyms 17
Table 4: Glossary of Terms 18

Index of Figures

Figure 1: Typical installation of iDeras which consist of the TOE........ 6

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), iDeras Unified Threat Management (UTM) v5.02 (hereafter referred as iDeras) is a Unified Threat Management (UTM) or hybrid solution consists of firewall packet filtering technology, offering server hosting services, network security with management features and gateway security management within a single appliance.

2 iDeras can be used as a hosting server, where it is pre-equipped with MySQL feature, web server hosting and RAID support feature. Its network management feature has the capabilities of recognising hardware and software network configuration within the existing enterprise network, managing domains, directories, files, remote printing services and messaging (email hosting) services. The gateway features are to manage enterprise network traffic flow with supporting security features of Intrusion Detection/Prevention, firewall packet filtering, antimalware, content filtration and many more. However, the scope of the evaluation only covers network gateway functions.

3 In the context of the evaluation, the TOE is expected to provide the following major security features:

a) **Identification and Authentication** - TOE administrator can access TOE by providing username and password in Webconfig interface and CLI interface. By default, administrator can use a built-in administrative account known as “admin” used for authenticating through Webconfig. TOE administrator will be granted role based on built-in Groups, access to services and pages within Webconfig. Password for each administrator account is governed by password policy. TOE administrator is able to modify the existing configurable settings as per required by the organisational security policies implemented or enforced.

b) **User Data Protection** - the TOE has capabilities of protecting internal network from external network intrusions by using information flow controls between internal and external network. The TOE will check the inbound and outbound IP network protocols, contents and ports before allowing or rejecting the IP networks and packets. TOE Administrator can configure packet filter rules and policies based on the subject and information security attributes. By default, all external traffic (internet) will be blocked. TOE administrator can configure any services, ports and protocols that are accessible between Internet and internal networks.

c) **Security Management** - TOE features can be managed through Webconfig and CLI by TOE Administrator. User of TOE, whom is assigned with TOE administrator roles, is configurable using built-in feature by assigning to administrator account “admin”. Administrator could enable, disable and modify the behaviour of services controlled by TOE, packet filtering rules, user attributes values, network settings, time-of-day web access, NTP Time Server, backup and restore configuration setting, restart and shutdown functions, password policies and related functions of TOE.

d) **Security Audit** – TOE will generates audit records for selected security events in several log files and categories. Each audited events will be recorded along with date and time of event, account user who performed the event, event name, system filename related to event and other event details. Audit record can be viewed by TOE administrator but it cannot be edited. TOE Administrator could select and filter the logs for easy viewing. TOE will create a new log file to store the audit records if the size limit is reached for a single log file. Limitation of the log storage is based on the internal hard disk equipped within the TOE appliance.

e) **Protection of the TSF** – The security audit function will generate audit record of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. TOE prevents modification of date and time manually.

1.2 TOE Identification

4 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	C045
TOE Name	iDeras Unified Threat Management (UTM)
TOE Version	5.02
Security Target Title	iDeras Security Target
Security Target Version	v1.3
Security Target Date	18 October 2013
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation 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 CC Part 3 Conformant Package conformant to EAL2

Sponsor and Developer	Infosys Gateway Sdn Bhd Unit 808, 8th Floor, Block E, Pusat Dagangan Phileo, Damansara 1, No.9, Jalan 16/11 off Jalan Damansara, 46350 Petaling Jaya, Selangor, Malaysia.
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

5 In order to ensure the security of the TOE and its environment, only authorised users are assigned by the organisation to have access to the TOE. Authorised users or administrators should also create and use the strong password that is complying with the organisation security policy implemented by the TOE and TOE operational environment (refer to Section 4.3 of the ST (Ref [6])).

6 The TOE enforces an information flow policy to restrict the ability of unauthenticated external IT entities that send and receive information to one another through the TOE. The TOE will check the inbound and outbound IP packets from unauthenticated external IT entities before allowing or rejecting the network traffic in forms of IP packets. The decision to allow or reject the network traffic will be based on the packet filtering rules created by the administrator through Webconfig and CLI interface.

7 The details of the security policy are described in Section 7.2 and Section 8 of the Security Target (Ref [6]).

1.4 TOE Architecture

8 The TOE includes both logical and physical boundaries which are described in Section 2.6 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

9 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:

a) **Identification and Authentication**

The TOE users (i.e. administrator) are required to perform identification and authentication via Webconfig login interface and CLI interface by providing username and password. By default, administrator can use a default build-in administrative account “admin” with password “admin” to be authenticated to Webconfig for the first time. Then the administrator should change the default password to a strong password based on the organisation security policy. Users will be granted role based on Built-in-Groups, access to services and pages in Webconfig. There are 3 built-in groups as follows:

i) *allusers* – contain all TOE users,

ii) *domain_admins* – Windows domain administrators, and

iii) *domain_users* – Windows domain users.

By default, TOE administrator will be in *allusers* group. For this evaluation, *domain_admins* and *domain_users* groups are not part of the evaluation scope.

By default, account "admin" has access to all services except Windows Networking. However, Windows Networking service can be enabled by administrator after successfully login to Webconfig.

A new account created by TOE administrator will have limited access to Webconfig pages and services. By default, a new account can only access account User Profile page to modify password and profiles. A new account user can also download security certificates in Security and Keys page (not in scope). A new account user can obtained administrator role if configured to access administrative page in Webconfig.

Password for each TOE administrator account is governed by a password policy that is configurable by the administrator as follows:

i) Minimum Password Length

ii) Minimum Password Age

iii) Maximum Password Age

iv) History size

The TOE enforce the users to setup the password that begins with a letter or number and must not contains characters "|"; which are build-in values that are not configurable by the TOE administrator.

b) User Data Protection

All data that pass through the TOE are protected by using information flow control policy where the TOE will check the inbound and outbound IP packets from unauthenticated external IT entities before allowing or rejecting the network traffic in forms of IP packets. The decision to allow or reject network traffic will be based on packet filter rules created by the administrator. Users must created packet filter rules based on the following criteria:

i) Source address of information (i.e. IP address, MAC address)

ii) Destination address of information (i.e. IP address, MAC address)

iii) Source port of information

iv) Destination port of information

v) Interface that the traffic arrives and departs

vi) Transport layer protocol information

vii) Service used by information

By default, all external (Internet) traffic will be blocked. TOE administrator will configure any services, protocols and ports that can be accessible from the

Internet. Pre-configured network traffic protocol listings are made available in the TOE. TOE administrator can block any unwanted network traffic using the ready-made protocol listings.

c) **Security Management**

The TOE functions can be managed by the administrator via 2 interfaces:

i) Console Interface Access through Command Line Interface (CLI) over SSH using RJ 45 cable, and

ii) Internal LAN Interface Access through Web Interface (Webconfig) over TLS/HTTPS in an internal network located in the same physical secure location.

By default, administrator account that is newly created will have limited access to the TOE. It is up to the default administrator account (username: admin) to give access to specific pages in Webconfig and access to the TOE core function. By default, administrator account can only access page to change their password and download security certificates (not part of the evaluation scope).

Administrator could enable, disable, or modify the management functionalities of TOE as mentioned in Section 8.3 of Security Target (Ref [6]).

By default, all external (Internet) traffic will be blocked. The administrator can configure any services, protocols and ports that can be accessible from the Internet. Pre-configured network traffic protocol listings are made available in the TOE. The administrator can block any unwanted network traffic using the ready-made protocol listings.

d) **Security Audit**

The TOE will generate audit record for selected security events in several log files. The security events that will be audited are as following:

i) Successful/failure authentication to iDeras web portal

ii) Web portal page accessed by user

iii) Reset user password

Each audited events will be recorded along with date and time of event, account user who performed the event, event name, system filename related to the event and other event details. Audit record can be viewed by administrator and cannot be modified. Administrator can select the log related to an event and/or filter the content of the log. Log filtering is executed by inserting the related key words in the filter field to search the log records in log file.

TOE will automatically create a new audit files to store the audit records if the size limit is reached for a log file. Refer to section 8.4 of Security Target (Ref [6]) for more details.

e) **Protection of the TSF**

The TOE enforces time stamps to be taken from a reliable source from the environment. This is important to ensure the integrity of the generated audit records where date and time will be captured together with the events. The NTP server is used as a reliable source from the TOE environment. However, NTP server is outside of the evaluation scope. The TOE will prevent manual modification of date and time in order to ensure the integrity of the date and time provided by the NTP server.

1.4.2 Physical Boundaries

10 The TOE is an application level firewall that provide traffic filtering, traffic inspection, network load controls, and content filtering of the network packets that travel in (incoming network packets) and out (outgoing network packets) of an organisation's networks.

11 The TOE executes on a dedicated hardware appliance model ID-1208 (Type:2U) or ID-2016 (Type:4U), with CentOS5 as the general operating system for the appliance. The hardware appliance and operating system are is not in the scope of this evaluation.

12 Figure 1 below describes the typical installation of iDeras which consist of the TOE.

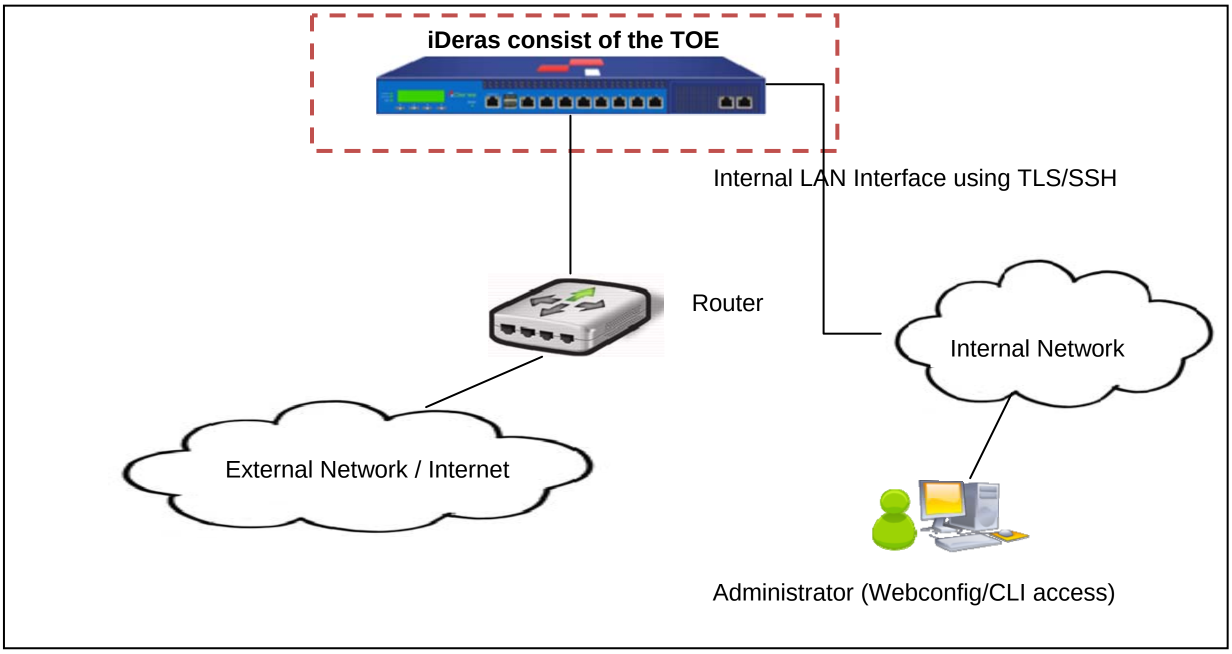
iDeras consist of the TOE
Internal LAN Interface using TLS/SSH
Router
Internal Network
External Network / Internet
Administrator (Webconfig/CLI access)

Figure 1: Typical installation of iDeras which consist of the TOE

13 The security architecture for the TOE has been designed in the various subsystems ensuring that the security principles have been inherently applied during the implementation of the TOE. Following are specific security architectural principles applied to the various TOE subsystems and architecture:

a) **OS kernel subsystem**: Provides the centralised controls for iDeras by providing memory management, process management and resources management for the services and daemons that run on the appliance.

b) **Logging subsystem**: Provides the TOE with the capability of capturing audit records from the various events of interest that should occur throughout the system. This subsystem also provides the mechanism for presenting audit records and logging data in a human-readable format; enables TOE administrators to select various presentation options.

c) **System subsystem**: Provides the underlying IP tools and local services used by the TOE administrator in managing and monitors various components of iDeras.

d) **Rules engine subsystem**: Provides the centralised capability in enforcing domain separation and enforcing information flow control policy for iDeras.

e) **Network subsystem**: Provides the underlying network packets routing and handling of IP packets that have arrived from the physical network interfaces.

f) **Proxy subsystem**: Provides the capability of configuring and establishing the information security policy associated with the Proxy services offered by TOE. This subsystem also provides the capability for configuring and establishing the information security policy associated with the application layer firewall functionality of the TOE.

g) **Rule-base subsystem**: Provides the capability of configuring and establishing the information security policy associated with the traffic filtering firewall functionality for the TOE.

h) **Management subsystem**: Provides the capability of configuring and establishing core administrative functions and policies for the TOE, such as identification, authentication and auditing/logging.

1.5 Clarification of Scope

14 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel, and secure communication in accordance with user guidance that is supplied with the product.

15 Section 1.4 of this document described the scope of the evaluation which was limited to those claimed made in the Security Target (Ref [6]). The TOE is an application level firewall that is responsible to manage the enterprise network traffic flow. Other components of iDeras which includes the hardware appliance, operating system, and other supporting features such as Intrusion Detection/Prevention, antimalware, content filtering, VPN, network management, hosting server, and other features specified in Section 2.6.3 of the Security Target (Ref [6]) are not part of TOE scope.

16 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.

1.6 Assumptions

17 This section summarises the security aspects of the environment/configuration in which IT product is intended to operate. Consumers should understand their own IT

environments and that required for secure operation of the TOE which has defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

18 Assumptions for the TOE usage as listed in Security Target are:

a) Data and information cannot flow through between internal and external networks and vice versa, unless it passes through the TOE.

b) The authorised TOE administrator is non-hostile and strictly follows the guidance documentation.

c) The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that secure and trusted connections can be established to the management network (i.e. through a trusted VPN or Virtual LAN).

d) Unauthorised users cannot access the TOE remotely from the internal, external or trusted networks.

e) Authorised TOE administrator will access the TOE using a secure connection.

1.6.2 Environment assumptions

19 Assumptions for the TOE environment listed in Security Target are:

a) The TOE and its environment are physically secure and managed by authorised TOE administrator.

b) The TOE environment will provide reliable time stamps and backup storage enough for TOE supporting operational environments.

1.7 Evaluated Configuration

20 The TOE is an application level firewall that pre-equipped with additional features known as Unified Threat Management (UTM), as described in Section 2.5 of the Security Target (Ref [6]). The TOE executes on a dedicated hardware appliance model ID-1208 (Type:2U) or ID-2016 (Type:4U), with CentOS5 as the general operating system for the appliance. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented user guidance (Ref 23c)) and defined in Section 2.5.3 of the Security Target (Ref [6]).

1.8 Delivery Procedures

21 iDeras is sent to the customers using delivery procedure (Ref 23a)), which ensures that the TOE is securely transferred from development environment to the responsibility of the customer. The brief delivery procedures are outlined below:

a) Procurement - Customer will purchase iDeras and complete the payment. Once payment is confirmed and legal documentation has been completed, the developer's (Infosys Gateway Sdn. Bhd) personnel will start the delivery process.

b) Delivery process – The Infosys Gateway personnel will prepare the User Guide documentation for iDeras. iDeras will be labelled with iDeras model's identification and serial number. iDeras casing is covered with security tape to avoid the product being tampered during distribution to customer. iDeras will be hand-delivered to customer.

c) Receipt and verification – Once the customer receive the product; the customer will acknowledge the delivery by accepting the receipts.

1.9 Documentation

22 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

23 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

a) iDERAS Delivery Order, v1, 6 September 2013

b) iDERAS Security Operational Procedure (2013-09-06-iDERAS-SOP-v1.1), v1.1, 6 September 2013

c) iDERAS User Guide (2013-03-21-iDERAS-User Guide-Rev1), v1, 6 September 2013.

2 Evaluation

24 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 (EAL2). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

26 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

27 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

28 The evaluators analysed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

29 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

30 The evaluators examined the TOE security architecture description; they 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.

2.1.3 Guidance documents

31 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to

securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

32 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from CyberSecurity Malaysia MySEF at CyberSecurity Malaysia MySEF lab. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

33 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).

34 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

35 At EAL2, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented developer tests.

36 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
Test Group A comprises a series of test cases on how TOE identified/authenticates user and its password policy.	Identification and Authentication	• between TOE and TOE Administrator • between TOE and Link-Layer • between TOE and IP • between TOE and TCP/UDP • between TOE and HTTPS	**PASS.** Result as expected.

		• between TOE and SSH • between TOE and FTP • between TOE and IRQ • between TOE and OS shell • between TOE and NTP • between TOE and Email Notification	
Test Group B comprises a series of test cases of auditing security events functions	Security Audit	• between TOE and TOE Administrator • between TOE and IRQ • between TOE and OS shell • between TOE and Link-Layer • between TOE and IP • between TOE and TCP/UDP • between TOE and HTTPS • between TOE and SSH • between TOE and FTP • between TOE and NTP • between TOE and Email Notification	**PASS.** Result as expected.
Test Group C comprises a series of test cases on how TOE mediates incoming and outgoing information of flow.	User Data Protection	• between TOE and IRQ • between TOE and Link-Layer • between TOE and IP • between TOE and TOE Administrator • between TOE and OS shell • between TOE and TCP/UDP • between TOE and HTTPS • between TOE and SSH • between TOE and FTP • between TOE and NTP • between TOE and Email	**PASS.** Result as expected.

		Notification	
Test Group D comprises a series of test cases of TOE management functions.	Security Management	• between TOE and IRQ • between TOE and Link-Layer • between TOE and IP • between TOE and TOE Administrator • between TOE and OS shell • between TOE and TCP/UDP • between TOE and HTTPS • between TOE and SSH • between TOE and FTP • between TOE and NTP • between TOE and Email Notification	**PASS.** Result as expected.
Test Group E comprises a series of test cases on how the TOE obtains time stamps from NTP server.	Protection of the TSF	• between TOE and IP • between TOE and TOE Administrator • between TOE and IRQ • between TOE and OS shell • between TOE and Link-Layer • between TOE and IP • between TOE and TCP/UDP • between TOE and HTTPS • between TOE and SSH • between TOE and FTP • between TOE and NTP	**PASS.** Result as expected.

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

2.1.4.3 Penetration Testing

38 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.

39 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 (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.

40 The penetration tests focused on:

a) Injection Attacks;

b) Information Gatherings;

c) Broken Authentication and Session Management;

d) Cross Site Scripting (XSS);

e) Insecure Direct Object References;

f) Cross-Site Request Forgery (CSRF);

g) Insecure Cryptography Storage;

h) Failure to Restrict URL Access;

i) Insufficient Transport Layer Protection;

j) Un-validated Redirects and Forwards;

k) Password Attack;

l) Configuration Backup File Unauthorised Modifications; and

m) Upload Malicious File.

41 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment together with the non-TOE hardware and software requirements as specified in Section 2.5.3 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

42 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.

3 Result of the Evaluation

43 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 iDeras Unified Threat Management (UTM) v5.02 performed by CyberSecurity Malaysia MySEF.

44 CyberSecurity Malaysia MySEF found that iDeras Unified Threat Management (UTM) v5.02 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level 2 (EAL2).

45 Certification is not 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

46 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

47 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.

48 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

49 In addition to ensure secure usage of the product, below are additional recommendations for iDeras users:

a) The TOE users are recommended to keep on updating, maintaining, backing up configuration, logs and related data/files of the TOE, auditing the security enforcing rules of the TOE and performing checks on the TOE regularly to maintain its secure operational environment.

b) A strict adherence to guidance documentations and procedures provided by the developer are highly recommended.

c) The TOE users should be aware and implement available security or critical updates related to the TOE security features and its supporting hardware, software, firmware or relevant guidance documents.

d) Users are advice to seek assistance or guidance directly from the developer of the TOE if specific requirements shall be configured or implemented by the TOE to meet certain policies, procedures and security enforcement within the users' organisation. This is important in order to reduce operational error, misconfiguration, malfunctions or insecure operations of the TOE that may compromise the confidentiality, integrity and availability of the assets that is protected by the TOE.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

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

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

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] iDeras Security Target, v1.3, 18 October 2013.

[7] E028 Evaluation Technical Report for iDERAS Unified Threat Management (UTM) v5.02, v1.2, 21 October 2013

A.2 Terminology

A.2.1 Acronyms

Table 3: 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
CLI	Command Line Interface
EAL	Evaluation Assurance Level
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
LAN	Local Area Network
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme

Acronym	Expanded Term
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
NTP	Network Time Protocol
PP	Protection Profile
RAID	Redundant Array of Independent Disk
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
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.

Term	Definition and Source
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
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.
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.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

--- END OF DOCUMENT ---