CyberSecurity Malaysia
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

# C055 Certification Report

## HP TippingPoint Intrusion Prevention Systems, comprising the S7500NX, S7100NX, S6200NX, S5200NX, S2600NX, S1400N, and S660N model appliances running TippingPoint Operating System v3.7.2

File name: ISCB-5-RPT-C055-CR-v1
Version: v1
Date of document: 9 March 2015
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme
mycc

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

CyberSecurity Malaysia
(726630-U)

Best Brand Internet Security 2008 & 2009
MS ISO/IEC 17021: 2011 ISMS 02082013 CB 02
MSC Malaysia Status Company

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

*Securing Our Cyberspace*

# C055 Certification Report

## HP TippingPoint Intrusion Prevention Systems, comprising the S7500NX, S7100NX, S6200NX, S5200NX, S2600NX, S1400N, and S660N model appliances running TippingPoint Operating System v3.7.2

9 March 2015
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

# Copyright Statement

Registered office:
Level 5, Sapura@Mines,
No 7 Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 726630-U

*Printed in Malaysia*

# Foreword

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

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

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

This certification report is associated with the certificate of product evaluation dated 18 March 2015, 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).

Reproduction of this report is authorized 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 |
|---|---|---|---|
| d1 | 26 February 2015 | All | Initial draft of certification report. |
| v1 | 9 March 2015 | All | Final version of certification report |

# Executive Summary

HP TippingPoint Intrusion Prevention System from HP is the Target of Evaluation (TOE) for the Evaluation Assurance Level 3 Augmented with ALC_FLR.2 Evaluation.

The HP TippingPoint Intrusion Prevention System (IPS) devices, comprising the S7500NX, S7100NX, S6200NX, S5200NX, S2600NX, S1400N, and S660N model appliances running TippingPoint Operating System v3.7.2. The devices covered within the scope of the evaluation are network-based intrusion prevention system appliances that are deployed in-line between pairs of networks.

The TOE is a hardware and software appliance that contains all the functions needed for intrusion prevention, including Internet Protocol (IP) defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of network protocols.

The primary function of the TOE is to protect networks from intrusion attempts by scanning network traffic, detecting intrusion attempts, and reacting to detected intrusion attempts according to the filters and action sets with which the device is configured.

The scope of evaluation covers major security features as follows:

a) Security Audit: The TOE is able to generate auditable events for the basic level of audit.

b) Identification and authentication: The TOE identifies and authenticates all administrative users of the TOE before granting them access to the TOE.

c) Intrusion Detection and Prevention: The TOE collects network traffic and subjects it to statistical and signature-based analysis, depending on configured IPS filters.

d) Traffic Management: The TOE can be configured to operate as a firewall, blocking or permitting network traffic based on protocol or IP address and port.

e) Security Management: The TOE provides the security management functions to enable the administrative users to manage user accounts, audit data and audit configurations, security configuration data, traffic management filters, and IDS data collection, analysis, and reaction.

f) TSF Protection: The TOE includes its own time source for providing reliable time stamps that are used in audit records and stored IDS data.

g) Trusted Path: The TOE provides a trusted path for remote administrative users of the TOE to communicate with the TOE. The trusted path is implemented over the network management port using HTTPS for access to the LSM and SSHv2 for access to the CLI.

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 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 3 (EAL3) 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 Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 30 January 2015.

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

# Table of Contents

# Index of Tables

# 1 Target of Evaluation

## 1.1 TOE Description

1 The Target of Evaluation (TOE) is the HP TippingPoint Intrusion Prevention Systems (IPS) devices, comprising the S7500NX, S7100NX, S6200NX, S5200NX, S2600NX, S1400N, and S660N model appliances running TippingPoint Operating System v3.7.2. The Target of Evaluation (TOE), is HP TippingPoint version 3.7.2 (hereinafter referred to as HP TippingPoint) are network-based intrusion prevention system appliances that are deployed in-line between pairs of networks.

2 The TOE is a hardware and software appliance that contains all the functions needed for intrusion prevention, including Internet Protocol (IP) defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of network protocols.

3 The primary function of the TOE is to protect networks from intrusion attempts by scanning network traffic, detecting intrusion attempts, and reacting to detected intrusion attempts according to the filters and action sets with which the device is configured. A filter comprises rules and conditions used by the TOE to detect and handle malicious network traffic. Each filter includes an action set that determines the TOE’s response when network traffic matches a filter.

4 The TOE provides intrusion prevention for the network according to the number of network connections and hardware capabilities of the specific model. A single instance of the TOE can be installed at the perimeter of the network, at the network core, on the customer’s Intranet, or in all three locations. HP TippingPoint IPS devices can secure up to 24 network segments depending upon traffic volumes and the load capacity of the model.

5 The details of TOE functions can be found starting in section 2.1 of the Security Target version 1.0

6 There are seven security functionalities covered under the scope of the evaluation which are:

| Security Function | Description |
|---|---|
| Security Audit | The TOE is able to generate auditable events for the basic level of audit. It provides Super-user administrative users with the ability to review audit records stored in the audit trail and prevents other administrative user roles from reviewing the audit data. |
| Identification and Authentication | The TOE identifies and authenticates all administrative users of the TOE before granting them access to the TOE. The TOE associates a user identity, authentication data (password), and authorizations (or security role) with each user. |

| | |
|---|---|
| Intrusion Detection and Prevention | The TOE collects network traffic and subjects it to statistical and signature-based analysis, depending on configured IPS filters. If the analysis of collected network traffic indicates a potential intrusion attempt, an action set associated with the detecting filter is triggered. |
| Traffic Management | The TOE can be configured to operate as a firewall, blocking or permitting network traffic based on protocol or IP address and port. |
| Security Management | The TOE defines three security management roles: Super-user; Administrator; and Operator. The TOE provides the security management functions to enable the administrative users to manage user accounts, audit data and audit configurations, security configuration data, traffic management filters, and IDS data collection, analysis, and reaction. |
| TSF Protection | The TOE includes its own time source for providing reliable time stamps that are used in audit records and stored IDS data. |
| Trusted Path | The TOE provides a trusted path for remote administrative users of the TOE to communicate with the TOE. The trusted path is implemented over the network management port using HTTPS for access to the LSM and SSHv2 for access to the CLI. |

## 1.2 TOE Identification

7 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** | C055 |
| **TOE Name** | HP TippingPoint Intrusion Prevention Systems |
| **TOE Version** | 3.7.2 |
| **Security Target Title** | HP TippingPoint Intrusion Prevention Systems Security Target |

| | |
|---|---|
| **Security Target Version** | 1.0 |
| **Security Target Date** | 9 Jan 2015 |
| **Assurance Level** | Evaluation Assurance Level 3 (EAL3) Augmented with ALC_FLR.2 |
| **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<br>CC Part 3 Conformant<br>Package conformant to EAL3 Augmented (ALC_FLR.2) |
| **Sponsor and Developer** | HP TippingPoint<br>14231 Tandem Blvd<br>Austin, Texas 78728<br>USA |
| **Evaluation Facility** | BAE Systems Applied Intelligence MySEF |

## 1.3 Security Policy

8 There are no organisational security policies that have been defined regarding the use of the TOE.

## 1.4 TOE Architecture

9 The TOE includes both logical and physical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

10 The following figure 1 and figure 2 shows the subsystems that comprise the TOE:

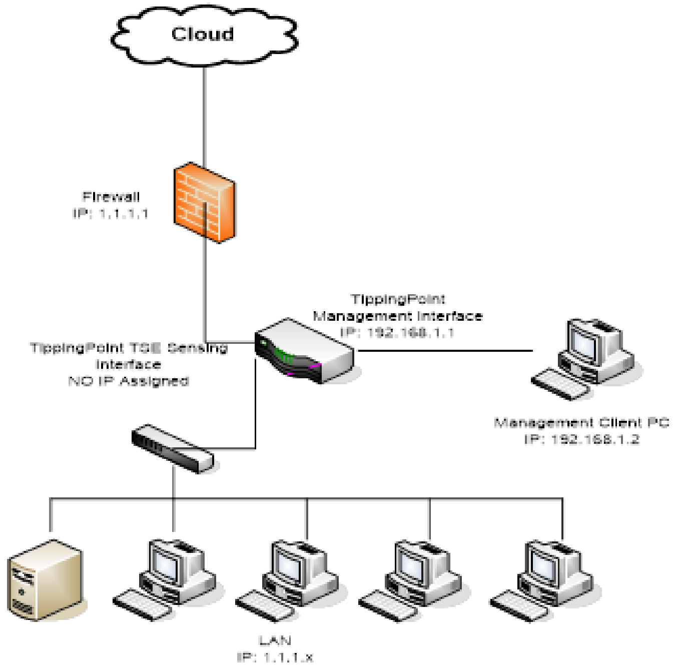

Figure 1

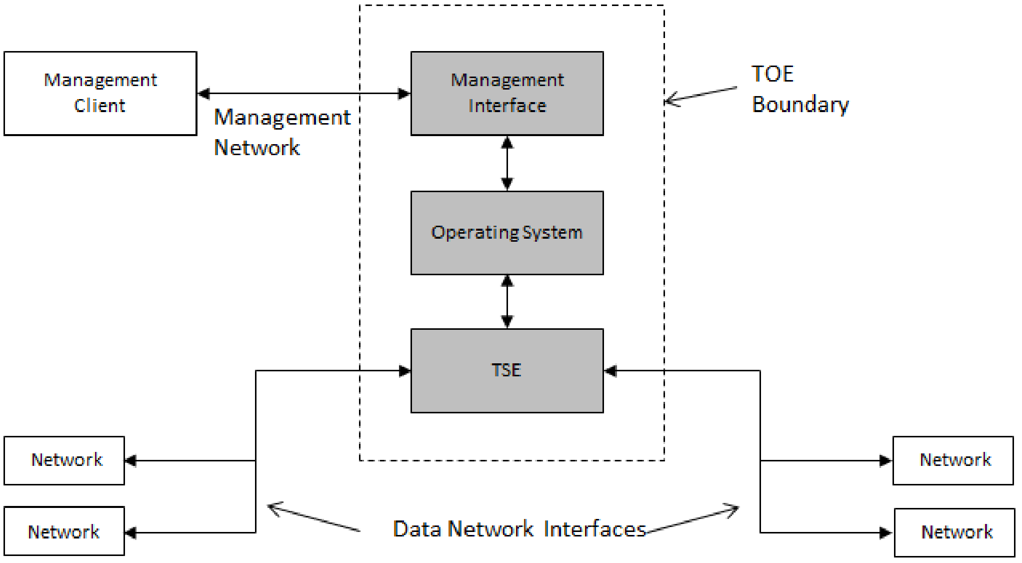

Figure 2

### 1.4.1 Logical Boundaries

11 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) Security Audit: The TOE is able to generate auditable events for the basic level of audit. It provides Super-users with the ability to review audit records stored in the audit trail and prevents other administrative user roles from reviewing the audit data. Super-users are able to select auditable events to be audited, based on event type. The audit records are stored in the underlying file system, where they are protected from unauthorized modification and deletion. When the space available for audit storage is exhausted, the oldest 50% of audit records are deleted and an audit record to this effect is generated.

b) Identification and authentication: The TOE identifies and authenticates all administrative users of the TOE before granting them access to the TOE. The TOE associates a user identity, authentication data (password), and authorizations (or security role) with each user. The TOE enforces minimum requirements for the construction of user passwords and provides a mechanism to lock or disable a user account after a configured number of consecutive failed attempts to logon.

c) Intrusion Detection and Prevention: The TOE collects network traffic and subjects it to statistical and signature-based analysis, depending on configured IPS filters. If the analysis of collected network traffic indicates a potential intrusion attempt, an action set associated with the detecting filter is triggered. The action set determines if the traffic is permitted or blocked. If traffic is permitted, an alert will be written to the IDS data log (specifically, the Alert log). If traffic is blocked, writing an alert to the IPS data log (specifically, the Block log) is configurable—in the evaluated configuration, action sets that block traffic must also be configured to generate an alert. In addition to writing to the IDS data log, the TOE can generate alerts in the form of a notification to a syslog server, email address, or SNMP server. The TOE provides capabilities for the administrative users to review the IDS data logs. The TOE protects the IDS data logs from modification and deletion. When the space available for IDS data storage is exhausted, the oldest 50% of IDS data is deleted and an audit record to this effect is generated.

d) Traffic Management: The TOE can be configured to operate as a firewall, blocking or permitting network traffic based on protocol or IP address and port. Network traffic that is permitted based on traffic management filtering is still subject to IPS filtering, unless the traffic management filter is configured to allow traffic through the device without IPS filtering. On the NX models, inspection bypass rules can be configured that permit matching network traffic to pass through the TOE without being subject to either traffic management or IPS filters.

e) Security Management: The TOE defines three security management roles: Super-user; Administrator; and Operator. The TOE provides the security management functions to enable the administrative users to manage user accounts, audit data and audit configurations, security configuration data, traffic management filters, and IDS data collection, analysis, and reaction. The Super-user role has full access to all management functions and data. The Administrator role is restricted to managing IDS and traffic management filters and reviewing configuration and IDS data. The Operator role is restricted to reviewing configuration and IDS data.

f) TSF Protection: The TOE includes its own time source for providing reliable time stamps that are used in audit records and stored IDS data.

g) Trusted Path: The TOE provides a trusted path for remote administrative users of the TOE to communicate with the TOE. The trusted path is implemented over the network management port using HTTPS for access to the LSM and SSHv2 for access to the CLI. Remote users initiate the trusted path by establishing an HTTPS connection (using a supported web browser) or SSH session (using an SSH client). The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS or SSHv2 ensures all communication over the trusted path is protected from disclosure and undetected modification.

The TOE supports a FIPS mode of operation and, when configured in FIPS mode, will allow only FIPS 140-2 approved cryptographic algorithms to be used. Note the TOE is not required to operate in FIPS mode to be in the evaluated configuration—the choice to do so or not is left up to the customer.

### 1.4.2 Physical Boundaries

12 The TOE includes both logical and physical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

## 1.5 Clarification of Scope

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

14 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]). The HP TippingPoint Intrusion Prevention System is a hardware-based intrusion prevention platform consisting of network processor technology and HP TippingPoint’s own set of custom Field Programmable Gate Arrays (FPGAs). The TOE is a hardware and software appliance that contains all the functions needed for intrusion prevention, including Internet Protocol (IP) defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of network protocols.

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

## 1.6 Assumptions

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

### 1.6.1 Usage assumptions

17 Assumption for the TOE usage as listed in Security Target :

a) It is assumed that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

b) The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

### 1.6.2 Environment assumptions

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

a) TOE has access to all the IT System data it needs to perform its functions.

b) The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

## 1.7 Evaluated Configuration

19 A single instance of the TOE can be installed at the perimeter of the network, at the network core, on the customer's Intranet, or in all three locations. HP TippingPoint IPS devices can secure up to 24 network segments depending upon traffic volumes and the load capacity of the model.

A network segment is the portion of a computer network in which computers can access each other using a data link layer protocol (e.g., in Ethernet, this would be the ability to send an Ethernet packet to others using their MAC addresses). The TOE is installed in a network such that all traffic to and from a group of hosts is mediated by the TOE. A segment uses two ports on the TOE and all traffic flows between connected networks through the TOE. Members of the segment are hosts connected to those ports (as described in Section 2.2 of the Security Target (Ref [6]).

## 1.8 Delivery Procedures

20 The delivery process for the TOE is as follows:

a) Delivery requirements call for system controls and procedures that provide assurance in the delivery of the sender-intended TOE or product, without any modifications. For a valid delivery, what is received must correspond precisely to the TOE master copy, thus avoiding any tampering with the actual version, or substitution of a false version. Several procedures are necessary for TippingPoint to maintain security when distributing versions of the TOE or parts of it to a user's site. This section will present the procedures followed by TippingPoint during manufacture of the TOE.

b) Preparing for Release and Product Manufacture

  a. These procedures ensure that the TOE is manufactured in a manner that maintains the security of the TOE throughout the manufacturing cycle.

c) Product Documentation

  a. There is a small subset of documents that are shipped with each product. The documents include a Quick Start Guide, Warranty and Licensing information, Safety and Compliance information, and a Documentation contents notice.

d) Delivery for Customers

  a. Hardware: Once the TOE is manufactured, it is securely packaged. Packaging tape is used to seal the packages containing the hardware/software TOE and the accessory Kit, respectively.

b. Software Updates & Download: As part of the delivery process, TOE software updates are posted on the Threat Management Center (TMC) website. This site requires authentication via the customer assigned credentials.

c. Product Identification: The hardware is labelled externally with the hardware model number. This number identifies the hardware model and can be matched by the customer against the label on the shipping box to verify that they have received the correct, certified hardware.

e) Identification of Proper Delivery: There are several mechanisms provided in the above process for a customer to ensure that they have received a product that has not been tampered with.

a. Outside packaging. If the outside shipping box and tape have not been broken, and the outside shipping label properly identifies the customer and the product, then the product has not been tampered with.

b. Inside packaging. If the plastic bag or seal on the plastic bag is damaged or removed, the device may have been tampered with.

c. Tamper seals. If any tamper seals are broken or removed, the device or software may have been tampered with.

f) All the delivery procedures described details can be found at, HP TippingPoint IPS N and NX Platforms Delivery of Product to Buyer, Rev D, 19 Dec 14.

## 1.9 Documentation

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

22 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) Command Line Interface Reference TOS Version 3.7, April 2014

b) HP TippingPoint Read Me First - Registering and Contacting Support, Feb 2014

c) Local Security Manager (LSM) User's Guide for TOS v3.7, April 2014

d) MIB Guide for TOS v3.7, April 2014

e) N-Platform Hardware Installation and Safety Guide, October 2013

f) NX-Platform Hardware Installation and Safety Guide, 2013

g) NX-Platform Quick Start, April 2014

h) Quick Start TippingPoint N-Platform, Rev A5

i) TippingPoint Operating System V. 3.7.0 Release Notes, April 2014

j) Using the TippingPoint External Compact Flash, November 2010

# 2 Evaluation

23 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

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

### 2.1.1 Life-cycle support

25 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.

26 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

27 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).

28 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.

29 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

30 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

31 Testing at EAL3 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

#### 2.1.4.1 Assessment of Developer Tests

32 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).

33 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

34 At EAL3, 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.

35 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The evaluators confirmed that the developer supplied test documentation includes test plans, expected test results and actual test results. The result of the independent functional tests were developed and performed by the evaluators are consistent with the expected test results in the test documentation.

| Identifier | Security Function | Descriptions |
|---|---|---|
| F001 | FAU_STG.2.1, FAU_STG.2.2, FAU_STG.2.3, FAU_STG.4.1, FAU_SEL.1.1, FMT_SMF.1.1, FMT_MTD.1.1(4), FMT_MTD.1.1(5) | This test aims to verify that the TOE protects the audit records from unauthorised modification or deletion, and that only authorised users are able to perform such actions. |
| F002 | FPT_STM.1.1 | This test aims to verify that the TOE is able to provide reliable timestamps. |
| F003 | FMT_SMR.1.1, FMT_SMR.1.2 | This test aims to verify that the TOE maintains and associates users with roles. |
| F004 | FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3 | This test aims to verify that the TOE is able to provide a communication path between |

| Identifier | Security Function | Descriptions |
|---|---|---|
| | | itself and remote users that is assured identification of its end points and protection of communicated data from disclosure or undetected modification. |

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

#### 2.1.4.3 Penetration Testing

37 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.

38 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.

39 The penetration tests focused on:

a) Identification of Common Vulnerabilities

b) Network Packet Sniffing on the Communication Transaction between TOE and TOE

c) SQL Injections

d) Cross Site Scripting (XSS)

e) Broken Authentication & Session Management

f) Password Attack

g) Directory Traversal

40 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 as specified in Section 1.5.3 of the Security Target (Ref [6]).

#### 2.1.4.4 Testing Results

41 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. In addition, the documentation supplied as evidence for the EAL3 + ALC_FLR.2

Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

# 3 Result of the Evaluation

42 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 HP TippingPoint performed by BAE Systems Applied Intelligence MySEF.

43 BAE Systems Applied Intelligence MySEF, found that HP TippingPoint 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 3 Augmented with ALC_FLR.2 (EAL3+ALC_FLR.2).

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

## 3.1 Assurance Level Information

45 EAL3 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.

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

47 EAL3 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

## 3.2 Recommendation

48 The following recommendations are made:

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

b) The administrators should make themselves familiar with the administrator guidance provided with the TOE and pay attention to all security warnings.

# 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] HP TippingPoint Intrusion Prevention Systems Security Target, Version 1.0, 09 January 2015

[7] C055 Evaluation Technical Report for HP TippingPoint, EMY003494-S025-ETR-1.0, v1.0, 23 February 2015

## A.2 Terminology

### A.2.1 Acronyms

Table 2: List of Acronyms

| Acronym | Expanded Term |
|---|---|
| CB | Certification Body |
| Authentication Data | It is information used to verify the claimed identity of a user. |
| SFP | Security Function Policy |
| SMS | Security Management System—HP TippingPoint name for its architecture for managing multiple IPS devices. |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| TOS | TippingPoint Operating System—the software component of the HP TippingPoint IPS device |
| TSE | Threat Suppression Engine—a logical component of the HP TippingPoint IPS device |
| TSF data | Data created by and for the TOE, which might affect the operation of the TOE. |
| UDP | User Datagram Protocol |

| Acronym | Expanded Term |
|---|---|
| TSC | TOE Scope of Control, the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP |
| TSP | TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed. |
| Unauthorized users | Unauthorized users can mean a legitimate user with access rights to certain web resource, an external entity that has no rights to any protected resource or data. |
| Users | It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, there are users of the TOE access the TOE through a web browser. |
| User data | Data created by and for the user, which does not affect the operation of the TSF. |
| Audit records | An individual item of information contained in an audit trail |
| CC | Common Criteria (ISO/IEC15408) |
| CEM | Common Evaluation Methodology (ISO/IEC 18045) |
| CCRA | Common Criteria Recognition Arrangement |
| TSF | TOE Security Functions |
| TSFI | TOE Security Functions Interface |
| SFR | Security Functional Requirement |
| CLI | Command Line Interface |
| IEC | International Electrotechnical Commission |
| ISO | International Organisation for Standardization |
| ISCB | Information Security Certification Body |
| MyCB | Malaysian Common Criteria Certification Body |
| MyCC | Malaysian Common Criteria Evaluation and Certification Scheme |
| MyCPR | MyCC Scheme Certified Products Register |
| MySEF | Malaysian Security Evaluation Facility |
| PP | Protection Profile |
| ST | Security Target |
| TOE | Target of Evaluation |

### A.2.2 Glossary of Terms

Table 3: Glossary of Terms

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

| Term | Definition and Source |
|---|---|
| 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 ---