National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

HP TippingPoint

Intrusion Prevention Systems

Report Number:	**CCEVS-VR-VID10345-2011**
Dated:	**31 August 2011**
Version:	**1.0**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell

MITRE
Bedford, MA

Jean Hung

MITRE
Bedford, MA

Common Criteria Testing Laboratory

SAIC
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the HP TippingPoint Intrusion Prevention Systems product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in August 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 2. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 3 augmented with ALC_FLR.2. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The TOE is a hardware-based intrusion prevention platform comprising the HP TippingPoint Intrusion Prevention System (IPS) devices, including the models S6100N, S5100N, S2500N, S1400N, and S660N running TippingPoint Operating System v3.2.1, and the models S330, S110 and S10 model appliances running TippingPoint Operating System version 3.1.4. The IPS devices consist of network processor technology and HP Networking’s own set of custom Field Programmable Gate Arrays (FPGAs) and are hardware and software appliances that contain 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 products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the HP TippingPoint Intrusion Prevention Systems Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	HP TippingPoint Intrusion Prevention System (IPS) devices, comprising: o The model appliances S6100N, S5100N, S2500N, S1400N, and S660N running TippingPoint Operating System v3.2.1, and o The model appliances the S330, S110 and S10 running TippingPoint Operating System version 3.1.4.
Sponsor:	Enterprise Security Products TippingPoint/Hewlett-Packard Corporation 14231 Tandem Blvd. Austin, TX. 78728

Developer:	Enterprise Security Products TippingPoint/Hewlett-Packard Corporation 14231 Tandem Blvd. Austin, TX. 78728
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	24 April 2009
Completion Date:	30 August 2011
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 2, September 2007.
Evaluation Class:	EAL 3 augmented with ALC_FLR.2
Description:	HP TippingPoint Intrusion Prevention System devices are hardware-based intrusion prevention platforms consisting of network processor technology and HP Networking's own set of custom Field Programmable Gate Arrays (FPGAs). Each device is a hardware and software appliance that contains 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.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the HP TippingPoint Intrusion Prevention System devices product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, 25 July 2007 (IDSSPP).
Evaluation Personnel:	Science Applications International Corporation: Katie Sykes Dawn Campbell
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its IT environment are intended to counter:

- An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
- An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
- An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- Unauthorized attempts to access TOE data or security functions may go undetected.
- Improper security configuration settings may exist in the IT System the TOE monitors.
- Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
- Vulnerabilities may exist in the IT System the TOE monitors.
- The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
- The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
- The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
- Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
- Inadvertent activity and access may occur on an IT System the TOE monitors.
- Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

1.4 Organizational Security Policies

The ST identifies the following organizational security policies that the TOE and its IT environment are intended to fulfill:

- Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

- Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
- The TOE shall only be managed by authorized users.
- All data collected and produced by the TOE shall only be used for authorized purposes.
- Users of the TOE shall be accountable for their actions within the IDS.
- Data collected and produced by the TOE shall be protected from modification.
- The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

2 Identification

The evaluated product is **HP TippingPoint Intrusion Prevention System devices**, comprising:

- The model appliances S6100N, S5100N, S2500N, S1400N, and S660N running TippingPoint Operating System v3.2.1, and
- The model appliances the S330, S110 and S10 running TippingPoint Operating System version 3.1.4.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the HP TippingPoint Intrusion Prevention System devices security policy has been extracted and reworked from the HP TippingPoint Intrusion Prevention System devices ST and Final ETR.*

3.1 Security Audit

The TOE is able to generate auditable events for the basic level of audit. It provides Superuser 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. Superuser administrative 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.

3.2 Identification and Authentication

The TOE identifies and authenticates all administrative users[1] 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

[1] That is, those users who access the TOE for administrative purposes via the network management port or console port. Since the TOE is invisible to users on the networks being monitored by the TOE, there is no concept of such users being able or required to identify or authenticate themselves to the TOE.

to lock or disable a user account after a configured number of consecutive failed attempts to logon.

3.3 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 System data log (specifically, the Alert log). If traffic is blocked, writing an alert to the System 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 System data, 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 System data logs. The TOE protects the System data logs from modification and deletion. When the space available for System data storage is exhausted, the oldest 50% of System data is deleted and an audit record to this effect is generated.

3.4 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 S6100N, S5100N, and S2500N 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.

3.5 Security Management

The TOE defines three security management roles: Superuser; 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 System data collection, analysis, and reaction. The Superuser role has full access to all management functions and data. The Administrator role is restricted to managing IPS and traffic management filters and reviewing configuration and System data. The Operator role is restricted to reviewing configuration and System data.

3.6 Protection of the TSF

The TOE includes its own time source for providing reliable time stamps that are used in audit records and stored System data.

3.7 Trusted Path/Channels

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. All models of the TOE have completed FIPS 140-2 validation (Certificate #1545). 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.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 3 augmented with ALC_FLR.2).
2. This evaluation only covers the specific model numbers and software version identified in this document, and not any earlier or later versions released or in process.
3. The TOE is not required to be configured in FIPS mode in the evaluated configuration.
4. The TOE utilizes third-party software and hardware components in its operational environment, as follows:
    a. Serial terminal client, connected via the serial console port, to support local management of the TOE via the CLI
    b. Management client PCs, connected via the network management port, to support remote management of the TOE. The management client PC in turn requires:

i. A browser (Internet Explorer 6.x or higher; Firefox 1.5+; Mozilla 1.7+; or Netscape 8.1+) to connect to the LSM; and/or

ii. An SSHv2 client to connect to the CLI

c. Syslog server, SMTP server, and/or SNMP server, connected via the network management port, to receive alarms.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and design documentation.

5.1 Deployment Architecture

The HP TippingPoint IPS is designed for network transparency. The HP TippingPoint IPS is deployed into the network to be monitored with no IP address or MAC address assigned, and immediately begins filtering unwanted traffic.

The HP TippingPoint IPS is installed such that traffic to internal hosts flows through the IPS. This is shown in Figure 1 as the “Sensing Interface”. The S6100N, S5100N, S2500N, S1400N, and S660N appliance models are equipped with 10 1GbE copper ports paired into 5 segments, and 10 1GbE fiber ports paired into 5 segments. The S6100N, S5100N, and S2500N models also include 2 10GbE fiber ports paired into 1 10GbE segment. The S10 device is equipped with 4 10/100/1000BASE-T ports paired into two segments, while the S110 and S330 devices are both equipped with 8 10/100/1000BASE-T ports, paired into four segments. Additionally, each HP TippingPoint IPS has two dedicated management interfaces: a 1GbE network port and an RJ-45 serial console port. This is represented in Figure 1 as the Management Interface.

Administrators access the Management Interface using a web-based interface—the Local Security Manager (LSM)—or via a command line interface (CLI).

Once installed in the network, the TOE intercepts network packets as they pass through the TOE. These packets are inspected to determine whether they are legitimate or malicious. This determination is made based upon filters configured on the TOE.

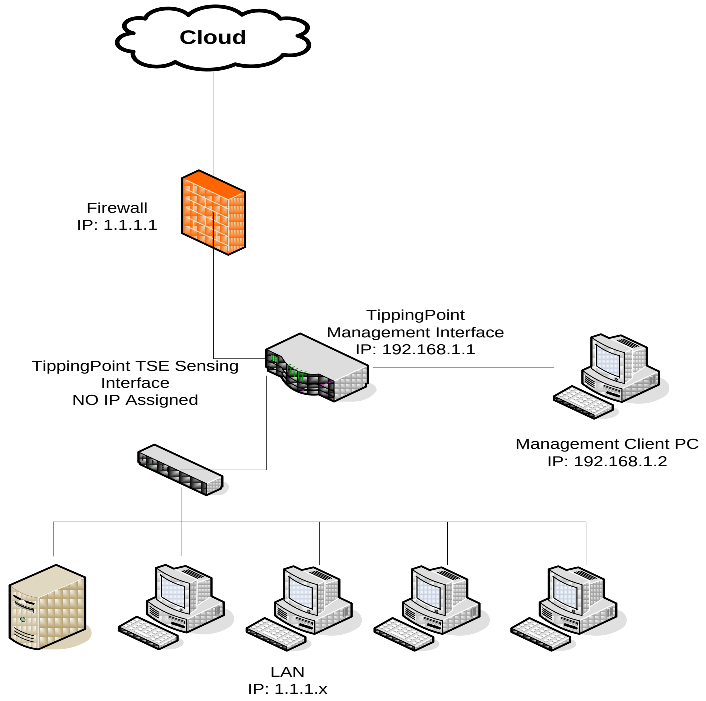

Figure 1: Deployment Scenario

5.2 Software Architecture

The TOE software, identified as the TippingPoint Operating System (TOS), comprises IPS-specific software developed by HP TippingPoint that runs on top of VxWorks v6.2, which is a real-time operating system made and sold by Wind River Systems. The TOE software comprises the following major components:

- Operating System (OS)
- Threat Suppression Engine (TSE)
- Management Interface.

The OS provides a set of support services to both the TSE and Management Interface. Amongst other functions, the OS provides services to utilize device hardware features (e.g., a reliable time stamping capability based upon a CMOS clock). More information regarding OS functions is given in section 5.2.1.

An administrator initiates a connection with the Management Interface using either the HTTPS or SSH protocol. Once identification and authentication have occurred, the administrator uses the Management Interface to configure the TOE based on the access level associated with the administrator’s account.

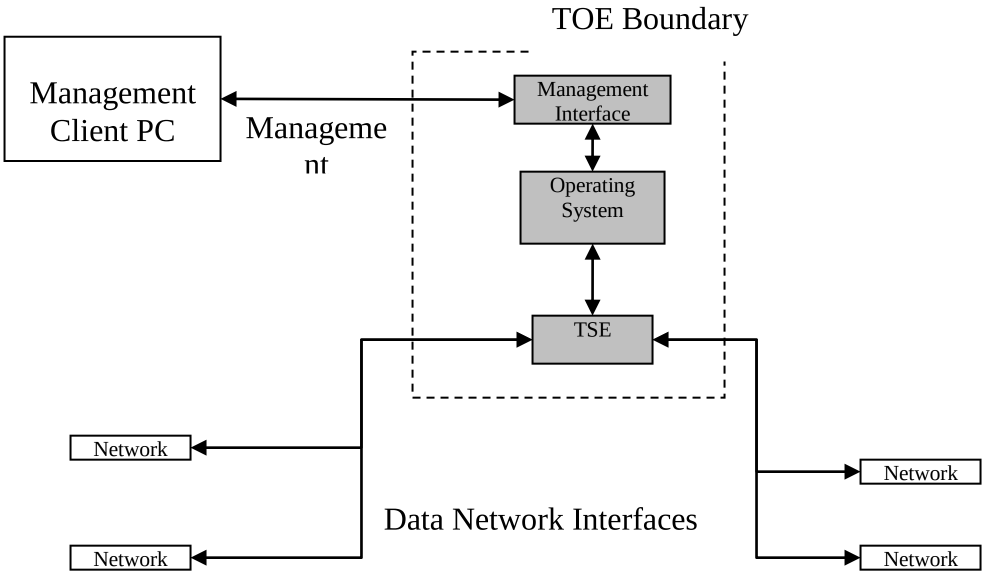

Figure 2: TOE Architecture

5.2.1 Operating System

The OS component provides the basic execution environment for the IPS-specific software. The IPS-specific software relies on the following OS services:

- Boot processing and system initialization
- File system services
- Process scheduling services
- POSIX library implementation
- Network and other hardware device drivers
- Real time clock
- Network protocol implementations
- Email client.

The file system service provides a layer of abstraction between various data elements and any external interfaces. User authentication data (username and passwords) are stored in the file system and are not directly accessible from the Management Interface. Additionally, filter data that is used by the TSE is also stored in the file system and not directly accessible from any external interface. The file system service is also used to store all audit data and to ensure that it is not directly accessible from any external interface.

The OS is supplied as part of the TOE and only contains trusted processes. There are no external capabilities to alter the function of the OS, or introduce any new processes.

5.2.2 Threat Suppression Engine

The main component of the IPS device is the Threat Suppression Engine (TSE), a custom engine designed to detect and block a range of attacks at wire speeds. The TSE is a “flow” based network security engine. Each packet is identified as a member of a flow. A flow can have one or more packets. Each flow is tracked in the “connection table”. A flow is uniquely identified by the port it was received on and its packet header information:

- IP protocol (ICMP, TCP, UDP)
- source IP address
- source ports (TCP or UDP)
- destination IP address
- destination ports (TCP or UDP).

The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet belonging to a flow arrives, the flow is re-evaluated for malicious content. When a flow is deemed malicious (by matching a configured filter), the current packet and all subsequent packets pertaining to the flow are handled according to the configured action (e.g., blocked). Once classified, each packet is inspected by the appropriate set of protocol and application filters. Out of the box, the IPS will identify flows in asymmetric mode—meaning the IPS only needs to see the transmit side or the receive side of a TCP connection (not both).

HP Networking’s Digital Vaccine Labs develop the filters that are included in the Digital Vaccine package provided as part of the TOE. The TOE provides the capability to update the Digital Vaccine package as new filters become available. Updated filters can be downloaded directly to the TOE appliance from Digital Vaccine Labs using a secure SSL tunnel. The filters are themselves encrypted and digitally signed. Use of this capability requires the management network be able to connect to the Internet.

The TSE provides the functionality of a sensor and analyzer as described by the IDS System PP. When intrusions are detected, the TSE generates alarms, blocks flows and/or logs activity depending upon its configuration. Logged data is stored and protected by the OS file system services. Logs are managed such that when the available storage capacity is exhausted, the oldest log is overwritten.

Sensor Capabilities

The TSE is used to monitor network traffic. The traffic is inspected according to a set of predefined filters or signatures. When network traffic that matches a particular filter is sensed, this component informs the notification mechanism.

Analyzer Capabilities

The TOE performs statistical and signature-based analysis of the collected traffic against configured IPS filters. The TOE additionally decodes protocol headers to support reconstructing fragmented packets or flows. Once decoded, the TOE applies its filters to achieve desired protections for the protected network segments.

Within each analytical result, the following information is stored:

- Date and time of the result
- Type of result (message, policy ID, signature ID, and classification)
- Identification of data source
- Data destination
- Protocol
- Severity.

5.2.3 Management Interface

The TOE offers two methods for configuring, monitoring, and reporting on the IPS device. Both of these methods are accessible through the secure management network connection, which protects all data transferred between the TOE and the administrative user.

The Command Line Interface (CLI) is used to issue commands in the TippingPoint command language via a command line prompt.

The TippingPoint Local Security Manager (LSM) manages the IPS via a web-based graphical user interface.

To access the security functions, users must authenticate by logging into the Management Interface with a username and password. The username is used to identify the role of the user and the password to authenticate them. There are three roles that can be assigned to a user:

- Superuser—full access to the TOE. This role is able to manage the users of the TOE and to view/modify the configuration of the TOE and the logs
- Administrator—write access to the TOE. This role is able to view/modify the configuration of the TOE (with the exception of managing user accounts) and the logs (with the exception of selection of auditable events and viewing/clearing of the audit log)
- Operator—read-only access to the TOE. This role is able to view the system data logs (with the exception of audit logs) and configuration of the TOE, but is not permitted to modify any information other than his/her own password.
- All security relevant and Management Interface actions are recorded in the Audit log. The Audit log records the command that was executed, the username of the user who performed an action, the interface from which the user logged in, such as the LSM or CLI, and a timestamp of when the action was performed. Storage services for the Audit log are provided by the operating system file system services. The Management Interface also provides a mechanism for administrators to review the contents of the audit trail.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE is as follows:

- *HP TippingPoint Command Line Interface Reference TippingPoint Operating System V. 3.1, Part number: TECHD-0000000291, TOS 3.1.4 edition: January 2011*
- *HP TippingPoint TippingPoint Command Line Interface Reference TippingPoint Operating System V. 3.2, Part number: TECHD-0000000291, Second edition: January 2011*
- *HP TippingPoint Local Security Manager User's Guide TippingPoint Operating System V. 3.1, Part number: TECHD-0000000293, TOS 3.1.4 edition: January 2011*
- *HP TippingPoint TippingPoint Local Security Manager User's Guide TippingPoint Operating System V. 3.2, Part number: TECHD-0000000293, Second edition: January 2011*
- *Quick Start TippingPoint 10, Part Number: TECHD-0300, Rev A03*
- *Quick Start TippingPoint N Platform, Part Number: TECHD-0000000284, Rev A06*
- *HP TippingPoint TippingPoint 10/110/330 Hardware Installation and Safety Guide, Part number: TECHD-0369, Rev A01, Second edition: January 2011*
- *HP TippingPoint TippingPoint N-Platform Hardware Installation and Safety Guide, Revision A04, Part number: TECHD-0000000285 Rev A04 Second edition: January 2011*

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the HP TippingPoint IPS.

Evaluation team testing was conducted at the vendor's development site July 11 through July 15, 2011.

7.1 Developer Testing

HP TippingPoint developed a set of test cases that correspond to security functions claimed in the ST, ensuring that all security functions presented at the external interfaces are tested and that all TSFI are tested. The test cases are grouped by security function and mapped to specific SFRs. Each test procedure targets the specific security behavior associated with that security function. A tracing of these tests to SFRs has been completed by the evaluation team.

The vendor ran the TOE test suites in various configurations, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results. The test configurations were representative of the HP TippingPoint IPS appliances included in the evaluated configuration. All tests passed.

7.2 Evaluation Team Independent Testing

The evaluation team executed a sample of the vendor test suite, per the evaluated configuration as described in the HP TippingPoint Intrusion Prevention Systems Security Target. The tests were run on a selection of the test configurations described in the developer's test documentation. The documentation describes the different test configurations and models of the TOE that were used in the test configurations.

The evaluation team executed a sample of the vendor test suite across three of the claimed appliances, one from each of the equivalence groups

In summary, the evaluation team performed its tests on three test bed configurations as follows:

- the high-end S5100N model appliance running TippingPoint Operating System v3.2.1,
- the mid-range S660N model appliance running TippingPoint Operating System v3.2.1 in FIPS mode, and
- the low-end S110 model appliance running TippingPoint Operating System v3.1.4.

The evaluation team performed the following additional functional tests:

- **Audit Data Generation**—the evaluation team confirmed, through examination and analysis of the audit trail produced by running the vendor test sample and the evaluation team's own tests, that all audit records specified in the ST can be generated by the TOE.
- **Audit Event Categories**—the evaluation team tested several audit event categories verify that each audit record includes its event type or category, and that the TOE is able to audit toggling on and off event categories.
- **Password Constraints**—the evaluation team confirmed the TOE enforces the following default Security Level 2 password requirements:
    - passwords must be at least 8 characters long
    - passwords must contain at least two alphabetic characters
    - passwords must contain at least one numeric character
    - passwords must contain at least one non-alphanumeric character
- **Account Lockout -** the evaluation team confirmed that the TOE can detect when an administrator configurable number of failed login attempts has occurred and will perform the configured failed login action which can be one of the following:
    - Lock the account for a configured Lockout period
    - Disable the account
    - Generate an audit event documenting the failed login attempt.

- **Trusted Path -** the evaluation team confirmed that HTTPS can be configured via the CLI and verified that access to the TOE can be restricted to HTTPS only.
- **Secure Data Storage -** the evaluation team confirmed that user authentication data (username and passwords), audit data and filter data stored in the file system cannot be directly accessed from the CLI or GUI Management Interfaces.
- **Maximum Simultaneous Sessions**—the evaluation team confirmed the claim in the User guides and Command Reference guides that indicate that the TOE provides simultaneous support for up to 10 web client connections, 10 telnet/SSH (for CLI) connections and one console connection.
- **Intrusion Detection Policy Priority -** the evaluation team confirmed that when a packet matches more than one Security Policy, the TOE applies the filtering rules specified in the Security Policy that has the most specific virtual segment defined.
- **IDS Notifications -** the evaluation team confirmed that the following types of notification contacts can be configured:
    - Remote System Log—sends messages to a syslog server on the management network
    - Management Console—sends messages to the LSM
    - Email and SNMP—sends messages to the email address or specified SNMP server on the management network.
- **Quarantine Action-** the evaluation team confirmed that a Quarantine action set can be configured through the CLI.
- **FIPS Algorithms -** the evaluation team confirmed that when the TOE is in Full FIPS mode, only the FIPS compliant algorithms are available, and that when the TOE was not in Full FIPS mode and non approved FIPS algorithms are chosen, the data was still protected when transmitted.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE. The evaluation team determined, through analysis of vulnerability descriptions and consideration of the method of use of the TOE, that one of these reported vulnerabilities might have been relevant to the TOE in its evaluated configuration. The TOE was tested against this potential vulnerability by the evaluation team and was found to be secure.

The evaluation team also performed a port scan of the TOE. The evaluation team confirmed all open ports identified by the scan were identified in the TOE guidance as allowable open ports that are only on the trusted side of the network.

In addition to the open source search and port scan, the evaluation team considered other potential vulnerabilities, based on a focused search of the evaluation evidence. The evaluation team performed tests to confirm:

- The TOEs LSM interface as a web browser GUI does not subject the system to any web application security flaws (OWASP Top Ten), such as cross site scripting (XSS), broken authentication and session management, failure to restrict URL access, etc. .
- The TOE is not susceptible to a denial of service attack via a flood of packets on TCP port 80.
- Password and configuration data transmitted between browser and appliance is not transmitted in the clear and only allowable protocols are used: SSL, HTTPS.
- The TOE is not vulnerable to the Open Source Search OpenSSH Root Login vulnerability found in CVE-2004-2760.
- The TOE accepts only SSHv2 connections. Attempts to connect to the CLI using SSHv1 are refused.

8 Evaluated Configuration

The evaluated version of the TOE is identified as the HP TippingPoint Intrusion Prevention System (IPS) devices, comprising the S6100N, S5100N, S2500N, S1400N, and S660N running TippingPoint Operating System v3.2.1, and the S330, S110 and S10 model appliances running TippingPoint Operating System version 3.1.4.

The IPS devices consist of network processor technology and HP Networking's own set of custom Field Programmable Gate Arrays (FPGAs) and are hardware and software appliances 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 TOE may rely on third-party software and hardware components in the operating environment such as a serial terminal client, and management client PCs. The TOE can also utilize external syslog, SMTP, and SNMP servers to receive alarms. The remote administrator can use a web browser to access the Web GUI interface and/or use SSH client to access the CLI. The local administrator can use the serial port to access the CLI. Neither the web browser or SSH client is part of the TOE. Note that Telnet cannot be used to access the CLI in the CC evaluated configuration.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 Revision 2 of the CC and the CEM.

The evaluation team concluded that the HP TippingPoint Intrusion Prevention System met all "EAL3 augmented with ALC_FLR.2" evaluation criteria.

10 Validator Comments/Recommendations

The validators were satisfied with the evaluation team's evaluation and testing efforts. The validators did not identify any gaps or missing information. The CCTL was well prepared, and the material was complete and correct.

11 Security Target

The ST for this product's evaluation is **HP TippingPoint Intrusion Prevention Systems Security Target,** Version 1.0, dated July 29, 2011.

12 Bibliography

- Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 1, September 2006, CCIMB-2006-09-001.
- Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-002.
- Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-003.
- Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-004.
- HP TippingPoint Intrusion Prevention Systems Security Target, Version 1.0, July 29, 2011