National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

TippingPoint Intrusion Protection System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E), Software version: 2.5.3.6933

Report Number: CCEVS-VR-VID10179-2008
Dated: 5 September 2008
Version: 1.7

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 6757
Fort George G. Meade, MD 20755-67457

ACKNOWLEDGEMENTS

Validation Team

John Nilles and Jean Hung

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary 4
2 Identification 5
3 Organizational Security Policy 6
4 Assumptions and Clarification of Scope 8
5 Architectural Information 9
6 Documentation 11
7 IT Product Testing 13
7.1 Developer Testing 13
7.2 Evaluation Team Independent Testing 13
7.3 Vulnerability Testing 14
8 Evaluated Configuration 14
9 Results of the Evaluation 15
9.1 Evaluation of the Security Target (ASE) 15
9.2 Evaluation of the Configuration Management Capabilities (ACM) 15
9.3 Evaluation of the Delivery and Operation Documents (ADO) 16
9.4 Evaluation of the Development (ADV) 16
9.5 Evaluation of the Guidance Documents (AGD) 16
9.6 Evaluation of the Life Cycle Support Activities (ALC) 16
9.7 Evaluation of the Test Documentation and the Test Activity (ATE) 16
9.8 Vulnerability Assessment Activity (AVA) 17
9.9 Summary of Evaluation Results 17
10 Validator Comments/Recommendations 17
11 Security Target 17
12 Glossary 17
13 Bibliography 18

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the TippingPoint Intrusion Protection System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E), software version: 2.5.3.6933. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of TippingPoint Intrusion Protection System (IPS) E-Series was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 29 July 2008.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1. The product is conformant with the United States Government Intrusion Detection System System Protection Profile, version 1.6 Protection Profile. All security functional requirements are derived from the Protection Profile, Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is TippingPoint Intrusion Protection System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E), software version 2.5.3.6933 provided by TippingPoint Technologies, Inc. TippingPoint Intrusion Prevention System (IPS) E-Series is a network-based intrusion prevention system. The IPS appliance is deployed inline so that all traffic passes through a pair of ports.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	TippingPoint Intrusion Protection System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E), software version 2.5.3.6933
Protection Profile	United States Government Intrusion Detection System System Protection Profile, version 1.6
ST	TippingPoint Intrusion Prevention System (IPS) E-Series Security Target, Version 1.0, 28 July 2008
Evaluation Technical Report	Evaluation Technical Report For TippingPoint Intrusion Protection System (IPS) E-Series, Part 1 (Non-Proprietary), Version 2.0 28 July 2008, Part 2

Item	Identifier
	(Proprietary), Version 1.0, 27 May 2008
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Conformance Result	CC Part 2 extended and Part 3 conformant, EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1
Sponsor	TippingPoint Technologies, Inc.
Developer	TippingPoint Technologies, Inc.
CCTL	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Evaluation Personnel	Science Applications International Corporation: Terrie Diaz, Anthony J. Apted
Validation Body	NIAP CCEVS: John Nilles, Jean Hung

3 Organizational Security Policy

The TippingPoint IPS provides protection for applications and infrastructure within a network using sets of filters. The TippingPoint IPS is configured with filters and global settings. The TippingPoint IPS can perform prevention and/or detection services, depending upon the instructions (i.e., actions) chosen for the deployed filters. When operating to perform intrusion prevention, the appliance scans and reacts to network traffic according to the filter instructions. When operating to perform intrusion detection, the appliance scans network traffic and generates alerts (also as directed by filter instructions). Action sets in these filters provide the instructions for the TOE to block, permit, and/or send alerts. Thus, blocking and permitting actions imply intrusion prevention while sending alerts implies intrusion detection.

A Management Interface is used for administering the TippingPoint IPS. 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 point-and-click interface.

To access the security functions, users must authenticate by logging into the Management Interface with a username and password.

The IPS allows its administrative users to manage either a single filter or a TippingPoint-defined grouping of filters (category of filters). This grouping cannot be changed by an administrator and simplifies administration tasks. Configuration values that are set for a group are applied for all filters in that group. The IPS has the following predefined categories and groups of filters.

- Application Protection
    - Exploits
    - Identity Theft
    - Reconnaissance
    - Security Policy
    - Spyware
    - Virus
    - Vulnerabilities
- Infrastructure Protection
    - Network Equipment
    - Traffic Normalization
- Performance Protection
    - IM
    - P2P
    - Streaming Media

Two additional categories (i.e., Distributed Denial of Service and Traffic Management) require the collection of additional configuration information for filters. While the underlying filter mechanism is the same for these categories of filters, additional configuration information is needed for these filters. Thus, the view of the management GUI for these categories differ from the view of the management GUI for the application protection, infrastructure protection and performance protection categories.

All filters provide detection and response instructions for segments and devices. The action sets for these filters can be set according to category or customized settings entered per

filter. Each action set can also include a set of notification contacts to receive alerts when the device detects and responds to traffic. The TippingPoint IPS E-Series also enables you to set exceptions and inclusions (or apply only rules) for filters. These settings can also be set and enacted according to filter or for all categories of filters.

4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which the TOE will be used and the manner in which it is expected to be deployed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE is appropriately scalable to the IT System the TOE monitors and has access to all the IT System data it needs to perform its functions.
- It is assumed information can not flow among the internal and external networks unless it passes through the TOE.
- It is assumed the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access and modifications.
- It is assumed the TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- It is assumed those responsible to manage the TOE are competent individuals, that only authorized users can gain access to the TOE, and that they are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

- All data collected and produced by the TOE shall only be used for authorized purposes and must be protected.
- The TOE must be protected from unauthorized accesses and disruptions of TOE data and functions.
- Users of the TOE must be accountable for their actions within the system.
- The TOE must collect data 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.

- The TOE must perform analytical processes and information to derive conclusions about inappropriate activity (past, present, or future) on collected system data and appropriate response actions taken.

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- 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.

The TOE provides a secure environment that monitors a network for potentially malicious and anomalous traffic. The TOE identifies such traffic through rules and algorithms designed to distinguish normal data flows from suspect ones.

5 Architectural Information[1]

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

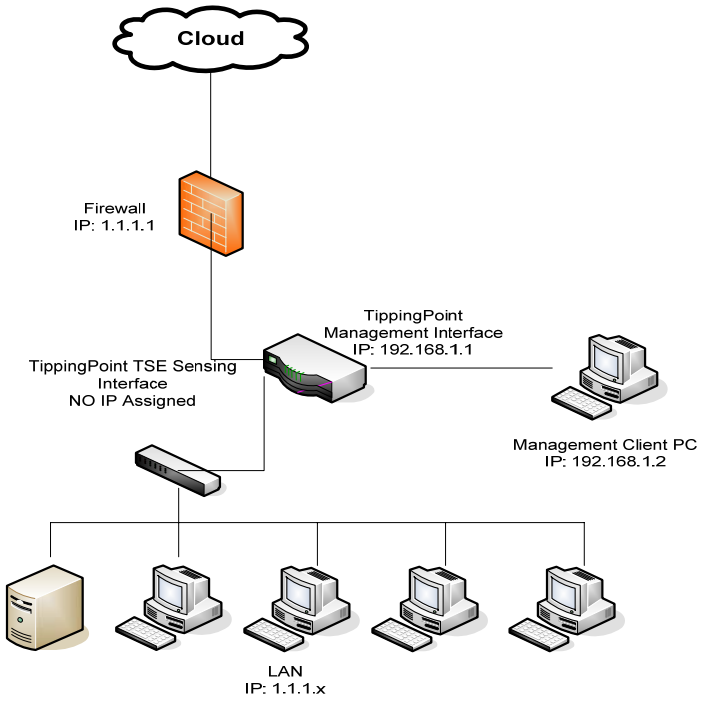
The TippingPoint IPS is designed for network transparency. The TippingPoint IPS is deployed into the network with no IP address or MAC address assigned to the sensor, and immediately begins filtering unwanted traffic.

The TippingPoint IPS is installed such that traffic to internal hosts flows through the IPS. This is shown in the figure below as the "Sensing Interface". Depending upon the model, a TippingPoint IPS can support up to 5 Sensing Interfaces. Additionally, each TippingPoint IPS has two dedicated management interfaces: an RJ-45 network port and a serial port.

[1] Extracted from SAIC Final ETR Part 1 Version 2.0, 28 July 2008

This is represented in the diagram below as the Management Interface. Administrators access the Management Interface using a web-based interface (the Local Security Manager, a.k.a., LSM) or via command line interface (CLI).

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



The physical boundary of the TOE is the TippingPoint Intrusion Prevention System E-Series Device.

- Hardware Models

  The TippingPoint E-Series system comprises a single chassis that uses a front-access, eight-port (10-ports for the model 210E) architecture supporting connections to four (or five) network segments. It is rack-mountable on a 19- or 23-inch rack and takes up either 1 or 2 Rack Units of space (2 Rack Units = 3.5 inches) depending on model. There are no removable cards in the chassis. Physical interfaces

  The physical interfaces are a set of network ports for monitored traffic called the data networks, a single network management port, and a serial port to connect a local terminal.

- Logical Boundaries

  The TOE is logically divided into three parts:

- The network management interface that is used to configure and manage the TOE
- The operating system provides the basic execution environment for the IPS-specific software. The operating system also provides services to utilize device hardware features (e.g., a reliable time stamping capabilities based upon a CMOS clock).
- The Threat Suppression Engine (TSE) provides the functionality of a sensor, scanner, and analyzer as described in the TippingPoint Intrusion Prevention System (IPS) E-Series Version 2.5.3.6933 Security Target

All three of these parts execute within a TippingPoint IPS E-Series device.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation

Document	Version	Date
TippingPoint Intrusion Prevention System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E) FSP & HLD Design Document for Common Criteria	Revision M, TECH - 00000000276	August 20, 2008

Guidance documentation

Document	Version	Date
TippingPoint Local Security Manager User's Guide 2.5.3	TECHD-0000000082	
TippingPoint Command Line Interface Reference 2.5.3	TECHD-0000000084	
Tipping Point IPS 5000E TOS ver. 2.5.3 Evaluated Installation Guide	Revision F, TECH-0000000279	May 12, 2008

Configuration Management documentation

Document	Version	Date
Tipping Point E-Series Products Configuration Items for Common Criteria	Revision I, TECHD-0000000274	May 21, 2008

Delivery and Operation documentation

Document	Version	Date
Tipping Point 5000E Delivery of Product to Buyer for Common Criteria EAL2	Revision D, TECH-0000000275	May 9, 2008
Tipping Point IPS 5000E TOS ver. 2.5.3 Evaluated Installation Guide	Revision F, TECH-0000000279	May 12, 2008

Life Cycle Support documentation

Document	Version	Date
Tipping Point IPS Flaw Remediation Process Description	Revision E, TECH - 00000000281	Feb 26, 2008

Test documentation

Document	Version	Date
TippingPoint E-Series Functional Testing and Coverage for Common Criteria for Common Criteria	Revision I, TECH-0000000277	May 27, 2008
Test Case documents: CLI FAU Tests, CLI FIA Tests, CLI FMT Tests, CLI FPT Tests, CLI IDS Tests, LSM FAU Tests, LSM FIA Tests, LSM FMT Tests, LSM FPT Tests, and LSM IDS Tests		May 13, 2008

The actual test results have been submitted to the evaluation team in various text files, PDFs, screenshots, and .d, .i, and .s file types. Section 11 of the Test Plan describes how to correlate the log files to the test cases.

Vulnerability Assessment documentation

Document	Version	Date
Tipping Point E-Series (5000E, 2400E, 1200E, 600E, 210E) Vulnerability Analysis for Common Criteria	Revision I, TECH-0000000278	July 23, 2008

Security Target

Document	Version	Date
TippingPoint Intrusion Prevention System (IPS) E-Series Security Target	Version 1.0	July 28, 2008

7 IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, User data protection, Identification and authentication, Security management, Protection of the TSF, and Intrusion Detection (EXP). All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire suite of the vendor's manual tests. In addition to rerunning the vendor's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided the IPS E-series appliance models and the necessary computers for the test environment.

The following hardware is necessary to create the test configuration: Three TippingPoint Intrusion Protection System (IPS) appliances with the operating system (210E, 1200E, and 5000E), TOE software, firmware, and local storage required to function as an instance of the TippingPoint Intrusion Protection System (IPS) Version 2.5.3, External serial console – for installation, generation, and startup of TOE and for specified administrative maintenance activities, Computer/Workstation on which the authorized administrator's Web browser runs to present the LSM GUI, Computer running Tomahawk tool to generate traffic, and Ethernet router, CAT 5e cabling, and any other items required to create a functional Ethernet network environment.

The following software is required to be installed on the machines used for the test: TippingPoint Intrusion Protection System (IPS) version 2.5.3 (TOE software) and the Tomahawk tool.

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

7.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8 Evaluated Configuration

The evaluated configuration requires one TippingPoint Intrusion Protection System (IPS) E-Series (5000E, 2400E, 1200E, 600E, or 210E) running software version 2.5.3.6933. The TippingPoint IPS provides protection for applications and infrastructure within a network using sets of filters. The TippingPoint IPS is configured with filters and global settings. The TippingPoint IPS can perform prevention and/or detection services, depending upon the instructions (i.e., actions) chosen for the deployed filters. When operating to perform intrusion prevention, the appliance scans and reacts to network traffic according to the filter instructions. When operating to perform intrusion detection, the appliance scans network traffic and generates alerts (also as directed by filter instructions). Action sets in these filters provide the instructions for the TOE to block, permit, and/or send alerts. Thus, blocking and permitting actions imply intrusion prevention while sending alerts implies intrusion detection.

A Management Interface is used for administering the TippingPoint IPS. 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 point-and-click interface.

For specific configuration settings required in the evaluated configuration see TippingPoint Local Security Manager User's Guide, TippingPoint Command Line Interface Reference, and TippingPoint IPS E-Series TOS ver. 2.5.3 Evaluated Installation Guide.

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on August 2006. The evaluation confirmed that the TippingPoint Intrusion Protection System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E), software version: 2.5.3.6933 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extended, and assurance requirements (Part 3) for EAL2 Augmented with ALC_FLR.2 and AVA_MSU.1.

The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report For TippingPoint Intrusion Protection System (IPS) E-Series, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the TippingPoint Intrusion Prevention System (IPS) E-Series Security Target, Version 1.0, 28 July 2008. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the TippingPoint Intrusion Prevention System (IPS) E-Series Version 2.5.3.6933 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. In addition the evaluation team ensured changes to the implementation representation are controlled and that TOE associated configuration item modifications is properly controlled.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed identification of the TOE and allows for detection of unauthorized modifications of the TOE. The evaluation team followed the TippingPoint Local Security Manager User's Guide, TippingPoint Command Line Interface Reference, and TippingPoint IPS E-Series TOS ver. 2.5.3 Evaluated Installation Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and high-level design documents. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The TippingPoint Local Security Manager User's Guide, TippingPoint Command Line Interface Reference, and TippingPoint IPS E-Series TOS ver. 2.5.3 Evaluated Installation Guide were assessed during the design and testing phases of the evaluation to ensure it was complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation Team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that systematic procedures exist for managing flaws discovered in the TOE.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team exercised the complete Vendor test suite and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis, the evaluation team's misuse analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's performance of the entire set of the vendor's test suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

11 Security Target

The Security Target is identified as TippingPoint Intrusion Prevention System (IPS) E-Series, Version 1.0, dated 28 July 2008. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1.

12 Glossary

The following definitions are used throughout this document:

CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DO	Delivery Operation
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
HTTP(S)	HyperText Transfer Protocol Secure
I/O	Input/Output

IPS	Intrusion Prevention System
LSM	[TippingPoint] Local Security Manager
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirement(s)
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] TippingPoint Intrusion Protection System (IPS) E-Series FINAL Non-Proprietary ETR – Part 1.

[6] TippingPoint Intrusion Protection System (IPS) E-Series FINAL Proprietary ETR – Part 2 and Supplemental Team Test Plan.

[7] TippingPoint Intrusion Protection System (IPS) E-Series Security Target, Version 1.0, 28 July 2008.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.