TippingPoint Intrusion Prevention System (IPS) E-Series

Security Target

VERSION 1.0

July 28, 2008

Developed for:

7501 North Capital of Texas Highway
Building B
Austin, Texas 78731 USA
Phone: (512) 681-8000
Fax: (512) 681-8099

Prepared by:

8310 N. Capital of Texas Highway, Ste 275
Austin, TX 78731
Office: (512) 310-2228
(877) 321-RISK
Fax: (512) 233-5924

[This page is intentionally left blank.]

Table of Contents

List of Tables

1.0 ST Introduction

1.1 ST Identification

Title:	TippingPoint TippingPoint Intrusion Prevention System (IPS) E-Series Security Target
Version:	1.0
Status:	FINAL
Prepared By:	En Pointe Technologiesneal
TOE Identifier(s):	TippingPoint Intrusion Protection System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E) • Software version: 2.5.3.6933
Assurance Level:	EAL2 Augmented with ALC_FLR.2 and AVA_MSU.1
Common Criteria:	Common Criteria for Information Technology Security Evaluation (CC), Version 2.3, August 2005.
Interpretations:	Final National and International interpretations included within this ST that that have been released on or before the kick-off date are identified within section 9.3 of this ST.
Keywords:	Intrusion Prevention System (IPS), TippingPoint Command Line Interface (CLI), TippingPoint Local Security Manager (LSM)

1.2 CC Conformance

This TOE is conformant to the following CC specifications:

CC Version 2.3, Part 2 – EXTENDED

CC Version 2.3, Part 3 – CONFORMANT

- Assurance Level: EAL2 – augmented with ALC_FLR.2 and AVA_MSU.1

Intrusion Detection System System Protection Profile, version 1.6 (a.k.a., the IDS System Protection Profile or IDS System PP)

- TippingPoint has chosen to augment the Protection Profile with ALC_FLR.2 and AVA_MSU.1

1.3 Document Conventions

Application Notes:	An application note is additional informative and non-normative text that assists the intended audience to better understand the intent of the TOE and its security features. Application notes are identified as a footnote to the corresponding item requiring further clarification with a number in the upper-right position (e.g. FAU_GEN.1[1]). The accompanying text of the application note is then displayed at the bottom of the page containing the corresponding item.
Assignment:	An assignment allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
Explicit:	Explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified with "(EXP)".
Interpretation:	An interpretation is a clarification or further definition to a security functional or assurance requirement that has been reviewed and approved by CCIMB or the associated Common Criteria scheme representative as being acceptable to incorporate into a complying ST. CCIMB and NIAP interpretations are identified by labeling the affected security requirement as they are mentioned in the guidance found at the following internet address: http://cio.nist.gov/esd/emaildir/lists/cc-cmt/msg00019.html
Iteration:	Iteration allows for the use of a component more than once with varying operations. Iterations are indicated with a lowercase alphabetic character (e.g. FAU_GEN.1a).
Refinement:	A refinement allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Refinements resulting from an interpretation are additionally indicated with a red font.

Selection:	A selection allows the specification of one or more elements from a list. Selections are indicated by underlining the text and are surrounded by brackets (e.g., [selection]).

1.4 ST Overview

This Security Target (ST) defines the security environment, security requirements, security functions, and assurance measures of the TippingPoint Intrusion Prevention System (IPS) E-Series.

The Target of Evaluation (TOE) is the TippingPoint Intrusion Prevention System E-Series (5000E, 2400E, 1200E, 600E, 210E) Software version: 2.5.3.6933, a network-based intrusion prevention system. The IPS appliance is deployed inline so that all traffic passes through a pair of ports.

The IPS can provide protection for applications and infrastructure within a network using sets of filters. A filter is a combination of an action set and a signature. The word signature is used to describe detection logic. That is, the collection of test criteria used to discriminate attack traffic from benign traffic is commonly referred to as a signature by the IDS community. Because a signature does not imply any action, it is commonly used to refer to detection (hence IDS). However, when detection is considered in conjunction with an active response the common term used is a filter.

The IPS is configured with filters and global settings. The appliance can perform prevention and/or detection services, depending upon the instructions (i.e., actions) chosen for 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 available for administering the IPS. The Management Interface enables hardware configuration and set up of the IPS using the management port of the IPS. In addition, the Management Interface enables the user to review system data collected by the IPS appliance. Audit data can also be viewed with this interface, including administrator actions performed on the IPS. The Management Interface is a standard embedded system interface that provides access to hardware and embedded software configuration. The following sections provided within this ST are stated in accordance with a Security Target as specified in Annex C.2 of CC Part 1:

ST Introduction:	The ST introduction provides a unique identification and overview of this ST.
TOE Description:	The TOE description provides an overview of the TOE and describes the physical and logical boundaries of the TOE.
TOE Security Environment:	The security environment describes the assumptions, threats, and organizational security policies that pertain to both the TOE and TOE environment.
Security Objectives:	The security objectives describe the objectives necessary to counter the defined threats and satisfy the assumptions and organizational security policies.
IT Security Requirements:	The IT security requirements provide a set of security functional requirements to be met by the TOE and the TOE environment. The IT security requirements also provide a set of security assurance requirements that are to be satisfied by the TOE.
TOE Summary Specification	The TOE Summary Specification describes the security functions of the TOE.
PP Claims:	The PP claims identify any PPs that the TOE claims compliance to.

Rationale:	The rationale provides mappings along with rationale for the security environment, security objectives, security requirements, and security functions to assess their completeness, consistency, and suitability.
Annex A:	Annex A lists the acronyms, terms, interpretations, and references used within this ST.

2.0 TOE Description

2.1 Overview of the TOE

The TippingPoint Intrusion Prevention System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E) Software version: 2.5.3.6933 is a network-based intrusion prevention system that monitors a network for potentially malicious and anomalous traffic. This system identifies such traffic through rules and algorithms designed to distinguish normal data flows from suspect ones.

The principal component of the TippingPoint system is the Intrusion Prevention System device. All of the functionality of the IPS runs directly on a single device. A single IPS can be installed at the perimeter of your network or on your Intranet or both. TippingPoint E-Series IPS devices can secure up to 5 network segments depending upon the model.

In this context, 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). Much the same way a firewall separates a protected network from another network. The IPS is installed in a network such that all traffic to and from a group of hosts is mediated by the IPS. A segment uses two ports on the IPS and all traffic flows between connected networks through the IPS. Members of the segment are hosts connected to those ports.

The word signature is used to describe detection logic. That is, the collection of test criteria used to discriminate attack traffic from benign traffic is commonly referred to as a signature by the intrusion detection system (IDS) community. Because a signature does not imply any action, it is commonly used to refer to detection. However, when detection is considered in conjunction with an active response the common term used is a filter. A filter is a combination of an action set and a signature.

A segment is protected when its traffic passes through a pair of ports and the IPS applies filters that are configured for that segment.

The IPS scans and reacts to network traffic according to the filter instructions, or action set. To protect a multi-segment network, an appliance enforces a different set of filters to manage (and block) the traffic and malicious attacks on each segment. Action sets in these filters provide the instructions for the device to block traffic, permit traffic, and send alerts[1].

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 [2]

- Exploits
- Identity Theft
- Reconnaissance
- Security Policy
- Spyware
- Virus
- Vulnerabilities

Infrastructure Protection

- Network Equipment

[1] Alerts will be discussed in more detail in section 6.1.5

[2] The categories of “application protection”, “infrastructure protection” and “performance protection” are simply GUI labeling constructs and do not represent a functional mechanism in the TOE.

- 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.

The functionality of the IPS can be accessed using the Management Interface. The Management Interface provides a method to set values, run setup commands, and perform general functions.

2.1.1 Deployment Architecture

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. 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 interace (CLI).

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

Also, an SNMP (e-mail) server is required in the environment. The server needs to be installed and configured as specified in the product documentation.

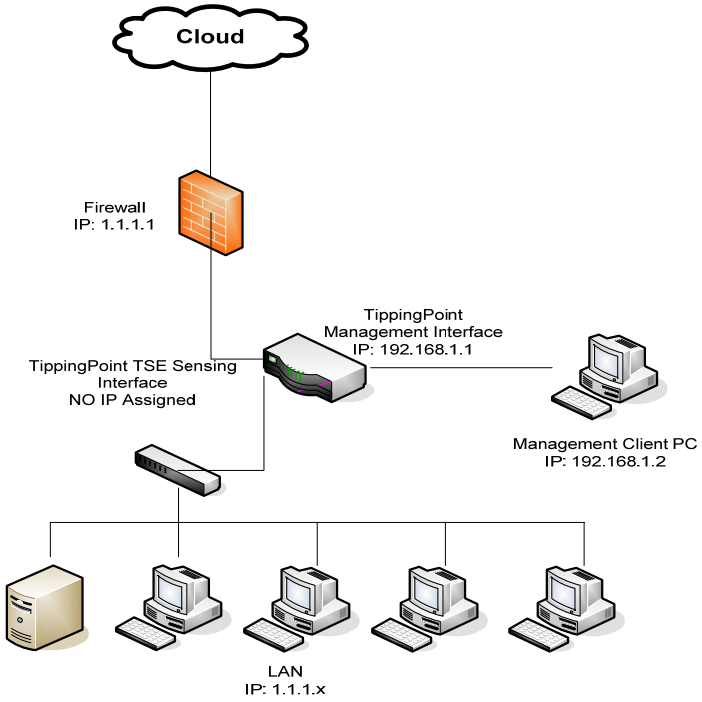

Figure 1 Deployment Scenario

2.1.2 Intrusion Prevention System

TippingPoint's IPS is a hardware-based intrusion prevention platform consisting of network processor technology and TippingPoint's own set of custom FPGAs (Field Programmable Gate Arrays). The IPS is a line-speed hardware engine that contains all the functions needed for Intrusion Prevention, including IP defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of network protocols. These functions are provided by the IPS using filters.

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, other)
- source IP address
- source ports (TCP or UDP)
- destination IP address
- destination ports (TCP or UDP)

The Threat Suppression Engine 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. The instant a flow is deemed malicious, the current packet and all subsequent packets pertaining to the flow are blocked. This ensures that the attack never reaches its destination. 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 either the transmit or the receive side of a TCP connection (not both).

2.2 Scope and Boundaries of the TOE

2.2.1 Physical Boundaries

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

2.2.1.1 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. The devices contain two redundant hot swappable power supplies and three chassis cooling fans, except for the 210E model. The 210E model contains 1 internal power supply and 6 chassis cooling fans plus 1 power supply cooling fan. There are no removable cards in the chassis.

2.2.1.2 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.

The ports associated with the data networks, through which monitored traffic flows, can be connected to either wired networks or fiber optic networks depending upon the model. For wired networks, the Copper Segments interface is used via RJ45 connectors. For fiber networks the Fiber Optic Segment connectors are used. Once connected, network traffic on these interfaces can be monitored by the TOE.

The single network management port presents either the LSM (over HTTPS) or CLI (over SSH) administrative interfaces. In order to support email alarms, the IT environment must provide an email server which must also be connected to this dedicated management network port. The dedicated management network port expects physical security to protect the confidentiality and integrity of the data being transported between the TOE and any device connected to this dedicated management network port (i.e., the systems providing the LSM interface, the CLI interface or the email server).

Users must enter a username and password to authenticate to the TOE prior to issuing commands over the LSM or CLI interfaces.

Finally, a serial port is provided to allow a local terminal to be connected. When connected, a command line interface is available on the local terminal. As with the dedicated network management port, physical security protects the confidentiality and integrity of the data being transported between the console and the appliance.

Physical protection is necessary for any device used to provide the management interface. That is, the console that is connected through the serial port and the platform connected through the network management port must be provided with physical protections[3]. While the LSM and CLI are accessed using protocols that include encryption, that encryption is NOT relied upon to ensure a secure connection of the TOE to the administrator, it is the physical protections that ensures a secure connection.

2.2.2 Logical Boundaries

The TOE is logically divided into three parts: a network management interface, an operating system and a Threat Suppression Engine. All three of these parts execute within a TippingPoint IPS E-Series device.

The operating system provides a series of support services to both the Threat Suppression Engine and Management Interface. Amongst other functions, the operating system provides services to utilize device hardware features (e.g., a reliable time stamping capabilities based upon a CMOS clock). More information regarding operating systems functions is given in section 2.2.2.2

An administrator initiates a connection with the Management Interface using either the HTTPS or SSH protocol. Once identification and authentication have occurred, the Management Interface may be used to configure the TOE based upon the permissions of the administrator that is logged in.

[3] Since the appliance and all connected management devices require the same physical protections, the cabeling must also be provided this same level of physical protections.

The operating system not only stores data obtained through the management interface, but is also fed data by the Administrator via the Management Interface and the TSE. No contact can be made from the Management Interface directly to the TSE.

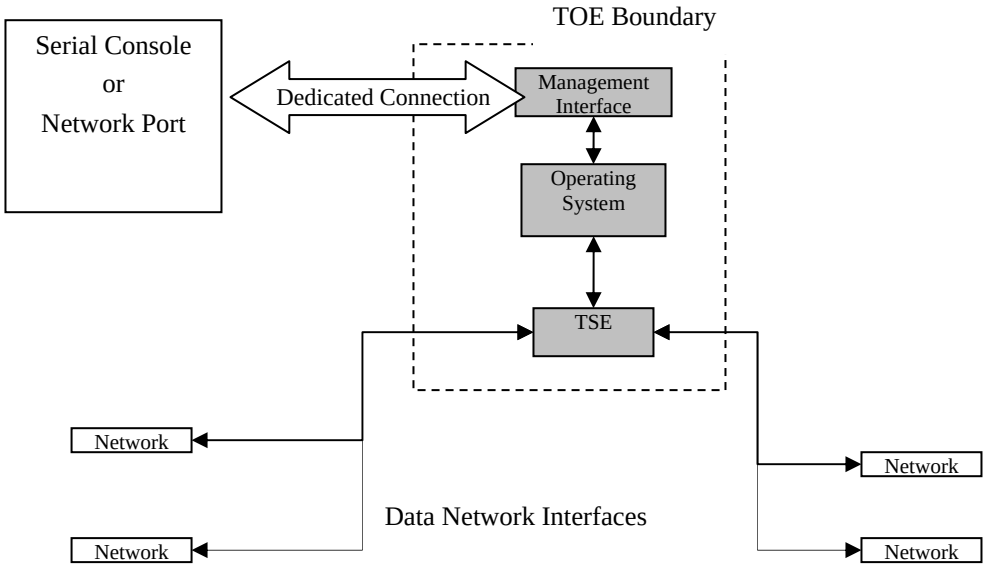

Figure 2. TOE logical boundaries

2.2.2.1 Threat Suppression Engine – Sensor, Scanner, and Analyzer

The Threat Suppression Engine provides the functionality of a sensor, scanner, 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 by the operating system's files system services, and are protected. Logs are managed such that when logs exhaust the available storage capacity 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. Other filters, called "anomaly filters", identify and report reconnaissance activities such as port scans and host sweeps.

Analyzer Capabilities

The TSE supports the analysis of collected data by supplying the information necessary to further qualify the severity of an attack. For example, an attack is downgraded in its severity if the TSE database notes that the target address of the attack packet is offline or if the service running on the attacked port is not vulnerable to the attack.

The TSE also installs signature-based rules into the sensor component, together with the action as defined by the security policy.

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; and
- Severity.

2.2.2.2 Operating System

The operating system 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;
- E-mail client.

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

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

2.2.2.3 Management Interface (CLI & LSM)

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 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[4]:

Operator — Basic access to review the status of the system

Administrator — Advanced access to monitor and manage functions in the system

[4] Throughout this document variation in capitalization of the names of these roles does not imply a different role, but may occur for emphasis or readability.

Superuser — Full access to use and manage all functions available in the system

The user role defines the types of operations that may be invoked by a user. In the case of the CLI, it employs the use of the proprietary language. The CLI has two types of commands:

- Global commands are available from within any menu level in the CLI. Global commands do not report on or change configuration items.
- Hierarchal commands are available only within a menu or submenu level.

The LSM represents these same commands graphically in a web interface. In both instances (CLI or LSM), commands that are not usable by a certain role are not offered by either interface method.

All security relevant and management interface actions are recorded in the Audit Log. The audit log displays the command that was executed, the username of the user who performed an action and the interface from which the user logged in, such as the LSM or CLI. Storage services for the Audit log are provided by the Operating Systems File Systems Services. The management interface also provides a mechanism for administrators to review the contents of the audit trail.

3.0 TOE Security Environment

All of the security environment statements have been drawn from a validated PP (IDS System PP). Please consult that protection profile for the description of the security environment. The policies, threats and assumptions from that PP are the definitive statement of the security environment.

4.0 Security Objectives

All of the security objective statements have been drawn from a validated PP (IDS System PP). Please consult that protection profile for the description of the security objectives. The security objectives from that PP are the definitive statement of the security objectives.

5.0 IT Security Requirements

This part of the ST defines the detailed IT security requirements that shall be satisfied by the TOE or its environment.

Table 1: IT Security Requirements

Security Functional Requirements
FAU_GEN.1 Audit data generation
FAU_SAR.1 Audit review
FAU_SAR.2 Restricted audit review
FAU_SAR.3 Selectable audit review
FAU_SEL.1 Selective audit
FAU_STG.2 Guarantees of audit data availability
FAU_STG.4 Prevention of audit data loss
FIA_ATD.1 User attribute definition
FIA_UAU.1 Timing of authentication
FIA_UID.1 Timing of identification
FMT_MOF.1 Management of security functions behaviour
FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles
FPT_RVM.1 Non-bypassability of the TSP
FPT_SEP.1 TSF domain separation
FPT_STM.1 Reliable time stamps
IDS_SDC.1 System Data Collection (EXP)
IDS_ANL.1 Analyser analysis (EXP)
IDS_RCT.1 Analyser react (EXP)
IDS_RDR.1 Restricted Data Review (EXP)
IDS_STG.1 Guarantee of System Data Availability (EXP)
IDS_STG.2 Prevention of System data loss (EXP)
Security Assurance Requirements for the TOE
ACM_CAP.2: Configuration items
ADO_DEL.1: Delivery procedures

ADO_IGS.1: Installation generation and start-up procedures
ADV_FSP.1: Informal functional specification
ADV_HLD.1: Descriptive high-level design
ADV_RCR.1: Informal correspondence demonstration
AGD_ADM.1: administrator guidance
AGD_USR.1: User guidance
ATE_COV.1: Evidence of coverage
ATE_FUN.1: Functional testing
ATE_IND.2: Independent testing – sample
AVA_SOF.1: Strength of TOE security function evaluation
AVA_VLA.1: Developer vulnerability analysis
ALC_FLR.2: Flaw Reporting Procedures
AVA_MSU.1: Examination of Guidance

5.1 Security Functional Requirements

5.1.1 Security Functional Requirements for the TOE

5.1.1.1 FAU: Security Audit

5.1.1.1.1 FAU_GEN: Security audit data generation

5.1.1.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [basic] level of audit (**as included in Table 2**.); and

c) [**Access to the System and access to the TOE and System data**].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**the additional information specified in the Details column of Table 2**].

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU. 1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 2: Auditable Events

5.1.1.1.2 FAU_SAR: Security audit review

5.1.1.1.2.1 FAU_SAR.1 Audit review

FAU_SAR.1.1

The TSF shall provide [**the authorized system administrator**] with the capability to read [**all auditable events that are recorded**] from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.1.2.2 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.1.2.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1

The TSF shall provide the ability to perform [sorting] of audit data based on [date and time, subject identity, type of event, and success or failure of related event].

5.1.1.1.3 FAU_SEL: Security audit event selection

5.1.1.1.3.1 FAU_SEL.1 Selective audit

FAU_SEL.1.1

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [event type];

b) [**No additional attributes**].

5.1.1.1.4 FAU_STG: Security audit event storage

5.1.1.1.4.1 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1

The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2

The TSF shall be able to [prevent] **unauthorized** modifications to the **stored** audit records **in the audit trail**.

FAU_STG.2.3

The TSF shall ensure that [**at least 50% of the space available for**] audit records will be maintained when the following conditions occur: [audit storage exhaustion].

5.1.1.1.4.2 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1

The TSF shall [overwrite the oldest stored audit records] and [**send an alarm**] if the audit trail is full.

5.1.1.2 FIA: Identification & Authentication

5.1.1.2.1 FIA_UAU: User authentication

5.1.1.2.1.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1

The TSF shall allow [**no actions**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.2.2 FIA_ATD: User attribute definition

5.1.1.2.2.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [

a) User identity;

b) Authentication data;

c) Authorisations; and

d) [**No additional attributes**].

5.1.1.2.3 FIA_UID: User identification

5.1.1.2.3.1 FIA_UID.1 Timing of identification

FIA_UID.1.1

The TSF shall allow [**no actions**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.3 FMT: Security Management

5.1.1.3.1 FMT_MOF: Management of functions in TSF

5.1.1.3.1.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to [modify the behaviour of] the functions **of System data collection, analysis and reaction** to [**authorized system administrators**].

5.1.1.3.2 FMT_MTD: Management of TSF data

5.1.1.3.2.1 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to [query [**and add System and audit data, and shall restrict the ability to query and modify all other TOE data**]] to [**authorized administrators and authorized system administrators**].

Application Note: The statement "query and add system and audit data" in this requirement refers to the ability to look at and to change the set of events for which audit and system log records are actually collected. It does not refer to the capability of looking at and changing the data in these logs after it has been collected. The ability to look at the records within the audit log is specified using FAU_SAR.1. The ability to look at the records within the system data log is specified using IDS_RDR.1. Furthermore, the FMT_MTD.1 SFR is included to resolve a dependency upon FAU_SEL.1. In order to properly resolve this dependency, the FMT_MTD.1 SFR would need to address management of the collection of audit data.

5.1.1.3.3 FMT_SMF: Specification of management functions

5.1.1.3.3.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [

1. **Management of user accounts;**
2. **Management of audit data and audit configurations;**
3. **Management of TSF data;**
4. **Management of Security Policies**;]

5.1.1.3.4 FMT_SMR: Security management roles

5.1.1.3.4.1 FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the **following *roles*: authorized administrator, authorized system administrator and [none]**[5].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

[5] Refer to Section 6.1.3 for the correspondence of the TOE supported roles to those defined in the IDSSPP.

5.1.1.4 FPT: Protection of the TSF

5.1.1.4.1 FPT_RVM: Reference mediation

5.1.1.4.1.1 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.1.4.2 FPT_SEP: Domain Separation

5.1.1.4.2.1 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.1.4.3 FPT_STM: Time stamps

5.1.1.4.3.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.1.1.5 IDS: IDS Component Requirements

5.1.1.5.1 IDS_SDC: System Data Collection

5.1.1.5.1.1 IDS_SDC.1 System Data Collection (EXP)

IDS_SDC.1.1

The System shall be able to collect the following information from the targeted IT System resource(s):

a) [network traffic] and

b) [**No additional events**]. **(EXP)**

IDS_SDC.1.2

At a minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the *Details* column of Table 3: System Events. **(EXP)**

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address

Table 3: System Events

5.1.1.5.2 IDS_ANL: Analyser analysis

5.1.1.5.2.1 IDS_ANL.1 Analyser analysis (EXP)

IDS_ANL.1.1

The System shall perform the following analysis function(s) on all IDS data received:

a) [signature]; and

b) **[none]**. **(EXP)**

IDS_ANL.1.2

The System shall record within each analytical result at least the following information:

a. Date and time of the result, type of result, identification of data source; and

b. [**Data destination, protocol, and severity**]. **(EXP)**

5.1.1.5.3 IDS_RCT: Analyser react

5.1.1.5.3.1 IDS_RCT.1 Analyser react (EXP)

IDS_RCT.1.1

The System shall send an alarm to [**the system data log, the user defined in the security policy, or both**] and take [**no additional actions**] when an intrusion is detected. **(EXP)**

5.1.1.5.4 IDS_RDR: Restricted Data Review

5.1.1.5.4.1 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1

The System shall provide [**authorized system administrators and authorized administrators**] with the capability to read **[all system data]** from the System data. **(EXP)**

IDS_RDR.1.2

The System shall provide the System data in a manner suitable for the user to interpret the information. **(EXP)**

IDS_RDR.1.3

The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access. **(EXP)**

5.1.1.5.5 IDS_STG: System Data Storage

5.1.1.5.5.1 IDS_STG.1 Guarantee of System Data Availability (EXP)

IDS_STG.1.1

The System shall protect the stored System data from unauthorized deletion. **(EXP)**

IDS_ STG.1.2

The System shall protect the stored System data from modification. **(EXP)**

Application Note from the PP: Authorized deletion of data is no considereda modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3

The System shall ensure that **[at least 50% of the space available for]** System data will be maintained when the following conditions occur: [System data storage exhaustion]. **(EXP)**

5.1.1.5.5.2 IDS_STG.2 Prevention of System data loss (EXP)

IDS_STG.2.1

The System shall [overwrite the oldest stored System data] and send an alarm if the storage capacity has been reached. **(EXP)**

5.2 Security Assurance Requirements for the TOE

EAL 2 – Structurally tested

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis, and independent testing based upon more detailed TOE specifications.

The assurance requirements of the TOE have been augmented with ALC_FLR.2 and AVA_MSU.1 components as defined in Part 3 of the Common Criteria.

5.2.1 ACM: Configuration Management

Configuration management (CM) is one method or means for establishing that the functional requirements and specifications are realized in the implementation of the TOE. CM meets these objectives by requiring discipline and control in the processes of refinement and modification of the TOE and the related information. CM systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorized.

5.2.1.1 ACM_CAP.2: Configuration items

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Unique identification of the configuration items leads to a clearer understanding of the composition of the TOE, which in turn helps to determine those items which are subject to the evaluation requirements for the TOE.

Developer action elements:

ACM_CAP.2.1D	The developer shall provide a reference for the TOE.
ACM_CAP.2.2D	The developer shall use a CM system.
ACM_CAP.2.3D	The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2C	The TOE shall be labeled with its reference.
ACM_CAP.2.3C	The CM documentation shall include a configuration list.
ACM_CAP.2.4C	The configuration list shall **uniquely** describe the configuration items that comprise the TOE.
ACM_CAP.2.5C	The CM documentation shall describe the method used to uniquely identify the configuration items **that comprise the TOE**.
ACM_CAP.2.6C	**The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.**
ACM_CAP.2.7C	The CM system shall uniquely identify all configuration items **that comprise the TOE**.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 ADO: Delivery and Operation

Delivery and operation provides requirements for correct delivery, installation, generation, and start-up of the TOE.

5.2.2.1 ADO_DEL.1: Delivery procedures

The requirements for delivery call for system control and distribution facilities and procedures that detail the measures necessary to provide assurance that the security of the TOE is maintained during distribution of the TOE. For a valid distribution of the TOE, the procedures used for the distribution of the TOE address the threats identified in the PP/ST relating to the security of the TOE during delivery.

Developer action elements:

ADO_DEL.1.1D	The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2D	The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 ADO_IGS.1: Installation generation and start-up procedures

Installation, generation, and start-up procedures are useful for ensuring that the TOE has been installed, generated, and started up in a secure manner as intended by the developer. The requirements for installation, generation and start-up call for a secure transition from the TOE's implementation representation being under configuration control to its initial operation in the user environment.

Developer action elements:

ADO_IGS.1.1D	The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C	The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2E	The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.3 ADV: Development

The development class encompasses four families of requirements for representing the TSF at various levels of abstraction from the functional interface to the implementation representation. The development class also includes a family of requirements for a correspondence mapping between the various TSF representations, ultimately requiring a demonstration of correspondence from the least abstract representation through all intervening representations to the TOE summary specification provided in the ST. In addition, there is a family of requirements for a TSP model, and for correspondence mappings between the TSP, the TSP model, and the functional specification. Finally, there is a family of requirements on the internal structure of the TSF, which covers aspects such as modularity, layering, and minimization of complexity.

5.2.3.1 ADV_FSP.1: Informal functional specification

The functional specification is a high-level description of the user-visible interface and behavior of the TSF. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all the TOE security functional requirements are addressed.

Developer action elements:

ADV_FSP.1.1D	The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C	The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2C	The functional specification shall be internally consistent.
ADV_FSP.1.3C	The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C	The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 ADV_HLD.1: Descriptive high-level design

The high-level design of a TOE provides a description of the TSF in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide. The high-level design requirements are intended to provide assurance that the TOE provides an architecture appropriate to implement the TOE security functional requirements.

The high-level design refines the functional specification into subsystems. For each subsystem of the TSF, the high-level design describes its purpose and function, and identifies the security functions contained in the subsystem. The interrelationships of all subsystems are also defined in the high-level design. These interrelationships will be represented as external interfaces for data flow, control flow, etc., as appropriate.

Developer action elements:

ADV_HLD.1.1D	The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C	The presentation of the high-level design shall be informal.
ADV_HLD.1.2C	The high-level design shall be internally consistent.
ADV_HLD.1.3C	The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4C	The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5C	The high-level design shall identify any underlying hardware**, firmware** and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware**, firmware** or software.
ADV_HLD.1.6C	The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7C	The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2E	The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.3 ADV_RCR.1: Informal correspondence demonstration

The correspondence between the various TSF representations (i.e. TOE summary specification, functional specification, high-level design, low-level design, and implementation representation) addresses the correct and complete instantiation of the requirements to the least abstract TSF representation provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.

Developer action elements:

ADV_RCR.1.1D	The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C	For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 AGD: Guidance Documents

The guidance documents class provides the requirements for user and administrator guidance documentation. For the secure administration and use of the TOE it is necessary to describe all relevant aspects for the secure application of the TOE.

5.2.4.1 AGD_ADM.1: administrator guidance

Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. Because the secure operation of the TOE is dependent upon the correct performance of the TSF, persons responsible for performing these functions are trusted by the TSF. Administrator guidance is intended to help administrators understand the security functions provided by the TOE, including both those functions that require the administrator to perform security-critical actions and those functions that provide security-critical information.

Developer action elements:

AGD_ADM.1.1D	The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C	The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2C	The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3C	The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4C	The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5C	The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6C	The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7C	The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8C	The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 AGD_USR.1: User guidance

User guidance refers to material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE's external interfaces. User guidance describes the security functions provided by the TSF and provides instructions and guidelines, including warnings, for its secure use.

The user guidance provides a basis for assumptions about the use of the TOE and a measure of confidence that non-malicious users, application providers and others exercising the external interfaces of the TOE will understand the secure operation of the TOE and will use it as intended.

Developer action elements:

AGD_USR.1.1D	The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C	The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 ALC: Life Cycle

TippingPoint ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. TippingPoint includes security controls in the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. TippingPoint achieves this through the use of a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results. TippingPoint has procedures for accepting and addressing identified operational flaws as well as security flaws, including tracking of all identified flaws, describing, correcting, and taking other remedial actions such as producing guidance related to such flaws. These procedures are documented in:

5.2.5.1 ALC_FLR.2: Flaw Reporting Procedures

Flaw remediation ensures that flaws discovered by the TOE consumers will be tracked and corrected while the TOE is supported by the developer. In order for the developer to be able to act appropriately upon security flaw reports from TOE users, and to know to whom to send corrective fixes, TOE users need to understand how to submit security flaw reports to the developer. Flaw remediation guidance from the developer to the TOE user ensures that TOE users are aware of this important information.

Developer action elements:

ALC_FLR.2.1D	The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2D	The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3D	The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation of evidence elements:

ALC_FLR.2.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5C	The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C.	The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users
ALC_FLR.2.7C	The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8C	The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements

ALC_FLR.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6 ATE: Tests

The class "Tests" encompasses three families: coverage (ATE_COV), independent testing (e.g. functional testing performed by evaluators) (ATE_IND), and functional tests (ATE_FUN) Testing will help to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements; although it cannot establish that the TOE does no more than what was specified. Testing may also be directed toward the internal structure of the TSF, such as the testing of subsystems and modules against their specifications.

The aspects of coverage and depth have been separated from functional tests for reasons of increased flexibility in applying the components of the families. However, the requirements in these three families are intended to be applied together.

The independent testing family has dependencies on the other families to provide the necessary information to support the requirements, but is primarily concerned with independent evaluator actions.

The emphasis in this class is on confirmation that the TSF operates according to its specification. This will include both positive testing based on functional requirements, and negative testing to check that undesirable behavior is absent. This class does not address penetration testing, which is directed toward finding vulnerabilities that enable a user to violate the security policy. Penetration testing is based upon an analysis of the TOE that specifically seeks to identify vulnerabilities in the design and implementation of the TSF, and is addressed separately as an aspect of vulnerability assessment in the class AVA.

5.2.6.1 ATE_COV.1: Evidence of coverage

In this component, the objective is to establish that the TSF has been tested against its functional specification. This is to be achieved through an examination of developer evidence of correspondence.

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.2 ATE_FUN.1: Functional testing

Functional testing performed by the developer establishes that the TSF exhibits the properties necessary to satisfy the functional requirements of its PP/ST. Such functional testing provides assurance that the TSF satisfies at least the security functional requirements; although it cannot establish that the TSF does no more than what was specified. The family "Functional tests" is focused on the type and amount of documentation or support tools required, and what is to be demonstrated through developer testing. Functional testing is not limited to positive confirmation that the required security functions are provided, but may also include negative testing to check for the absence of particular undesired behavior (often based on the inversion of functional requirements).

The objective is for the developer to demonstrate that all security functions perform as specified. The developer is required to perform testing and to provide test documentation.

Developer action elements:

ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C	The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C	The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.3 ATE_IND.2: Independent testing – sample

The objective is to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests.

Developer action elements:

ATE_IND.2.1D	The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.7 AVA: Vulnerability Assessment

The class addresses the existence of exploitable covert channels, the possibility of misuse or incorrect configuration of the TOE, the possibility to defeat probabilistic or permutational mechanisms, and the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.

5.2.7.1 AVA_SOF.1: Strength of TOE security function evaluation

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.

Developer action elements:

AVA_SOF.1.1D	The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C	For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2E	The evaluator shall confirm that the strength claims are correct.

5.2.7.2 AVA_VLA.1: Developer vulnerability analysis

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorized access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorized capabilities of other users.

A vulnerability analysis is performed by the developer to ascertain the presence of obvious security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the TOE.

Developer action elements:

AVA_VLA.1.1D	The developer shall perform ~~and document~~ a~~n~~ **vulnerability** analysis**.** ~~of the TOE deliverables searching for obvious ways in which a user can violate the TSP.~~
AVA_VLA.1.2D	The developer shall ~~document the disposition of obvious vulnerabilities~~ **provide vulnerability analysis documentation.**

Content and presentation of evidence elements:

AVA_VLA.1.1C	The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2C	The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3C	The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2E	The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.2.7.3 AVA_MSU.1 Examination of guidance

The objective is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

Developer action elements:

AVA_MSU.1.1D	The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C	The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2C	The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3C	The guidance documentation shall list all assumptions about the intended environment
AVA_MSU.1.4C	The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

AVA_MSU.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2E	The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3E	The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3 Strength of Function Claim

5.3.1 Minimum Strength of Function Claim

This ST claims a minimum strength of function level of SOF-Basic for the TOE security functional requirements.

5.3.2 Explicit Strength of Function Claims

All of the SOF claims are based on password space calculations and based on the SOF rationale provided in the Vulnerability Assessment. Also refer to section 8.2.4, “Validation of Strength-Of-Function Claims” later in this security target.

6.0 TOE Summary Specification

6.1 TOE Security Functions

This statement of TOE security functions describes the IT security functions in terms of how these functions satisfy the TOE security functional requirements. Each TOE security function statement identifies the security functional requirements that are satisfied by that TOE security function. Each security function, as a minimum, contributes to the satisfaction of at least one TOE security functional requirement.

The following table lists the security functions that are identified for this TOE.

Table 4: TOE Security Functions

TOE SECURITY FUNCTIONS
Security Audit
Identification and Authentication
Security Management
Protection of the TSF**Error! Reference source not found.**
Intrusion Detection

6.1.1 Security Audit

The Security Audit security function is implemented within the Intrusion Prevention System (IPS). The IPS generates two types of activity monitoring logs:

- Audit data logs; and
- System data logs (i.e., the Block log and the Alert log).

System data logs record activity pertinent to the TOE's intrusion detection and prevention capabilities. These logs are different from Audit data logs in their contents and controls. The system data logs are implemented by the Intrusion Detection security function.

The IPS provides the capability to generate audit data and stores audit data that has been generated until the audit data is cleared using the Management Interface or automatically overwritten. In addition, the Management Interface ensures that only the superuser is allowed to view the audit data and that the audit data is presented in an interpretable manner. The Management Interface provides a means for the superuser to determine what audit data the system collects, as well as, the capability to sort the audit data that is being viewed through the Management Interface.

FAU_GEN.1 Audit data generation

The Security Audit security function generates audit records for the following auditable events:

1. Start-up and shutdown of audit functions
2. Access to the system
3. Access to the TOE and System data (these records identify the IDS object and requested access)
4. Reading of information from the audit records
5. All modifications to the audit configuration that occur while the audit collection functions are operating

6. All use of the authentication mechanisms (these records identify the user identity and location of the attempt)
7. All use of the user identification mechanisms (these records identify the user identity and location of the attempt)
8. All additions, deletions and modifications to security policies
9. Enabling and disabling filters within a security policy
10. Addition, deletion and modification to custom action sets
11. All modifications to the date, time and network configuration values
12. Modifications to the group of users that are part of a role (these records identify the user identity)

The Security Audit security function also includes in the audit record for each auditable event, the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. All audit data is stored within the Operating System component of the IPS.

The TOE does not support the ability to start up and shutdown the audit functions outside the ability to startup and shutdown the entire TOE. Thus, each time the TOE starts, the auditing functions are started (the same is true for shutdown). Thus, audits of TOE startup and TOE shutdown correspond to audits of audit startup and audit shutdown.

The TOE offers users only those commands the user is authorized to perform.

FAU_SAR.1 Audit review

The Security Audit security function provides the mechanims to view data from the Audit log, as well as from the System data log (i.e., the Block log and the Alert log). The operator, administrator and the superuser have the ability to view the events that have been recorded in the System data log. Only the Superuser can view events logged in the audit log.

The management interface contains commands to configure how terminal sessions behave. The presentation format of data within the management interface can be defined. Data from any log (including Audit data) can be displayed in text format over the management interface. The default settings in Table 5 can be modified to provide for the optimal viewing of data.

Table 5: Default Console Settings

Setting	Default Value	Command to Change Setting
columns	80	**hostname#** conf t session col <number of columns>
rows	25	**hostname#** conf t session row <number of rows>
more	On	**hostname#** conf t session no more
wraparound	On	**hostname#** conf t session no wrap
timeout	20 minutes	**hostname#** conf t session timeout <number of minutes>

FAU_SAR.2 Restricted audit review

All users must log into the Management Interface before any commands can be executed. Each logged in user is authorized for a given type of access (i.e., a role). The Security Audit security function prohibits read-access to the audit trail for all users in roles other than the superuser role. This is done by restricting access using the file system service capabilites to protect the audit log such that only the authenticated Superusers can read audit data.

FAU_SAR.3 Selectable audit review

The Security Audit security function provides the ability to sort audit data. This capability is only provided by the LSM Interface and is not available in the CLI. Using the mouse to select the column that you would like to sort will allow sorting by the criteria shown in Table 6: Sorting Criteria

Table 6: Sorting Criteria

Criteria	Description
time	Sorts log entries in an ascending or descending list based on the time of the entry
user <"login name">	Sorts logs by the login name of the user that was logged in when the log entry was created
status [PASS|FAIL]	Display only records with pass or fail status.
ip <nnn.nnn.nnn.nnn>	Displays log records whose access was from the IP address entered
Interface [WEB,CLI, LSM, SNMP, OTHER]	Filters on the interface through which the user accessed the TippingPoint device
Event type	Sorts events based on the severity of the event in one column, or by the specific name of the event in another column

FAU_SEL.1 Selective audit

Auditable events (i.e., the auditable events for the basic level of auditing as specified in the Common Criteria) can be included or excluded from the set of audited events based on event categories. These event categories are shown in

Event Category	Description
boot	This flag toggles the auditing of boot information for the system
report	This flag toggles the auditing of events related to reports, including the viewing and clearing of logs to include both audit and syste data logs.
login	This flag toggles the auditing of login events.
logout	This flag toggles the auditing of logout events.
config	This flag toggles the auditing of configuration data. This includes changing the auditable events in the logs.
user	This flag toggles the auditing of changes to user account related data. This includes user creation, modification and deletion of user accounts.
time	This flag toggles the auditing of changes to time settings.
policy	This flag toggles the auditing of TSE system policy data.
host	This flag toggles the collection of audit records whenever audit starts or stops6.
general	This flag toggles the auditing of the rotation of logs.
conn-table	This flag toggles the auditing of connection table information
high-availability	This flag toggles the auditing of high-availability information

[6] Note: Auditing only starts and stops when the system starts and stops.

Event Category	Description
host-communications	This flag toggles the auditing of host-communication information
ip-filter	This flag toggles the auditing of HOST IP filter information
monitor	This flag toggles the auditing of monitor information, such as packet and network traffic scanning and events
oam	This flag toggles the auditing of OAM information
segment	This flag toggles the auditing of network segment information, such as port and system settings per segment of a device
server	This flag toggles the auditing of server information
sms	This flag toggles the auditing of SMS information
tse	This flag toggles the auditing of events related to the threat suppression engine.
update	This flag toggles the auditing of system and software updates, such as Digital Vaccine and software updates

A user of the TOE can select the event categories to use in gathering audit records via the CLI using the 'configure' command. This function is not available in the LSM interface. For each event category, the CLI allows the category to be enabled or disabled, thus determining which events are written to the audit log. Only the Superuser role is able to select which event categories to audit.

It should be understood that the IPS architecture is such that a single command (e.g. 'configure t log audit select report') may enable/disable audited events that correspond to more than one Common Criteria functional component and/or event type. The issue of locating log events relating to a specific CC functional component is resolved through post-selection sorting of the audit records (FAU_SAR.3).

FAU_STG.2 Guarantees of audit data availability

The Security Audit security function prevents unauthorized access (i.e., deletion, viewing and modification) of audit records by requiring users to be successfully authenticated before allowing access to the IPS. The Security Audit security function additionally ensures that when the audit storage becomes exhausted, that only the oldest audit record files are purged to ensure adequate disk space for the more recent auditable events.

The TOE does not allow a user to modify audit data outside of allowing a Superuser to completely purge the Audit Log either by using the clear CLI command or by resetting the log in the LSM by clicking the "reset log" icon next to the Audit Log entry. The TOE compares the user access level for all incoming audit review requests to the access level of the role provided and maintained by the TOE. If the access level of the requested action is greater than the current user's access level, the requested action to purge is denied. This purge action is logged, allowing for detection of the deletion, or attempted deletion, of audit records.

The only modification that can be made to audit records within an audit log is a clear operation. This action is also logged. Once a clear operation is executed all log entries are removed. Only super-user level users can clear the audit log.

Log records are stored sequentially in a log file[7]. Thus, audit records are stored sequentially in an audit log file, and operations upon the audit log are considered part of the auditing security function. The IPS uses a volume threshold to limit the size of each log file (default is 4 mb). When a log file reaches the threshold file size, the log file is closed, a new log file is created, and an alarm is sent. The log file that is closed becomes a historical log file and the new file becomes the current log file. If a historical log file already existed, it is deleted. Every

[7] The term 'log file' is used here and throughout this paragraph to indicate that the mechanism that is being described applies to any type of log file supported by the TOE (e.g., audit log, Block log, and alert log).

type of log has at most a historical log file and a current log file. Subsequent log records are then written to the newly created current log file. This mechanism which is applied to all types of log files (e.g., audit, block, and alert) is used to limit the amount of audit data that is overwritten when the system's capacity to store audit records is reached. Access to any type of log file through the Management Interface for the purpose of viewing or clearing always treats both the historical log file and the current log file as one log. Therefore, viewing audit records in the audit log would display all records from both files. Similarly, clearing the audit log would delete both files.

FAU_STG.4 Prevention of audit data loss

The deletion of the historical audit log file when the current audit log file becomes full, effectively overwrites the oldest audit records. The alarm that is sent when a new current log file (see the preceeding discussion about changing log files) is created takes the form of an E-mail alarm that is sent to a specified user. The IPS also writes a new log record to the Alert log when new log files are created. This mechanism which applies to all log types is used to for generate alarms whenever the audit log overwrites the oldest stored audit records.

6.1.2 Identification and Authentication

The Identification and Authentication security function is implemented only within the Management Interface subsystem of the TippingPoint Intrusion Prevention System (IPS) E-Series. In general, the Identification and Authentication security function provides a means for users to be identified and authenticated.

A password security level dictates the password contraints that must be followed for all passwords on the TOE. The default security level is 2, which is also the required security level in the evaluated configuration.

FIA_ATD.1 User attribute definition

The Identification and Authentication security function provides the capability to manage the user attributes for the operator, administrator, and superuser roles. The security attributes managed by the TOE include user identity, authentication data, authorizations (roles), password expiration, security level, information, and other user specific parameters. The capability to manage all aspects of user attributes is granted only to the Superuser role. With respect to user attributes, the operator and administrator roles are only provided the capability to change their own authentication data (passwords). The user attributes defined for these all roles are stored in the file system implemented by the operating system and are managed through the Management Interface.

FIA_UAU.1 Timing of authentication & FIA_UID.1 Timing of identification

The Identification and Authentication security function provides the capability to identify and authenticate the operator, administrator and the superuser roles. The Identification and Authentication security function prevents actions from being performed prior to identification and authentication of the user. Establishing a connection requires the submission of user credentials (username and password) through the Management Interface. Once a valid username/password pair is provided, the management functionality is available to the logged in user over the management interface.

6.1.3 Security Management

FMT_SMR.1 Security roles

The TOE maintains a list of security attributes in the form of individual records that belong to a particular user[8]; one of these attributes is the user's role. The following roles are defined on the TOE:

[8] All users of the TOE are privileged users. There are no "untrusted" user accounts defined in the TOE. The term user is used throughout this document to refer to a person acting in any one of the three administrative roles. This document will refer to 'users' rather than 'administrators' in order to reduce confusion with the one role that is named 'administrator'

- **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.

Each authorized user of the TOE is assigned to one and only one role.

A user account cannot be created without an associated role; if this is attempted, the action is denied and the interface enforces that a role be specified before proceeding with account creation. Superusers are permitted to change their role or the roles of other users. This is accomplished either by using the configure user CLI command or by navigating to the Authentication-User List page of the LSM. These two options will also allow a user to display a list of all users and their associated roles.

Table 8: Mapping of TOE-defined Roles to PP-defined Roles

TOE-defined Role	PP-defined Role
Superuser	Authorized System Administrator
Administrator	Authorized System Administrator
Operator	Authorized Administrator

FMT_MOF.1 Management of security functions behaviour

The Security Management security function restricts the ability to modify the behavior of the functions of System data collection, analysis and reaction to users associated with the Administrator or Superuser role. These roles have the ability to modify the security policies that determine how System data is analyzed, displayed, and reacted to. Users with the Operator role only have the ability to view the security policies that affect how the System data is analyzed, displayed, and reacted to.

FMT_MTD.1 Management of TSF data

The Security Management security function provides the following restrictions to the user roles.

Table 7: Management Operations and Roles

Management function	Role Required to perform action
Query TOE configuration	Operator, Administrator, or Superuser
Query system data	Operator, Administrator, or Superuser
Clear system data logs, define users to receive alarm emails for system data logs and configure system data collection	Administrator or Superuser
Manage configuration of filters	Administrator or Superuser
Managing user accounts	Superuser
Select auditable events	Superuser

View, clear and define users to receive alarm emails for the audit log	Superuser

The Security Management security function provides the capability to manage user accounts, audit data, audit configurations, and security policies. The management capabilities are provided by the operating system but are accessed through the Management Interface.

The Management Interface controls access to services provided by the TOE. The TSF maintains information about that defines the role a user operates at and the authorizations of the role. Access to commands is based on the user's role. Commands that the user is not authorized to perform are not recognized and are inaccessible. Furthermore, any commands that are unavailable based upon the user's authorization will not be displayed to the user. Access to restricted data is not be permitted.

This function supports FMT_MOF.1(1) and FMT_MTD.1 by providing the specification of data protection attributes and management of security functions provided by the TOE. This function limits such modifications to the TOE to the roles managed by the TOE and specified in FMT_SMR.1.

FMT_SMF.1 Specification of Management Functions

The Security Management security function provides the capability to perform management operations using either the CLI or LSM interfaces. These interfaces allow logged in users with appropriate authorization to

- Create, delete and change user accounts,
- Query or clear audit log, Block log, and Alert log data
- Define the audit configuration,
- Manage configuration of filters (both categories/groups and individual filters),
- Manage the system data log, and
- Define users to receive alarms

6.1.4 Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

The **Error! Reference source not found.** Protection of the TSF security function ensures that TSP enforcement functions are invoked and succeed before each function within the TSE is allowed to proceed. This is accomplished by verifying that the set of permitted activities defined within the role(s) associated with the user allows the requested operation to be performed prior to allowing the operation to be performed. Users must log into the Management Interface before any functions can be executed.

The placement of the IPS in a network, such that all traffic to a segment flows through the IPS, allows the IPS to ensure that its Intrusion Detection capabilities are always enforced. That is, since all traffic to a segment flows through the IPS, the IPS can perform operations in support of intrusion detection and prevention.

FPT_SEP.1 TSF domain separation

The Protection of the TSF **Error! Reference source not found.** security function provides the TSE a security domain for its own execution that protects it from interference and tampering of any untrusted subjects by providing separate interfaces for the sensing and management of the sensor.

The **Error! Reference source not found.** Protection of the TSF security function provides the IPS a security domain for its own execution that protects it from interference and tampering of any untrusted subjects by not permitting any user process to exist in the IPS.

Internal the IPS utilizes an operating system to provide services used by the TSE and the management interface. The operating system is a trusted component of the TOE that provides no direct administrative interfaces to non-management interfaces (management capabilities are only available through the management interface). The operating system is supplied with the TOE and only contains trusted software. There are no external capabilities to alter the function of the internal operating system, or introduce any new processes.

FPT_STM.1 Reliable time stamps

A system time maintained by the operating system is read by a TOE component. The IPS keeps time internally using its own internal CMOS clock. Alternatively, it can use a Simple Network Time Protocol Server (SNTP Server) to check and synchronize time periodically. However, the use of SNTP is outside the scope of this evaluation and is not used in the CC-evaluation configuration of the TOE.

The time can only be modified by a users in the Superuser or administrator role either by using the configure CLI command or by making changes in the System-Time Options screen of the LSM.

6.1.5 Intrusion Detection (EXP)

IDS_SDC.1 System Data Collection (EXP)

The Threat Suppression Engine (TSE) provides the IPS with the sensing capabilities to collect network traffic, generate alert records for certain network traffic, block certain network traffic and pass along certain network traffic. For each event in which data is collected, the IPS records the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

The TSE is the data collector for IPS system data. The TSE records the collected system data into two logs: the Block log and the Alert log. The Block log holds records associated with filters that block traffic and the Alert log holds records associated with notification filters.

The TSE component also acts as an IDS Sensor. In this capacity the IPS, inspects network traffic according to filter settings. When network traffic that matches a particular filter is sensed, this component informs the notification mechanism. This component also supports the “anomaly filters” – these are filters designed to identify and report reconnaissance activities such as port scans and host sweeps. These activities are precursors to a future intrusion or attack, and, as such, considered part of the IDS Analyzer functionality.

IDS_ANL.1 Analyser analysis (EXP)

The TOE performs signature-based analysis of traffic as it flows through the IPS. The TOE decodes protocol headers to support reconstructing fragmented packets or flows. Once decoded, the TOE uses installed filters to achieve desired protections for the protected network segments (e.g., statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of network protocols).

Analysis methodologies match specific signatures or patterns (associated with filters) that may characterize attack attempts to characteristics of known attacks. This analysis qualifies the severity of the potential threat.

The TSE groups filters (i.e., signature-based rules combined with an action) into categories that the TSE analyzer uses in order to provide protection versus malicious network traffic as it passes through the data network interface of the TOE. The groups of filters provided by the TSE allows for simplified administration of a large number of filters by allowing the administrator or superuser to enable, disable or specify an action set for a group of filters. The grouping for pre-defined filters cannot be changed and contains the following categories.

Table 8 Filter Categories visible in LSM

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

The TSE also supports filters in categories of Distributed Denial of Service (DDoS) and Traffic Management. However, these categories exist not to group filters for ease of administration, but because filters in these categories require additional configuration information.

Intrusion prevention capabilities such as traffic shaping are accomplished using traffic management filters and/or traffic normalization filters. Flow state tracking, flow blocking and application-layer parsing of network protocols are characteristics of most of the filters in the categories described in Table 8.

The TSE records the analytical results to the Block log or Alert log, depending on the action prescribed for the filter. 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; addr and port
- Data destination; addr and port
- Protocol; and
- Severity.

IDS_RCT.1 Analyser react (EXP)

The detection of an intrusion in the context of the TOE is the matching of network traffic to the configured security policies (i.e., filters). When an intrusion is detected, the TOE reacts based upon the action associated with the matched filter. When the action includes “notify”, an alert record is written to the Alert log and, if so configured, an email is generated.

The IPS is capable of sending alerts (a.k.a., alarms) either to the Alert log or via email.

IDS_RDR.1 Restricted Data Review (EXP)

The TOE compares the user access level for all incoming data review requests to the access level of the user role provided. If the access level of the requested action is greater than the current user’s access level, the requested action is denied. This applies to requests to review system data stored by the TOE in the Block log

and Alert log. This data can either be accessed using the show CLI command or by using the Navigation Tree of the LSM to select Events, then Logs, then choosing the appropriate log from the list provided.

The ability to read the logs stored on the TOE is restricted to authorized users. The three access levels supported by the TOE – Superuser, administrator and operator – all have read access to the logs once authenticated to the TOE with the exception of the Audit Log. Only Superusers are permitted to read the Audit Log.

IDS_STG.1 Guarantee of System Data Availability (EXP)

If the access level of the requested action is greater than the current user's access level, the requested action is denied. This control prevents the unauthorized deletion of the IPS system data log contents. Deletion can be performed by using the clear CLI command or by using the Navigation Tree of the LSM to select Events, then Logs, then choosing the appropriate log from the list provided. Administrator and Superuser roles have the ability to modify the TOE system data logs (this is not referring to data stored in the Audit Log).

The IPS system data logs are stored on the TOE in the Block log and Alert log (a.k.a., system data logs). Operator roles have read-only access to these two logs (this does not include the Audit Log) via the Management Interface.

As discussed in Section 6.1.1, the IPS maintains a historical log file and a current log file for each type of log. Thus, there is a historical Block log file and a historical Alert log file, as well as a pair of current log files for these logs. Whenever either current log file becomes full an alarm is sent. The operations of the TOE on the Block log and Alert log are part of the intrustion detection & prevention security function.

IDS_STG.2 Prevention of System data loss (EXP)

The deletion of the historical log files that form the system data when the corresponding current log file becomes full effectively overwrites the oldest system data records. The alarm that is sent when a new current log file (see the preceeding discussion about changing log files) is created takes the form of an E-mail alarm that is sent to a specified user. The IPS also writes a new log record to the Alert log when new log files are created. This mechanism which applies to all log types is used to generate alarms whenever the audit log overwrites the oldest stored audit records.

E-mail alarm contacts can be created in the Management Interface.

6.2 Assurance Measures

Table 9: TOE Assurance Measures

CC Assurance Components	TippingPoint Assurance Measures
ACM_CAP.2 Configuration items	TippingPoint Configuration Items for Common Criteria Rev A
ADO_DEL.1 Delivery procedures	TippingPoint Delivery of Product to Customer Rev C
ADO_IGS.1 Installation, generation, and start-up procedures	*Common Criteria Certified TippingPoint Hardware Installation and Safety Guides for Version 2.5.3*; TECHD-0000000073; Publication Control Number 11907 which then references the following: *Quick Start TippingPoint 200/400/1200/2400 Intrusion Prevention Appliance Installation and Configuration Guide Version 2.5.3*; Part Number TECHD -00000000089 *Quick Start TippingPoint 210E Version 2.5.3*, Part Number TECHD-0000000139 *Quick Start TippingPOint 600E/1200E/2400E/5000E Version 2.5.3*, Part Number TECHD-0000000090 *TippingPoint Command Line Interface Reference Version 2.5.3*; Part Number TECHD-0000000084; Publication Control Number 11907 *TippingPoint Local Security Manager User Guide Version 2.5.3*; Part Number TECHD-00000000082; Publication Number 11907
ADV_FSP.1 Informal functional specification	TippingPoint Functional Specification REVF *TippingPoint Command Line Interface Reference Version 2.5.3*; Part Number TECHD-0000000084; Publication Control Number 11907 *TippingPoint Local Security Manager User Guide Version 2.5.3*; Part Number TECHD-00000000082; Publication Number 11907 *Common Criteria Certified TippingPoint Hardware Installation and Safety Guides for Version 2.5.3*; TECHD-0000000073; Publication Control Number 030308 *Draft High Level Design Document*; Pub Number: Not Assigned; Revision unpub 2002-10-28.
ADV_HLD.1 Descriptive high-level design	*Draft High Level Design Document; Pub Number: Not Assigned; Revision unpub 2002-10-28.* TippingPoint Functional Specification REVF
ADV_RCR.1	TippingPoint Informal Correspondence Analysis

CC Assurance Components	TippingPoint Assurance Measures
Informal correspondence demonstration	
AGD_ADM.1 Administrator guidance	*TippingPoint Command Line Interface Reference Version 2.5.x*; Part Number TECHD-0000000084; Publication Control Number 11907 *TippingPoint Local Security Manager User Guide Version 2.5.3*; Part Number TECHD-00000000082; Publication Number 11907 *Common Criteria Certified TippingPoint Hardware Installation and Safety Guides for Version 2.5.3*; TECHD-0000000073; Publication Control Number 030308
AGD_USR.1 User guidance	*TippingPoint Command Line Interface Reference Version 2.5.3*; Part Number TECHD-0000000084; Publication Control Number 11907 *TippingPoint Local Security Manager User Guide Version 2.5.3*; Part Number TECHD-00000000082; Publication Number 11907
ATE_COV.1 Evidence of coverage	UnityOne v1.2 CC test package - June 26 2003.zip.pgp
ATE_FUN.1 Functional testing	UnityOne v1.2 CC test package - June 26 2003.zip.pgp which includes: TippingPoint Technologies, Inc. UnityOne Version 1.2 Functional Specification Manifest Document Version 1.7
ATE_IND.1 Independent testing	SAIC Test Report
AVA_SOF.1 Strength of TOE security function evaluation	TippingPoint UnityOne™ version 1.2 Vulnerability Assessment v1.3
AVA_VLA.1 Developer vulnerability analysis	TippingPoint UnityOne™ version 1.2 Vulnerability Assessment v1.3

7.0 PP Claims

7.1 PP Reference

This ST complies with all security requirements, security objectives, and security environment statements for the defined TOE and its environment as they are stated within Intrusion Detection System System Protection Profile, version 1.6.

7.1.1 IT Security Requirement Statements

The following IT security requirement statements are stated within this ST using the permitted operations specified within the Intrusion Detection System System Protection Profile, version 1.6:

IT Security Assurance Requirements

- ACM_CAP.2: Configuration items
- ADO_DEL.1: Delivery procedures
- ADO_IGS.1: Installation generation and start-up procedures
- ADV_FSP.1: Informal functional specification
- ADV_HLD.1: Descriptive high-level design
- ADV_RCR.1: Informal correspondence demonstration
- AGD_ADM.1: administrator guidance
- AGD_USR.1: User guidance
- ATE_COV.1: Evidence of coverage
- ATE_FUN.1: Functional testing
- ATE_IND.2: Independent testing – sample
- AVA_SOF.1: Strength of TOE security function evaluation
- AVA_VLA.1: Developer vulnerability analysis
- ALC_FLR.2 : Flaw Reporting Procedures
- AVA_MSU.1: Examination of guidance

IT Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_SAR.1 Audit review
- FAU_SAR.2 Restricted audit review
- FAU_SAR.3 Selectable audit review
- FAU_SEL.1 Selective audit
- FAU_STG.2 Guarantees of audit data availability
- FAU_STG.4 Prevention of audit data loss
- FIA_ATD.1 User attribute definition
- FIA_UAU.1 Timing of authentication
- FIA_UID.1 Timing of identification

- FMT_MOF.1 Management of security functions behaviour
- FMT_MTD.1 Management of TSF data
- FMT_SMR.1 Security roles
- FPT_RVM.1 Non-bypassability of the TSP
- FPT_SEP.1 TSF domain separation
- FPT_STM.1 Reliable time stamps
- IDS_SDC.1 System Data Collection (EXP)
- IDS_ANL.1 Analyser analysis (EXP)
- IDS_RCT.1 Analyser react (EXP)
- IDS_RDR.1 Restricted Data Review (EXP)
- IDS_STG.1 Guarantee of System Data Availability (EXP)
- IDS_STG.2 Prevention of System data loss (EXP)

7.2 PP Tailoring

This section identifies the security requirements, security objectives, or security environment statements that are tailored from their original specification in the Intrusion Detection System System Protection Profile, version 1.6. All requirements not identified as modified or removed were included in their original and complete form.

7.2.1 Modified PP Items

The following table identifies items that were modified from the original specification within the PP. Braces have been added to numerous requirements in order to adapt the conventions from the PP to match the conventions defined for this ST. The addition of braces is NOT mentioned as a change to the requirements because it does not affect the meaning of the requirement.

Also, the IDS System PP utilized a spelling of “authorised” which has been changed to “authorized”, without a change in meaning.

Table 10: Modified PP Items

Modified Item:	Rationale:
FAU_GEN.1.1 b) FAU_GEN.1.2 b)	The table identifier has been changed to refer to the table as numbered in this ST.
FAU_SAR.1	Completed both assignments that were left by the PP. In the first, the “authorized user” specified by the PP is defined to be the “authorized administrator”. In the second, the “list of audit information” is defined as “all auditable events that are recorded.”
FAU_SEL.1.1 b)	Item b) was modified to complete the assignment to indicate that no additional attributes are used in the audit selectivity decision.

Modified Item:	Rationale:
FAU_STG.2	The assignment for a "metric for saving audit records" has been completed in the ST as "at least 50% of the space available for". The PP's selection of "detect" has been replaced by the selection of "prevent" because it is a stricter interpretation of the CC requirement. The selection in the 3rd element has been completed by choosing "audit storage exhaustion". The SFR has been refined to match the CC Version 2.3 requirement for FAU_STG.2
FAU_STG.4.1	The selection has been completed by choosing, "overwrite the oldest stored audit records".
FIA_UAU.1	The assignment in element 1 has been completed by specifying "no action".
FIA_ATD.1 d)	The assignment has been completed by specifying "No additional attributes".
FIA_UID.1	The assignment in element 1 has been completed by specifying "no action".
FMT_MTD.1.1	The assignment to specify "the authorized identified roles" has been completed to indicate "**authorized administrators and authorized system administrators**".
FMT_SMR.1	The assignment to specify "other authorized identified roles" has been completed to identify the role "operator".
IDS_SDC.1	The selection in the first element was completed by choosing "network traffic" from the set of choices provided by the PP. The assignment in the first element for "other specifically defined events" was completed by specifying "no additional events". In the second element the table identifier has been changed to refer to the table as numbered in this ST. Finally, the table contents have been reduced to coincide with the selection performed in the first element.
IDS_ANL.1	The selection in the first element was completed by choosing "signature" from the set of choices provided by the PP. The assignment in the first element for "other analytical functions" was completed by "none". The assignment in the 2nd element for "other security relevant information about the result" was completed with "Data destination, protocol, and severity".
IDS_RCT.1	This requirement was modified as follows: 1) The alarm destination was defined as "**the system data log and the administrators defined in the security policy"** 2) The appropriate action was defined as "**no additional actions"**
IDS_RDR.1	The assignment for "authorized users" was completed using "Operators, Authorized system administrators, and authorized administrators". The assignment for a "list of system data" was completed with "all system data"

Modified Item:	Rationale:
IDS_STG1.3	This requirement was modified as follows: 1) The metric for saving System data was defined as "**the most recent, limited by available storage"** 2) The following condition was selected "System data storage exhaustion"
IDS_STG.2.1	The selection has been completed by choosing "overwrite the oldest stored System data".
ACM_CAP.2 ADV_HLD.1 AVA_VLA.1	These assurance requirements have been refined to match the CC version 2.3 requirements.

7.2.2 Removed PP Items

The following SFR's from the PP were not included in the ST

Item Removed:	Rationale:
FIA_AFL.1, FPT_ITA.1, FPT_ITC, and FPT_ITI.1	Per PD-0097 Compliance with IPS System PP Export Requirements, since there are no communication from external IT products and the TOE these SFR's are not required. The PD states "The inter-TOE SFR's (FPT_ITA.1, FPT_ITC.1 and FPT_ITI.1) apply to communication with remote IT systems. However, these requirements were incorrectly included in the system PP because the IPS system has no such communication." "Additionally, the requirement to detect attempts to access the TOE by untrusted external IT products (FIA_AFL.1) was incorrectly included in the system PP"

Per PD-0097 Compliance with IPS System PP Export Requirements, since there is no communication from external IT products and the TOE the objective O.EXPORT is not required. The PD states

"Likewise, the O.EXPORT objective was erroneously replicated into the system PP"

7.3 PP Additions

The following security requirement, assurance measures or security objective statements are identified as being additional to the security requirement and security objective statements that are already stated within Intrusion Detection System System Protection Profile, version 1.6:

Table 11: PP Additions

Item Added:	Rationale:
ALC_FLR.2	This assurance measure provides the necessary steps for flaw remediatation required to augment the EAL level.
AVA_MSU.1	This assurance measure was added to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed
FMT_SMF.1	This requirement was added to comply with a CCEVS interpretation.

8.0 Rationale

This section presents the evidence used in the ST evaluation to support the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements. This section also demonstrates that any PP conformance claims are valid.

8.1 Security Objectives Rationale

All of the security objectives have been drawn from a validated PP (IDS System PP). Please consult that protection profile for the description of the rationale associated with the security objectives.

8.2 Security Requirements Rationale

All of the security functional requirements have been drawn from a validated PP (i.e., the IDS System PP). Please consult that protection profile for the relevant rationale.

- IDS System PP section 7.3, “Rationale for Security Requirements”;
- IDS System PP section 7.4, “Rationale for Assurance Requirements”;
- IDS System PP section 7.5, “Rationale for Explicitly Stated Requirements”;
- IDS System PP section 7.7, “Rationale for Satisfying All Dependencies”;

8.2.1 Dependency Rationale for Added Requirements

This ST adds oen security functional requirement, FMT_SMF.1, beyond those included in the PP. This ST also adds two assurance requirements. The mapping to demonstrate that dependencies for these requirements have been satisfied is shown below.

Requirement	Dependency	Satisfied by
FMT_SMF.1	No dependencies	NA
ALC_FLR.2	No dependencies	NA
AVA_MSU.1	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1

8.2.2 Internal Consistency of SFR’s

The IT security requirements defined for the TOE are taken from a validated PP, and thus no further justification is needed for conflicting IT security requirements.

8.2.3 EAL Justification

TippingPoint has chosen to pursue a Common Criteria evaluation because of the government customer requirements that are mandated by USDoD NSTISSP #11. This policy requires a Common Criteria certification for all products to be used within systems used for entering, processing, storing, displaying, or transmitting national security information.

TippingPoint has specifically chosen an EAL2 evaluation assurance level to meet the requirements mandated by the DoD and Air Force divisions of the government in accordance with the USDoD NSTISSP #11 Interpretation

and the USAF CIO Memorandum. EAL2 has been specifically chosen to meet the requirements mandated in the Protection Profile Intrusion Detection System System Protection Profile, version 1.6.

This ST contains the assurance requirements from the CC EAL2 assurance package augmented with ALC_FLR.2 and AVA_MSU.1. The CC permits assurance packages to be augmented, which allows the addition of assurance components from the CC not already included in the EAL. Augmentation was chosen to provide the added assurance obtained by defining flaw remediation procedures and ensuring that there is no misleading, conflicting or unreasonable guidance. The addition of these assurance components is based on good commercial development practices.

While the System may monitor a hostile environment, it is expected to be located within a non-hostile environment and embedded in or protected by other products designed to address threats that correspond with the intended environment. The security environment also assumes that the TOE components are physically protected. The TOE is also restricted from unauthorized remote administration, which prevents offering any opportunity for an attacker to bypass the security policies without physical access. As such, it is believed that EAL 2, augmented with ALC_FLR.2 and AVA_MSU.1, provides an appropriate level of assurance in the security functions offered by the TOE

8.2.4 Validation of Strength-Of-Function Claims

Tipping Point IPS devices are targeted at a generalized IT environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a low attack potential. As such, minimum and explicit strength of function claims of ‘SOF-basic’ is appropriate for the intended environment.

The TOE (specifically, the TOE’s password mechanism under FIA_UAU.1) meets or exceeds the minimum strength of function claim of SOF-basic. The TOE requires user defined authentication tokens (i.e., passwords) that can be analyzed via probabilistic or permutational means. In the evaluated configuration, the TOE requires that the minimum password length used to authenticate a user be equal to or greater than 8 characters. The password must contain at least two alpha characters, one numeral and one non-alphanumeric character.

8.3 TOE Summary Specification Rationale

8.3.1 Security Functions Meet SFR's

Table 12: Mapping of TOE SFR's to TOE Security Functions

	Security Audit	**Identification and Authentication**	**Security Management**	**Protection of the TSF**Error! Reference source not found.	**Intrusion Detection (EXP)**
FAU_GEN.1 Audit data generation	**X**				
FAU_SAR.1 Audit review	**X**				
FAU_SAR.2 Restricted audit review	**X**				
FAU_SAR.3 Selectable audit review	**X**				
FAU_SEL.1 Selective audit	**X**				
FAU_STG.2 Guarantees of audit data availability	**X**				
FAU_STG.4 Prevention of audit data loss	**X**				
FIA_ATD.1 User attribute definition		**X**			
FIA_ATD.1 User attribute definition		**X**			
FIA_UID.1 Timing of identification		**X**			

	Security Audit	**Identification and Authentication**	**Security Management**	**Protection of the TSF**Error! Reference source not found.	**Intrusion Detection (EXP)**
FMT_MOF.1 Management of security functions behaviour			**X**		
FMT_MTD.1 Management of TSF data			**X**		
FMT_SMF.1 Specification of Management Functions			**X**		
FMT_SMR.1 Security roles			**X**		
FPT_RVM.1 Non-bypassability of the TSP				**X**	
FPT_SEP.1 TSF domain separation				**X**	
FPT_STM.1 Reliable time stamps				**X**	
IDS_SDC.1 System Data Collection (EXP)					**X**
IDS_ANL.1 Analyser analysis (EXP)					**X**
IDS_RCT.1 Analyser react (EXP)					**X**
IDS_RDR.1 Restricted Data Review (EXP)					**X**
IDS_STG.1 Guarantee of System Data Availability (EXP)					**X**
IDS_STG.2 Prevention of System data loss (EXP)					**X**

Table 13: Rationale for Security Functions Satisfying SFR's

Security Functions	SFR's	Rationale
Security Audit	FAU_GEN.1	The TOE implements audit data generation for events related to operations performed by TippingPoint Intrusion Prevention System (IPS) E-Series. These events include the start-up and shutdown of audit functions, access to System, access to the TOE and System data, reading of information from the audit records, unsuccessful attempts to read information from the audit records, all modifications to the audit configuration that occur while the audit collection functions are operating, all use of the authentication mechanism, all use of the user identification mechanism, all modifications in the behavior of the functions of the TSF, all modifications to the values of TSF data, and modifications to the group of users that are part of a role.
	FAU_SAR.1	The TOE implements audit review by providing the superuser with the capability to view the auditable events recorded in a manner that is interpretable.
	FAU_SAR.2	The TOE implements restricted audit review by restricting access to view the audit records to the operator and the administrator or Superuser.
	FAU_SAR.3	The TOE implements selectable audit review by providing the superuser with the capability to sort audit data based on the date, time, subject identity, type of event, and success or failure of each related event.
	FAU_SEL.1	The TOE implements selective auditing by providing the capability to select the audit events that are allowed to be recorded based on the type of event, such as attack, config, and traffic events.
	FAU_STG.2	The TOE guarantees audit data availability by preventing unauthorized access to the audit data, and ensuring the availability of the most recent audit data upon audit data storage exhaustion.
	FAU_STG.4	The TOE prevents audit data loss by providing the capability to ensure the availability of the most recent audit data upon audit data storage exhaustion.
Identification and Authentication	FIA_ATD.1	The TOE implements the association of security attributes to users by providing the capability to maintain users' identity, authentication data, and authorizations.
	FIA_UAU.1	The TOE implements user authentication by providing the capability for users to authenticate to the TippingPoint Intrusion Prevention System (IPS) E-Series.
	FIA_UID.1	The TOE implements user identification by providing the capability for users to be identified to TippingPoint Intrusion Prevention System (IPS) E-Series.

Security Functions	SFR's	Rationale
Security Management	FMT_MOF.1	The TOE implements the management of security functions behavior by providing the capability to restrict the ability to modify the behavior of the functions of System data collection, analysis and reaction to administrators and Superusers.
	FMT_MTD.1	The TOE implements management of TSF data by providing the capability to restrict the ability to query and add System and audit data and to restrict the ability to query and modify all other TOE data to the administrator and Superuser role.
	FMT_SMR.1	The TOE implements security management roles by providing roles for an administrator and Superuser role.
Protection of the TSF**Error! Reference source not found.**	FPT_RVM.1	The TOE implements non-bypass ability of the TOE security policy by requiring users to be successfully authenticated prior to allowing any other TSF-mediated actions to be performed.
	FPT_SEP.1	The TOE implements domain separation by providing the capability to manage the TOE on an interface that is inaccessible from the interface that is used to monitor traffic.
	FPT_STM.1	The TOE implements reliable time stamping by providing the capability to directly request and retrieve the time stamp for each audit event directly from the underlying operating system or kernel.
Intrusion Detection (EXP)	IDS_SDC.1	The TOE implements system data collection by providing the capability to generate Alert log and Block log records based upon the configured filter's reactions to network traffic.
	IDS_ANL.1	The TOE performs signature-based analysis of traffic as it flows through the IPS. Analysis methodologies match specific signatures (that may characterize attack attempts) to characteristics of known attacks. This analysis qualifies the severity of the potential threat and uses installed filters to achieve desired protections for the protected network segments.
	IDS_RCT.1	The TOE implements an analyzer reaction by providing the capability to gather an Alert log record and/or send an alarm to an administrator upon the detection of an intrusion.
	IDS_RDR.1	The TOE implements restricted data review by restricting capability to read system data logs, security policies, profiler data, and user account information from the System data to only the administrators and Superusers.
	IDS_STG.1	The TOE guarantees system data availability by preventing unauthorized access to the system data, and ensuring the availability of the most recent system data upon system data storage exhaustion.

Security Functions	SFR's	Rationale
	IDS_STG.2	The TOE prevents system data loss by providing the capability to ensure the availability of the most recent system data upon audit data storage exhaustion.

8.3.2 Assurance Measures Meet Assurance Requirements

This section demonstrates that the claim is justified that the stated assurance measures are compliant with the assurance requirements. This ST contains the assurance requirements from the CC EAL2 assurance package that are already stated within Intrusion Detection System System Protection Profile, version 1.6: The assurance requirements have been augmented with ALC_FLR.2 and AVA_MSU.1. The CC permits assurance packages to be augmented, which allows the addition of assurance components from the CC not already included in the EAL. Augmentation was chosen to provide the added assurance obtained by defining flaw remediation procedures and ensuring that there is no misleading, conflicting or unreasonable guidance. The addition of these assurance components is based on good commercial development practices.

Table 14: Rationale for Assurance Measures Satisfying SARs

Assurance Requirements	Assurance Measures	Rationale
ACM_CAP.2	TippingPoint Configuration Items for Common Criteria	This document provides a unique identifier for the TOE.
		This document lists the configuration items that comprise the TOE and describes the methods used for identifying them.
ADO_DEL.1	TippingPoint Delivery of Product to Customer	This document provides a unique identifier for the TOE and identification of the TOE components to be delivered.
		This document provides procedures for the delivery method of the TOE to the consumer.
ADO_IGS.1	*Common Criteria Certified TippingPoint Hardware Installation and Safety Guides for Version 2.5.3*; TECHD-0000000073; Publication Control Number 030308 *TippingPoint Command Line Interface Reference Version 2.5.3*; Part Number TECHD-0000000084; Publication Control Number 11907 *TippingPoint Local Security Manager User Guide Version 2.5.3*; Part Number TECHD-00000000082; Publication Number 11907	These documents identify unique TOE identifier, the TOE components to be installed, and the required configuration(s) for the TOE. These documents describe the steps necessary for secure installation, generation, and start-up of the TOE
ADV_FSP.1	*TippingPoint Command Line Interface Reference Version 2.5.3*; Part Number TECHD-0000000084; Publication	These documents identify the security functions that are covered by the functional specification.

Assurance Requirements	Assurance Measures	Rationale
	Control Number 11907 *TippingPoint Local Security Manager User Guide Version 2.5.3*; Part Number TECHD-00000000082; Publication Number 11907 *FSP & HLD Design Document for Common Criteria*	These documents describe the TSF and the external interfaces to the TOE security functions.
ADV_HLD.1	*FSP & HLD Design Document for Common Criteria*	These documents identify the security functions that are covered by the high-level design.
		This document groups the security functions claimed in the ST into logical subsystems. This document also describes the TOE subsystems, their interfaces, and any mechanisms required by the TOE IT environment.
ADV_RCR.1	*RCR TippingPoint Revision F (Spreadsheet)*	These documents identify the security functions that are covered by the correspondence.
		These documents identify the interfaces that are to be mapped to security functions and also provide this analysis.
AGD_ADM.1	*TippingPoint Command Line Interface Reference Version 2.5.3*; Part Number TECHD-0000000084; Publication Control Number 11907 *TippingPoint Local Security Manager User Guide Version 2.5.3*; Part Number TECHD-00000000082; Publication Number 11907	These documents identify the TOE unique identifier, any security configurations required, and assumptions to be made.
		These documents provide administrative guidance to the TOE administrative users with detailed, accurate information of how to administer the TOE in a secure manner.
AGD_USR.1	*TippingPoint Command Line Interface Reference Version 2.5.3*; Part Number TECHD-0000000084; Publication Control Number 11907 *TippingPoint Local Security Manager User Guide Version 2.5.3*; Part Number TECHD-00000000082; Publication Number 11907	This document identifies the TOE unique identifier, any security configurations required, and assumptions to be made.
		This document provides user guidance to the TOE users with the necessary background and specific information on how to correctly use the TOE's protection functions.

Assurance Requirements	Assurance Measures	Rationale
ATE_COV.1	Functional Testing Coverage for Common Criteria, TECH-0000000277, Revision I, 5/27/2008 CC test cases	These documents identify and describe the TOE security functions that are to be mapped to individual test cases.
		These documents identify the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. The testing coverage is provided within the testing procedures document as it is listed here.
AVA_VLA.1	TippingPoint Vulnerability Assessment	This document identifies the TOE components and configuration(s) for which obvious vulnerabilities may be identified.
		This document identifies any obvious vulnerability pointed out in any of the TOE evaluation deliverables or identified within a public domain (i.e. website).
ALC_FLR.2	TippingPoint Flaw remediation procedure	This document provides the necessary steps for flaw remediate.

8.4 PP Claims Rationale

The differences between this ST and the IDSSPP v1.6 are identified and described within section 7.0 of this ST.

9.0 Annex A

Annex A provides a list of acronyms, terms, and references used throughout this document.

9.1 Acronyms

9.1.1 CC-Specific Acronyms

CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSE	Threat Suppression Engine
TSF	TOE Security Function
TSP	TOE Security Policy

9.1.2 TOE-Specific Acronyms

IPS	Intrusion Prevention System
IDS	Intrusion Detection System

9.2 Terms

9.2.1 CC-Specific Terms

These terms are drawn from section 2.3 of CC Part 1.

Assets	Information or resources to be protected by the countermeasures of a TOE.
Assignment	The specification of an identified parameter in a component.
Assurance	Grounds for confidence that an entity meets its security objectives.
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.
Authentication data	Information used to verify the claimed identity of a user.
Authorized user	A user who may, in accordance with the TSP, perform an operation.
Class	A grouping of families that share a common focus.
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.
Connectivity	The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
Element	An indivisible security requirement.
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Family	A grouping of components that share security objectives but may differ in emphasis or rigor.

Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.
Guidance documentation	Guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in section 6.2 of this ST.
Human user	Any person who interacts with the TOE.
Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Informal	Expressed in natural language.
Internal communication channel	A communication channel between separated parts of TOE.
Internal TOE transfer	Communicating data between separated parts of the TOE.
Inter-TSF transfers	Communicating data between the TOE and the security functions of other trusted IT products.
Iteration	The use of a component more than once with varying operations.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
Organizational security policies	One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.
Package	A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.
Product	A package of IT software and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Reference monitor	The concept of an abstract machine that enforces TOE access control policies.
Reference validation mechanism	An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
Security attribute	Characteristics of subjects, users, objects, information, and/or resources that is used for the enforcement of the TSP.

Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Selection	The specification of one or more items from a list in a component.
Semiformal	Expressed in a restricted syntax language with defined semantics.
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
SOF-basic	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.
SOF-high	A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential.
Subject	An entity within the TSC that causes operations to be performed.
System	A specific IT installation, with a particular purpose and operational environment.
Target of Evaluation (TOE)	An IT product or system and its associated guidance documentation that is the subject of an evaluation.
TOE resource	Anything useable or consumable in the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware and software of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Functions Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
TOE security policy model	A structured representation of the security policy to be enforced by the TOE.

Transfers outside TSF control	Communicating data to entities not under control of the TSF.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.
Trusted path	A means by which a user and a TSF can communicate with necessary confidence to support the TSP.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.

9.2.2 TOE-Specific Terms

Analyzer data	Data collected by the Analyzer functions.
Analyzer functions	The active part of the Analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.
Assets	Information or resources to be protected by the countermeasures of a TOE.
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Audit Trail	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	Establishing the validity of a claimed user or object.
Administrator	A subset of authorized users that manage an IPS component.
Authorized User	A user that is allowed to perform IPS functions and access data.
Availability	Assuring information and communications services will be ready for use when expected.
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.

IPS component	A Sensor, Scanner, or Analyzer.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection (ID)	Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
Intrusion Detection System (IPS)	A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
Intrusion Detection System Analyzer (Analyzer)	The component of an IPS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).
Intrusion Detection System Scanner (Scanner)	The component of an IPS that collects 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.
Intrusion Detection System Sensor (Sensor)	The component of an IPS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.
Network	Two or more machines interconnected for communications.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packet Sniffer	A device or program that monitors the data traveling between computers on a network.
Scanner data	Data collected by the Scanner functions.
Scanner functions	The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data)
Security	A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.
Sensor data	Data collected by the Sensor functions.
Sensor functions	The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data).
Security Policy	The set of rules (either administrator-defined or provided by default) that the TSE analyzer uses in order to provide protection versus malicious network traffic as it passes through the sensing interface of the TOE.
System data	Data collected and produced by the System functions.
System functions	Functions performed by all IPS components (i.e., Analyzer functions, Scanner functions, and Sensor functions).

Trojan Horse	An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.
Virus	A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.
Vulnerability	Hardware or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

9.3 Interpretations

9.3.1 International Interpretations

No international (CCIMB) interpretations are included within this ST.

9.3.2 National Interpretations

No national (NIAP) interpretations are included within this ST.