HP TippingPoint
Intrusion Prevention Systems
Security Target

Version 1.0
July 29, 2011

Prepared for:
TippingPoint/Hewlett-Packard Corporation
14231 Tandem Blvd
Austin, TX 78728
USA

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

Contents

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is HP TippingPoint Intrusion Prevention Systems, comprising the S6100N, S5100N, S2500N, S1400N, and S660N model appliances running TippingPoint Operating System v3.2.1, and the S330, S110 and S10 model appliances running TippingPoint Operating System v3.1.4.

The Security Target contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the assumptions, threats, and organizational security policies that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the objectives necessary to counter the defined threats and satisfy the assumptions and organizational security policies
- IT Security Requirements (Section 5)—provides a set of security functional requirements to be met by the TOE. The IT security requirements also provide a set of security assurance requirements that are to be satisfied by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the security functional requirements
- Protection Profile Claims (Section 7)—provides rationale that the TOE conforms to the PP(s) for which conformance has been claimed
- Rationale (Section 8)—provides mappings and rationale for the security environment, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – HP TippingPoint Intrusion Prevention Systems Security Target

ST Version – 1.0

ST Date – July 29, 2011

TOE Identification – HP TippingPoint Intrusion Prevention Systems, comprising the S6100N, S5100N, S2500N, S1400N, and S660N model appliances running TippingPoint Operating System v3.2.1, and the S330, S110 and S10 model appliances running TippingPoint Operating System v3.1.4

TOE Developer – HP Networking

Evaluation Sponsor – HP Networking

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007.

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 2, September 2007
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 2, September 2007
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL3 Augmented (ALC_FLR.2).

This ST and the TOE it describes are conformant to the following Protection Profile (PP):

- U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, 25 July 2007 (IDSSPP).

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements—Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - 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 …").
- Extended Requirements (i.e., those not found in Part 2 of the CC) are identified with "(EXT)" following the identification of the new functional class/name (i.e., Intrusion Detection System (IDS)) and the associated family descriptor. Example: Analyzer analysis (EXT) (IDS_ANL.1)
- Other sections of the ST—Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document. A brief definition is provided for abbreviations that are potentially unfamiliar, are specific to the TOE, or not obviously self-explanatory.

AES	Advanced Encryption Standard
AH	Authentication Header
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme—the US CC Scheme
CIDR	Classless Inter Domain Routing
CLI	Command Line Interface
CM	Configuration Management
CMOS	Complementary metal-oxide-semiconductor—a class of integrated circuits
DES	Digital Encryption Standard
DSA	Digital Signature Algorithm
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GbE	Gigabit Ethernet
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

ICMP	Internet Control Message Protocol
ID	Identity or Identification
IDS	Intrusion Detection System
IDSSPP	US Government Protection Profile Intrusion Detection System System for Basic Robustness Environments
IM	Instant Messaging
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LC	Local Connector—a type of optical fiber connector
LCD	Liquid Crystal Display
LSM	Local Security Manager—HP Networking name for the IPS device GUI
MAC	Media Access Control
NIST	National Institute of Standards and Technology
P2P	Peer-to-Peer
PC	Personal Computer
PD-0097	Precedent Decision 97, issued by CCEVS
POSIX	Portable Operating System Interface for Unix
PP	Protection Profile
RC2	Rivest Cipher 2—a block cipher designed by Ron Rivest
RC4	Rivest Cipher 4—a block cipher designed by Ron Rivest
RSA	Rivest-Shamir-Adleman—an asymmetric cryptographic algorithm
SAR	Security Assurance Requirement
SFP	Small form-factor Pluggable—extractable optical or electrical transmitter/receiver module used in telecommunications
SFP	Security Function Policy
SFR	Security Functional Requirement
SMS	Security Management System—HP Networking name for its architecture for managing multiple IPS devices.
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TOS	TippingPoint Operating System—the software component of the HP TippingPoint IPS device
TSE	Threat Suppression Engine—a logical component of the HP TippingPoint IPS device
TSF	TOE Security Functionality
TSFI	TSF Interface
UDP	User Datagram Protocol
USGv6	United States Government v6—technical infrastructure developed by NIST to support wide-scale adoption of IPv6 within the US government
ZPHA	Zero Power High Availability

2. TOE Description

The Target of Evaluation (TOE) is the HP TippingPoint Intrusion Prevention System (IPS) devices, comprising the S6100N, S5100N, S2500N, S1400N, and S660N running TippingPoint Operating System v3.2.1, and the S330, S110 and S10 model appliances running TippingPoint Operating System version 3.1.4. The devices covered within the scope of the evaluation are network-based intrusion prevention system appliances that are deployed inline between pairs of networks.

The following list summarizes the features provided by v3.2.1 of the TippingPoint Operating System that are not included in v3.1.4:

- Support for certification to USGv6
- SMS management of IPS users and roles, with support for RADIUS and Active Directory
- Recommended filter settings based on deployment location
- Congestion avoidance
- General throughput performance optimizations and improvements.

None of these features represents any differences in the security functionality of the evaluated version of the TOE. Both v3.1.4 and v3.2.1 of the TippingPoint Operating System satisfy the security functional requirements specified in this ST.

The remainder of this section provides an overview of the TOE and a description of the TOE, including a description of the physical and logical scope of the TOE.

2.1 TOE Overview

HP Networking's IPS is a hardware-based intrusion prevention platform consisting of network processor technology and HP Networking's own set of custom Field Programmable Gate Arrays (FPGAs). The TOE is a hardware and software appliance that contains all the functions needed for intrusion prevention, including Internet Protocol (IP) defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of network protocols.

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

A filter comprises rules and conditions used by the TOE to detect and handle malicious network traffic. Each filter includes an action set that determines the TOE's response when network traffic matches a filter.

The TOE provides intrusion prevention for the network according to the number of network connections and hardware capabilities of the specific model. A single instance of the TOE can be installed at the perimeter of the network, at the network core, on the customer's Intranet, or in all three locations. HP TippingPoint IPS devices can secure up to 11 network segments depending upon traffic volumes and the load capacity of the model.

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

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

The TOE organizes filters into groups and categories of filter groups, based on the type of protection provided by the filter. The TOE defines the following categories and filter groups:

Application Protection Filters—defend against known exploits and exploits that may take advantage of known vulnerabilities targeting applications and operating systems. This category comprises the following groups:

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

Infrastructure Protection Filters—protect network bandwidth and network infrastructure elements such as routers and firewalls from attack by using protocols and detecting statistical anomalies. This category comprises the following groups:

- Network Equipment
- Traffic Normalization

Performance Protection Filters—block or rate-limit traffic from applications that can consume excessive bandwidth, leaving network resources available for use by key applications. This category comprises the following groups:

- IM (Instant Messaging)
- P2P (Peer-to-Peer)
- Streaming Media.

Category settings are used to assign global configuration settings to filters in a filter group. For example, if there is no requirement to monitor P2P traffic, the category settings for the P2P filter group within the Performance Protection category can be set to disable these filters. Category settings comprise the following global parameters:

- State—determines whether filters within the filter group are enabled or disabled. If a filter group is disabled, all filters within the group are disabled
- Action Set—determines the action set that all filters within a group will execute when a filter match occurs.

It is also possible to override category settings on individual filters by editing the filter to define custom settings.

Each action set can include a set of recipients (termed "notification contacts") to receive alerts when the device detects and responds to traffic. A notification contact can be: a remote syslog server; an email address; an SNMP server; or the TOE's management GUI. The TOE also enables the administrator to set limits and exceptions for filters, which apply filters to specific IP addresses or exclude traffic from filtering based on source and destination IP addresses.

The TOE manages filter behavior using a mechanism known as Adaptive Filtering. This works by monitoring each filter and identifying any filter suspected of causing congestion. Any filter identified in this fashion is handled in one of two ways, depending on how global or filter-level Adaptive Filtering is configured:

- Automatic Mode—enables the TOE to automatically disable the identified filter and generate a system message
- Manual—enables the TOE to generate a system message regarding the identified filter. However, the filter is not disabled. Adaptive Filtering should be configured for this mode in the evaluated configuration to prevent filters being automatically disabled.

The TOE uses Security Profiles to define the traffic that it monitors and the filters that it applies. Traffic monitoring is based on incoming and outgoing port pairs. The default filtering configuration can be used to protect the segment or it can be customized as necessary. The segment specifies both the port and the traffic direction, allowing separate Security Profiles to be defined for traffic in and out of a port. The default Security Profile is set to ANY incoming ports and ANY outgoing ports, with all filters configured with their default settings (which could be to block or permit traffic).

In addition to IPS filters (which are also identified as 'Digital Vaccine' filters in the TOE documentation[1]), the TOE provides Traffic Management Profiles that allow traffic management filters to be configured and applied to traffic on virtual segments. These allow the TOE to operate like a firewall.

The TOE supports IPv6 traffic inspection, and IPv6 options are available when configuring the Security Profile options. Most IPS filters are compatible with both IPv4 and IPv6 traffic. The host management port, default gateway, and management port routes can also be configured with IPv6 addresses.

The TOE enables inspection of a wide range of tunneled traffic, including:

- Generic Routing Encapsulation (GRE)
- Mobile IPv4 (IP-in-IP)
- IPv6, including 6-in-4, 4-in-6, and 6-in-6
- Authentication Header (AH) tunnels
- Tunnels up to 10 layers of tunneling or a header size of 256 bytes.

The S6100N, S5100N and S2500N models also support inspection bypass rules for trusted traffic. Any network traffic matching an inspection bypass rule is transmitted through the TOE without further inspection, either by traffic management filters or IPS filters.

The TOE provides a Management Interface that enables authorized administrative users to access the security management capabilities of the TOE and to view System data and audit logs. Authorized administrative users are identified and authenticated by the TOE prior to gaining access to the TOE. The Management Interface provides two methods for accessing the TOE—a Command Line Interface (CLI) and a web-based Graphical User Interface (GUI) termed the Local Security Manager (LSM). The TOE supports secure access for both methods—SSHv2 for the CLI and HTTPS for the LSM.

The HP TippingPoint IPS documentation describes mechanisms (termed "High Availability") intended to support continued flow of network traffic in the event of a system failure of the IPS device. These mechanisms are outside the scope of the evaluation. However, the administrator needs to be aware of the following aspects of these mechanisms, as they have implications for the secure operation of the TOE:

- Intrinsic Network High Availability—if the device detects certain failed conditions, it enters Layer-2 Fallback mode and either permits or blocks all traffic on each segment, depending on the Layer-2 Fallback configuration setting for the segment. If the segment's Layer-2 Fallback mode is "permit", all traffic on the segment passes through the device without inspection (i.e., the IPS capability of the device is disabled). In the evaluated configuration, the Layer-2 Fallback mode should be set to "block" on each segment
- Zero-Power High Availability—allows network traffic to continue flowing without inspection (i.e., the IPS capability of the device is disabled) if the device loses power. This mechanism should not be used in the evaluated configuration.

[1] Digital Vaccine® is a registered trademark of TippingPoint Technologies, Inc. that refers to packages of filters developed by TippingPoint and supplied with the HP TippingPoint IPS devices.

2.2 TOE Architecture

2.2.1 Deployment Architecture

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

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

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

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

The HP TippingPoint IPS also forms one component of the HP TippingPoint System, a suite of security products that also includes the Security Management System (SMS) Secure Server, SMS Management Client, and Core Controller. The SMS Secure Server is a hardware appliance that can be used to manage multiple HP TippingPoint IPS appliances. The SMS Management Client is a Java-based application that provides a management interface to the SMS Secure Server. The Core Controller is a hardware appliance that can be used to balance traffic loads across multiple IPS appliances. These products are separately purchasable and are not required to support the operation of the HP TippingPoint IPS in its evaluated configuration. As such, none of these other products are included within the scope of this evaluation.

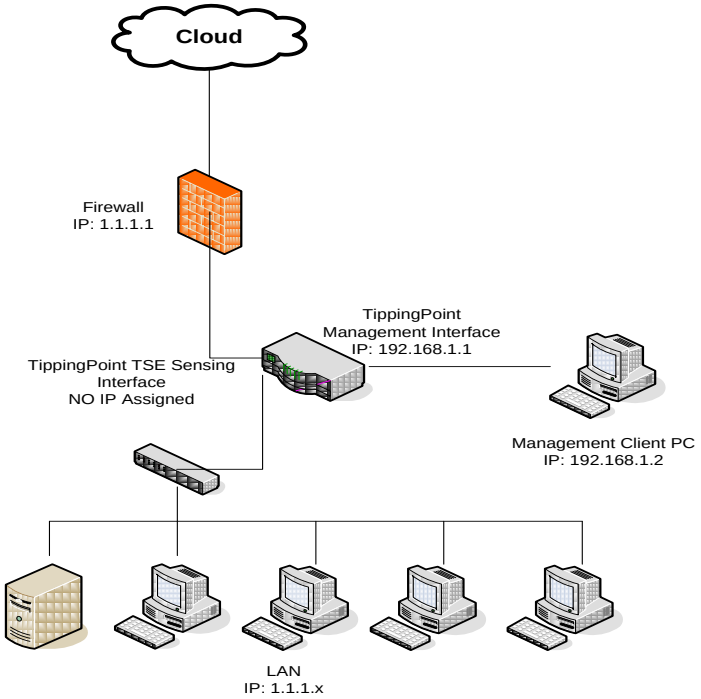

Figure 1: Deployment Scenario

2.2.2 Software Architecture

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

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

The OS provides a set of support services to both the TSE and Management Interface. Amongst other functions, the OS provides services to utilize device hardware features (e.g., a reliable time stamping capability based upon a CMOS clock). More information regarding OS functions is given in section 2.2.2.1.

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

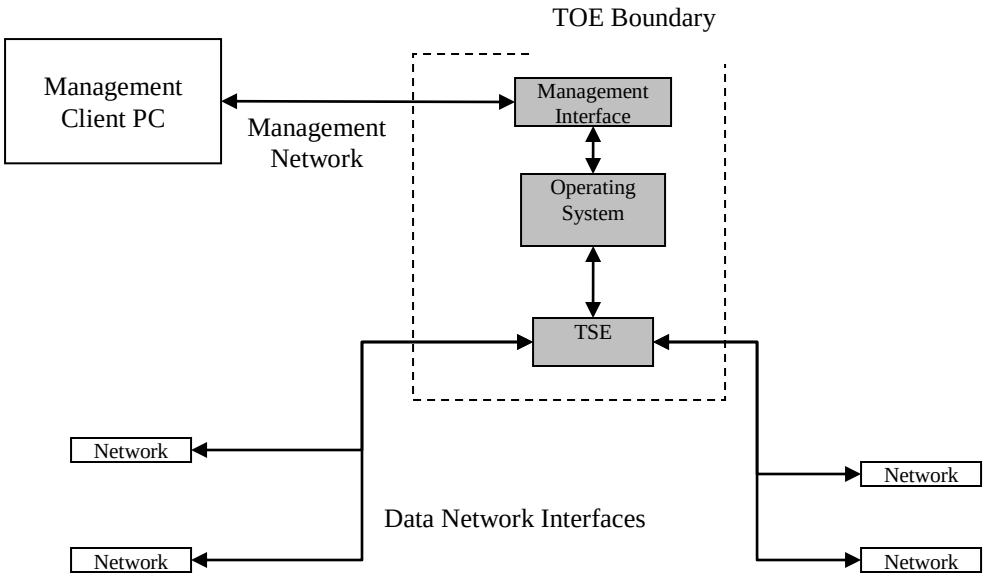

Figure 2: TOE Architecture

2.2.2.1 Operating System

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

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

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

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

2.2.2.2 Threat Suppression Engine

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

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

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

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

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

Sensor Capabilities

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

Analyzer Capabilities

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

Within each analytical result, the following information is stored:

- Date and time of the result
- Type of result (message, policy ID, signature ID, and classification)
- Identification of data source

- Data destination
- Protocol
- Severity.

2.2.2.3 Management Interface

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

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

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

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

- Superuser—full access to the TOE. This role is able to manage the users of the TOE and to view/modify the configuration of the TOE and the logs
- Administrator—write access to the TOE. This role is able to view/modify the configuration of the TOE (with the exception of managing user accounts) and the logs (with the exception of selection of auditable events and viewing/clearing of the audit log)
- Operator—read-only access to the TOE. This role is able to view the system data logs (with the exception of audit logs) and configuration of the TOE, but is not permitted to modify any information other than his/her own password.

All security relevant and Management Interface actions are recorded in the Audit log. The Audit log records the command that was executed, the username of the user who performed an action, the interface from which the user logged in, such as the LSM or CLI, and a timestamp of when the action was performed. Storage services for the Audit log are provided by the operating system file system services. The Management Interface also provides a mechanism for administrators to review the contents of the audit trail.

2.2.3 Physical Boundaries

The physical boundary of the TOE is the HP TippingPoint IPS device (i.e., a S6100N, S5100N, S2500N, S1400N, S660N, S330, S110 or S10 model device).

The S6100N, S5100N, S2500N, S1400N and S660N models each comprise a single chassis that is rack-mountable on a 19 or 23 inch rack and takes up 2 rack units of space. Each device provides the following external interfaces:

- 10 1GbE copper ports paired into 5 1GbE segments
- 10 1GbE fiber ports paired into 5 1GbE segments
- 1 1GbE copper network management port
- 1 RJ-45 console port
- 1 interface for external Zero Power High Availability (ZPHA) device
- 1 Compact Flash drive that provides a facility to store TSF data (such as logs, traffic threshold history, persistent statistics, packet traces) for long term persistence or archiving purposes
- A Liquid Crystal Display (LCD) screen and associated keypad that can be used to initially configure the appliance and to subsequently display basic configuration information (Note: use of the LCD/keypad, either for initial configuration or for subsequent information display, is excluded from the scope of evaluation).

Additionally, the S6100N, S5100N and S2500N models each include 2 10GbE fiber ports paired into 1 10GbE segment.

The S330, S110 and S10 devices are intended for smaller network deployments, such as remote offices (S10 model) and where bandwidth does not exceed 100Mbps (S110 model) or 300 Mbps (S330 model). Each S330, S110 and S10 device comprises a single chassis that provides the following external interfaces:

- 4 (for the S10) or 8 (for the S110 and S330) 1GbE copper ports paired into 2 or 4 1GbE segments
- 1 1GbE copper network management port
- 1 RJ-45 console port.

The ports on the S6100N, S5100N, S2500N, S1400N and S660N devices associated with the data networks, through which monitored traffic flows, can be connected to either twisted pair (copper) networks or fiber optic networks. The ports on the S330, S110 and S10 devices support only twisted pair networks. For twisted pair networks, the Copper Segments interface is used via RJ45 connectors. For fiber networks, Small Form-factor Pluggable (SFP) transceivers with Local Connector (LC) connectors are used. Both Single-Mode and Multi-Mode SFP fiber modules are supported. Once connected, network traffic on these interfaces can be monitored by the TOE.

The network management port supports the connection of a management network hosting management client PCs and the following optional servers: syslog; SMTP; SNMP. The network management port presents the LSM (over HTTPS) and CLI (over SSHv2) administrative interfaces. The LSM requires one of the following browsers on the management client PC: Internet Explorer 6.x or higher; Firefox 1.5+; Mozilla 1.7+; or Netscape 8.1+. The CLI requires an SSH client on the management client PC. Note that the LSM can also be accessed via HTTP and the CLI can be accessed via Telnet, but use of HTTP and Telnet over the management network is excluded from the evaluated configuration. The TOE's HTTP and Telnet servers are disabled by default and should not be enabled.

The TOE can be configured to send alarms (i.e., notifications of detected malicious network traffic) to the following external destination types: syslog server; email address (which requires an SMTP server); SNMP server. These alarms are in addition to the alarms the TOE writes to the System data logs.

The management network, management client PCs, optional servers, and all software on these clients and servers are in the operational environment of the TOE.

Additionally, a serial console port is provided to allow a local terminal to be connected. When connected, the CLI is available on the local terminal. Communication between the local terminal and the serial console port is not protected and so such connections should only be used when both the local terminal and the TOE are in the same physically secure location.

In summary, use of the TOE may require the following components in its operational environment:

- Serial terminal client, connected via the serial console port, to support local management of the TOE via the CLI
- Management client PCs, connected via the network management port, to support remote management of the TOE. The management client PC in turn requires:
    - A browser (Internet Explorer 6.x or higher; Firefox 1.5+; Mozilla 1.7+; or Netscape 8.1+) to connect to the LSM; and/or
    - An SSHv2 client to connect to the CLI
- Syslog server, SMTP server, and/or SNMP server, connected via the network management port, to receive alarms.

2.2.4 Logical Boundaries

This section summarizes the security functions provided by HP TippingPoint IPS devices.

2.2.4.1 Security Audit

The TOE is able to generate auditable events for the basic level of audit. It provides Superuser administrative users with the ability to review audit records stored in the audit trail and prevents other administrative user roles from

reviewing the audit data. Superuser administrative users are able to select auditable events to be audited, based on event type. The audit records are stored in the underlying file system, where they are protected from unauthorized modification and deletion. When the space available for audit storage is exhausted, the oldest 50% of audit records are deleted and an audit record to this effect is generated.

2.2.4.2 Identification and Authentication

The TOE identifies and authenticates all administrative users[2] of the TOE before granting them access to the TOE. The TOE associates a user identity, authentication data (password), and authorizations (or security role) with each user. The TOE enforces minimum requirements for the construction of user passwords and provides a mechanism to lock or disable a user account after a configured number of consecutive failed attempts to logon.

2.2.4.3 Intrusion Detection and Prevention

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

2.2.4.4 Traffic Management

The TOE can be configured to operate as a firewall, blocking or permitting network traffic based on protocol or IP address and port. Network traffic that is permitted based on traffic management filtering is still subject to IPS filtering, unless the traffic management filter is configured to allow traffic through the device without IPS filtering. On the S6100N, S5100N, and S2500N models, inspection bypass rules can be configured that permit matching network traffic to pass through the TOE without being subject to either traffic management or IPS filters.

2.2.4.5 Security Management

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

2.2.4.6 TSF Protection

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

2.2.4.7 Trusted Path

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

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

The TOE supports a FIPS mode of operation and, when configured in FIPS mode, will allow only FIPS 140-2 approved cryptographic algorithms to be used. All models of the TOE have completed FIPS 140-2 validation (Certificate #1545). Note the TOE is not required to operate in FIPS mode to be in the evaluated configuration—the choice to do so or not is left up to the customer.

2.2.5 Excluded Functionality

The following capabilities of the TOE are not included in the scope of the evaluation and no claims are made regarding them:

- High availability capabilities
- Uploading and use of X.509 certificates to support checking of client certificates when connecting to the LSM.

2.3 TOE Documentation

This section identifies the guidance documentation included in the TOE. The documentation for the S6100N, S5100N, S2500N, S1400N, and S660N model appliances running TippingPoint Operating System v3.2.1 comprises:

- *TippingPoint Local Security Manager User's Guide: TippingPoint Operating System V. 3.2, TECHD-0000000293, Second Edition: January 2011*
- *TippingPoint Command Line Interface Reference: TippingPoint Operating System V. 3.2, TECHD-0000000291, Second Edition: January 2011*
- *TippingPoint N-Platform Hardware Installation and Safety Guide*, *TECHD-0000000285 Rev A04, Second Edition: January 2011.*

The documentation for the S330, S110 and S10 model appliances running TippingPoint Operating System v3.1.4 comprises:

- *Local Security Manager User's Guide: TippingPoint Operating System V. 3.1, TECHD-0000000293, Second Edition: January 2011*
- *Command Line Interface Reference: TippingPoint Operating System V. 3.1, TECHD-0000000291, TOS 3.1.4 Beta edition: August 2010*
- *TippingPoint 10/110/330 Hardware Installation and Safety Guide*, *TECHD-0369, Rev A01, Second Edition: January 2011.*

3. Security Problem Definition

This section summarizes the threats addressed by the TOE, organizational security policies satisfied by the TOE, and assumptions about the intended environment of the TOE. There are no modifications to the security environment as described in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, to which this ST claims conformance.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

3.1.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.1.2 Physical Assumptions

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

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.1.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

3.2 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

3.2.1 TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

3.2.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the TOE.

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

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4. Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Information Technology (IT) Security Objectives

The following are the TOE security objectives:

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The Scanner must collect and store 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.
O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.TRAFFIC	The TOE must provide a capability to filter network traffic based on combinations of protocol, IP address and port.

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives.

OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.INTROP	The TOE is interoperable with the IT System it monitors.

OE.CONFID	The IT Environment will provide the capability to protect the confidentiality of data communicated by the administrative users to the TOE.

5. IT Security Requirements

5.1 Extended Components Definition

The U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments (IDSSPP) includes extended security functional requirements, which are included in this ST. The IDSSPP provides a rationale for the use of extended security requirements, identifying that the CC audit family (FAU) was used as a model. However, the IDSSPP does not provide a definition of the extended components on which the extended security functional requirements are based.

5.2 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria v3.1 Revision 2 and the Protection Profile (PP) identified in the Protection Profile Claims section.

This ST includes a number of extended requirements. Each of the extended requirements is defined in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments. The extended requirements can be identified by the use of the keyword "EXT" in the title.

Every SFR included in the PP is addressed in this ST. Note, however, that the PP was written using CC v3.1, Revision 1, whereas this ST claims conformance to CC v3.1, Revision 2. The SFRs therefore reproduce the wording of CC Part 2 v3.1, Revision 2. Section 7 (Protection Profile Claims) identifies the SFRs whose wording, for this reason, differs from that used in the PP.

Requirement Class	Requirement Component
FAU: Security Audit	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
FDP: User Data Protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling
	FIA_ATD.1: User Attribute Definition
	FIA_SOS.1: Verification of Secrets
	FIA_UAU.1: Timing of Authentication
	FIA_UID.1: Timing of Identification
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MTD.1: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles

Requirement Class	Requirement Component
FPT: Protection of the TOE Security Functions	FPT_STM.1: Reliable Time Stamps
FTP: Trusted path/channels	FTP_TRP.1: Trusted path
IDS: IDS Component requirements	IDS_ANL.1: Analyzer analysis (EXT)
	IDS_RCT.1: Analyzer react (EXT)
	IDS_RDR.1: Restricted Data Review (EXT)
	IDS_SDC.1: System Data Collection (EXT)
	IDS_STG.1: Guarantee of System Data Availability (EXT)
	IDS_STG.2: Prevention of System data loss (EXT)

Table 1: TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

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; 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 (if applicable), 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 Auditable Events**].

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_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FAU_STG.4	Actions taken due to the audit storage failure.	
FIA_AFL.1	Reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent restoration to the normal state.	User identity
FIA_SOS.1	Rejection by the TSF of any tested secret	User identity
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism, including the user identity provided.	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	

Component	Event	Details
FMT_SMF.1	Use of the management functions.	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FTP_TRP.1	All attempted uses of the trusted path functions	User identity

Table 2: Auditable Events

5.2.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**the authorized System administrators**] 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.

5.2.1.3 Restricted Audit Review (FAU_SAR.2)

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.

5.2.1.4 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply [**sorting**] of audit data based on [**date and time, subject identity, type of event, and success or failure of related event**].

5.2.1.5 Selective Audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to select the set of auditable events from the set of all auditable events based on the following attributes:

a) [***event type***]
b) [**no additional attributes**].

5.2.1.6 Guarantees of Audit Data Availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail 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***].

5.2.1.7 Prevention of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [**send an alarm**] if the audit trail is full**.**

5.2.2 User Data Protection (FDP)

5.2.2.1 Subset Information Flow Control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [**Traffic Management SFP**] on [

- **subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;**
- **information: traffic sent through the TOE from one subject to another;**
- **operation: pass information**].

5.2.2.2 Simple Security Attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**Traffic Management SFP**] based on the following types of subject and information security attributes: [

- **Subject security attributes: presumed IP address**
- **Information security attributes: protocol, source IP address, source port, destination IP address, destination port**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**if all the information security attribute values match the rules in a traffic filter, the TSF shall enforce the action configured for the filter, where the possible actions are:**

- **Block: traffic that triggers the filter is denied**
- **Allow: allows traffic that meets the filter criteria; this traffic is then subjected to IPS filtering**
- **Rate Limit: rate limits traffic that meets the filter criteria; this traffic is then subjected to IPS filtering**
- **Trust: allows traffic that meets the filter criteria through the TOE without being subjected to IPS filtering.**

Otherwise, the traffic is subjected to IPS filtering].

FDP_IFF.1.3 The TSF shall enforce the [**no additional rules**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**All the information security attribute values match an inspection bypass rule**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**none**].

Application Note: Note that the explicit authorization rule specified by FDP_IFF.1.4 is implemented only on the S6100N, S5100N, and S2500N models of the TOE.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 Authentication Failure Handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within [1..10]***] unsuccessful authentication attempts occur related to [**user login**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**perform the configured Failed Login Action, which can be one of the following:**

- **Lock the account for a configured Lockout Period**
- **Disable the account**
- **Generate an audit event documenting the failed login attempt**].

5.2.3.2 User Attribute Definition (FIA_ATD.1)

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]].

5.2.3.3 Verification of Secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**the following requirements:**

- **passwords must be at least 8 characters long**
- **passwords must contain at least two alphabetic characters**
- **passwords must contain at least one numeric character**
- **passwords must contain at least one non-alphanumeric character**].

5.2.3.4 Timing of Authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**network traffic filtering**] 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.

5.2.3.5 Timing of Identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**network traffic filtering**] 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.

5.2.4 Security Management (FMT)

5.2.4.1 Management of Security Functions Behavior (FMT_MOF.1)

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**].

5.2.4.2 Management of TSF Data (FMT_MTD.1)

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 (query only) 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, FMT_MTD.1 is included to satisfy a dependency of FAU_SEL.1. In order to properly satisfy this dependency, FMT_MTD.1 needs to address management of the collection of audit data.

5.2.4.3 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a.) **Management of user accounts**
b.) **Management of audit data and audit configurations**
c.) **Management of security configuration data**
d.) **Management of traffic management filters**
e.) **Management of inspection bypass rules (S6100N, S5100N and S2500N models only)**
f.) **Management of System data collection, analysis and reaction.**]

5.2.4.4 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the **following** roles [**authorized administrator, authorized System administrators, and [none]**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: The PP defined roles, as specified in FMT_SMR.1.1, are instantiated by the TOE-defined roles as follows: authorized administrator is instantiated by the Operator role; authorized System administrator is instantiated by the Administrator and Superuser roles.

5.2.5 Protection of the TOE Security Functions (FPT)

5.2.5.1 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.6 Trusted Path/Channels (FTP)

5.2.6.1 Trusted path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***disclosure, [undetected modification]***].

FTP_TRP.1.2 The TSF shall permit [***remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***initial user authentication, [all remote administrative actions]***].

5.2.7 IDS Component requirements (IDS)

5.2.7.1 Analyzer analysis (EXT) (IDS_ANL.1)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) [***statistical***, ***signature***]; and

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

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**]. (EXT)

5.2.7.2 Analyzer react (EXT) (IDS_RCT.1)

IDS_RCT.1.1 The System shall send an alarm to [**the System data log and the notification contacts configured for the filter triggered by the network traffic**] and take [**the action configured for the filter triggered by the network traffic, which can be to:**

- **Block the network traffic**
- **Permit the network traffic**

] when an intrusion is detected. (EXT)

Application Note: If traffic is permitted, an alert will be written to the System data log. If traffic is blocked, writing an alert to the System data log is configurable. In the evaluated configuration, action sets that block traffic must also be configured to generate an alert.

5.2.7.3 Restricted Data Review (EXT) (IDS_RDR.1)

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. (EXT)

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information. (EXT)

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. (EXT)

5.2.7.4 System Data Collection (EXT) (IDS_SDC.1)

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**]. (EXT)

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. (EXT)

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

Table 3: System Events

Application Note: The TOE can collect all network traffic on each configured network segment, for subsequent analysis as specified by IDS_ANL.1. However, the TOE will not collect for analysis any network traffic that has been Blocked or Trusted by the application of traffic management filters as specified in FDP_IFF.1, since traffic management filters are applied to network traffic before IPS filters. The TOE retains collected network traffic for as long as it requires to complete its analysis, after which the network traffic is allowed to pass through the TOE or is discarded, based on the action set associated with the triggered IPS filter (if any).

5.2.7.5 Guarantee of System Data Availability (EXT) (IDS_STG.1)

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion. (EXT)

IDS_STG.1.2 The System shall protect the stored System data from modification. (EXT)

PP Application Note: Authorized deletion of data is not considered a 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***]. (EXT)

5.2.7.6 Prevention of System data loss (EXT) (IDS_STG.2)

IDS_STG.2.1 The System shall [***overwrite the oldest stored System data***] and send an alarm if the storage capacity has been reached.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 3 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.3: Functional specification with complete summary
	ADV_TDS.2: Architectural design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.3: Authorisation controls
	ALC_CMS.3: Implementation representation CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model

Requirement Class	Requirement Component
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: basic design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 4: EAL 3 augmented with ALC_FLR.2 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

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

5.3.1.2 Functional specification with complete summary (ADV_FSP.3)

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Architectural design (ADV_TDS.2)

ADV_TDS.2.1D The developer shall provide the design of the TOE.

ADV_TDS.2.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.2.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.2.2C The design shall identify all subsystems of the TSF.

ADV_TDS.2.3C The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.

ADV_TDS.2.4C The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.5C The design shall summarise the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarise the behaviour of the SFR-supporting subsystems.

ADV_TDS.2.7C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

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

ADV_TDS.2.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance documents (AGD)

5.3.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance 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.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

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

5.3.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle support (ALC)

5.3.3.1 Authorisation controls (ALC_CMC.3)

ALC_CMC.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.1C The TOE shall be labelled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ALC_CMC.3.5C The CM documentation shall include a CM plan.

ALC_CMC.3.6C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMC.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Implementation representation CM coverage (ALC_CMS.3)

ALC_CMS.3.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.3.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.

ALC_CMS.3.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.3.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

5.3.3.4 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

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

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.3.3.5 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1D The developer shall document 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.2.1C 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 remediated and the remediation procedures 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.

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

5.3.3.6 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

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

5.3.4 Tests (ATE)

5.3.4.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

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

5.3.4.2 Testing: basic design (ATE_DPT.1)

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

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

5.3.4.3 Functional testing (ATE_FUN.1)

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

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

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

5.3.4.4 Independent testing - sample (ATE_IND.2)

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

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.

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 execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability assessment (AVA)

5.3.5.1 Vulnerability analysis (AVA_VAN.2)

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

AVA_VAN.2.1C The TOE shall be suitable for testing.

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

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions implemented by the TOE to satisfy the SFRs.

6.1 TOE Security Functions

The TOE implements the following security functions that together satisfy the SFRs claimed in Section 5.2 of this ST:

- Security Audit
- Identification and Authentication
- Intrusion Detection and Prevention
- Traffic Management
- Security Management
- TSF Protection
- Trusted Path.

6.1.1 Security Audit

The TOE generates two types of activity monitoring logs:

- Audit data logs
- System data logs (comprising the Block log and the Alert log).

System data logs record activity related to the TOE's intrusion detection and prevention capabilities. These logs differ from Audit data logs in their contents and controls. The System data logs are generated by the Intrusion Detection and Prevention security function (see Section 6.1.3).

The TOE provides the capability to generate and store audit records of auditable events. The TOE provides secure storage of audit records until they are automatically overwritten or cleared by an administrative user in the Superuser role. The TOE ensures that only the Superuser is able to view the audit data and that the audit data is presented in an interpretable manner. The TOE provides a means for the Superuser to determine what audit data the TOE generates, and the capability to sort the audit data that is being reviewed.

6.1.1.1 Audit Data Generation (FAU_GEN.1)

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

- Start-up and shutdown of the audit function
- Access to the System (i.e., to the TOE, by authorized users)
- Access to the TOE and System data (these records identify the IDS object and requested access)
- Reading of information from the audit records
- All modifications to the audit configuration that occur while the audit collection functions are operating
- Actions taken due to audit storage failure
- Reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent restoration to the normal state (these records include the user identity)
- Rejection by the TSF of any tested secret (these records include the user identity)
- All use of the authentication mechanisms (these records include the user identity and location of the attempt)

- All use of the user identification mechanisms (these records include the user identity and location of the attempt)
- All modifications in the behavior of the functions of the TSF
- All modifications to the values of TSF data
- Use of the management functions
- Modifications to the group of users that are part of a role (these records identify the user identity)
- All attempted uses of the trusted path functions (these records include the user identity).

The Security Audit security function 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.

Note that 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 and an "Audit facilities started" audit record is generated. Similarly, the audit functions are shutdown only when the TOE is shutdown. When this occurs, the TOE generates an "Audit facilities stopped" audit record.

6.1.1.2 Audit Review (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

The Security Audit security function provides mechanisms to view data from the Audit log. Only a user assigned the Superuser role can view events stored in the Audit log. This is done by restricting access using the file system service capabilities to protect the Audit log so that only authenticated Superusers can read audit data.

The Management Interface provides commands to configure how terminal sessions behave. The presentation format of data within the Management Interface can be defined. Data from the Audit log can be displayed in text format over the Management Interface. The default settings listed in **Table 5** can be modified to provide for the optimal viewing of data.

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>

Table 5: Default Console Settings

The Security Audit security function provides the ability to sort audit data. This capability is only provided by the LSM and is not available in the CLI. Sorting audit data is performed using the pointing device (e.g., mouse) to select the column to be sorted, based on the criteria shown in **Table 6**.

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

Criteria	Description
Interface [WEB,CLI, LSM, SNMP, OTHER]	Filters on the interface through which the user accessed the TOE
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

Table 6: Sorting Criteria

6.1.1.3 Audit Event Selection (FAU_SEL.1)

Audited events can be selected from the set of auditable events based on event categories (i.e., the event type). These event categories are listed in **Table 7**. A user in the Superuser role can use the CLI 'configure' command to select the event categories to be included in the set of auditable events. The 'configure' command allows the event category to be enabled or disabled, thus determining which auditable events are actually written to the Audit log.

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 System data logs.
login	This flag toggles the auditing of login events.
logout	This flag toggles the auditing of logout events.
compact-flash	This flag toggles the auditing of use of a compact-flash card with the TOE.
config	This flag toggles the auditing of configuration data. This includes changing the auditable events in the logs.
device	This flag toggles the auditing of device information.
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 stops.
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
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
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

Event Category	Description
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

Table 7: Auditable Event Categories

6.1.1.4 Audit Event Storage (FAU_STG.2, FAU_STG.4)

The TOE prevents unauthorized access (i.e., deletion, viewing and modification) to audit records by requiring users to be successfully identified and authenticated before gaining access to the TOE. The Security Audit security function ensures that when the audit storage becomes exhausted, that the oldest 50% of audit records are purged to ensure adequate disk space for the more recent auditable events.

The Security Audit security function 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 purge 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. All purge requests (successful and unsuccessful) are logged, allowing for detection of the deletion, or attempted deletion, of audit records.

Each of the logs maintained by the TOE (Audit, Block, Alert) comprises a "current" log file and a "historical" log file. Thus, there are six separate log files that provide the log storage—the current Audit, Block, and Alert log files, and the historical Audit, Block, and Alert log files. The TOE uses a volume threshold to limit the size of each log file (configured maximum size is 4 MB[3]). Entries for each type of log are initially written to the applicable current log file. When the current log file reaches the maximum file size, the log file is closed, a new log file is created, and an alarm is generated. This alarm comprises an email sent to a specified user, configurable by the Superuser role. The log file that is closed becomes the historical log file and the new file becomes the current log file. If a historical log file already exists, it is deleted. Subsequent log records are then written to the newly created current log file. This mechanism, which is applied to all types of log files (i.e., 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 displays all records from both files. Similarly, clearing the Audit log deletes both the current and historical files.

The deletion of the historical Audit log file when the current Audit log file becomes full effectively overwrites the oldest audit records. The TOE 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.

6.1.2 Identification and Authentication

The Identification and Authentication security function is implemented within the Management Interface subsystem of the TOE. The Identification and Authentication security function provides the capability for the TOE to identify and authenticate administrative users of the TOE.

6.1.2.1 User Identification and Authentication (FIA_UID.1, FIA_UAU.1)

The Identification and Authentication security function provides the capability to identify and authenticate the administrative users of the TOE. It prevents administrative user actions from being performed prior to identification and authentication of the user (all filtering of network traffic occurs without identification or authentication of users). In order to establish a connection with the TOE, the administrative user is required to submit user credentials, comprising user identity and authentication data (in the form of a password) through the Management Interface. The Identification and Authentication security function compares the submitted credentials with the details of user

[3] The TOE implements a capability to modify the configured maximum log file size, but this is intended only for HP TippingPoint QA and technical support staff.

accounts configured in the TOE. When a valid username/password pair is provided, the management functionality is available to the logged in user via the Management Interface.

6.1.2.2 Verification of Secrets (FIA_SOS.1)

The Identification and Authentication security function maintains a global configuration parameter, identified as 'Security Level', that determines the length and complexity requirements for all passwords on the TOE. The following options are provided:

- No Security Checking (Level 0)—passwords are not required
- Basic Security Checking (Level 1)—user names must be 6-32 characters long; passwords must be 8-32 characters long
- Maximum Security Checking (Level 2)—in addition to the Level 1 requirements, passwords must contain at least two alphabetic characters, at least one numeric character and one non-alphanumeric character (special characters such as '!', '?', or '#').

The Superuser or Administrator can configure the Security Level. The default security level is Level 2, which is the level that ensures passwords satisfy the strength requirements specified by FIA_SOS.1.

6.1.2.3 Authentication Failure Handling (FIA_AFL.1)

The Identification and Authentication security function is able to detect when the number of consecutive failed user login attempts meets an administrator-configured number (in the range 1..10, with 5 as the default value). When this occurs, the TOE takes the configured action. A user in the Superuser or Administrator role can configure the number of consecutive failed login attempts (Max Login Attempts) that will cause the Identification and Authentication security function to take action, and can also configure the action to be taken (Failed Login Action). The options for the Failed Login Action are as follows:

- Lockout Account—lock the user account for a configured Lockout Period
- Disable Account—disable the user account. The user will be unable to login until the account is enabled by a Superuser
- Generate an audit event and write an audit record to the Audit log documenting the failed login attempt.

The Superuser or Administrator can configure the Lockout Period, in minutes, for which the account will be locked if the Failed Login Action is Lockout Account. The Authentication Failure Handling mechanism applies to all user accounts.

6.1.2.4 User Attribute Definition (FIA_ATD.1)

The Identification and Authentication security function maintains the following security attributes associated with administrative users of the TOE:

- User identity—the user name the TOE uses to uniquely identify each administrative user
- Authentication data (password)—the credential used to authenticate the administrative user's identity
- Authorizations (roles)—the management role (Superuser, Administrator, Operator) to which the user has been assigned. The TOE documentation also identifies this attribute as 'Access Level'. Every administrative user must be assigned a management role.

The user security attributes maintained for administrative users are stored in the file system implemented by the TippingPoint Operating System and are managed through the Management Interface. The ability to manage the user attributes is restricted to the Superuser role (except that any user can modify their own password, regardless of their assigned role).

6.1.3 Intrusion Detection and Prevention

The Threat Suppression Engine (TSE) component implements the Intrusion Detection security function that provides the TOE with the sensing capabilities to collect network traffic, the analyzing capabilities to inspect

network traffic according to filter settings, and the reaction capabilities to generate alert records for certain network traffic, block certain network traffic and pass along certain network traffic.

6.1.3.1 System Data Collection, Analysis and Reaction (IDS_SDC.1, IDS_ANL.1, IDS_RCT.1)

The TOE collects network traffic and retains it for as long as it requires to complete its analysis, after which the network traffic is allowed to pass through the TOE or is discarded, based on the action set associated with the triggered IPS filter (if any).

The TOE performs statistical and signature-based analysis of the collected traffic, depending on configured IPS filters, as it enters the TOE. 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).

The TOE groups filters (i.e., signature-based rules combined with an action) into categories that the analyzer function uses in order to provide protection against malicious network traffic as it passes through the data network interface of the TOE. The categories provided by the TOE allow 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 filters cannot be changed. The categories defined by the TOE and the types of filter each contains are listed in **Table 8**.

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

Table 8: Filter Categories

Intrusion prevention capabilities such as traffic shaping are accomplished using traffic management filters (see Section 6.1.4) 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 sensor and analyzer capabilities, implemented in the TSE, work together to record relevant collected data, as 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—address and port
- Data destination—address and port
- Protocol
- Severity.

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 set associated with the matched filter.

An action set can specify the following possible actions:

- Block[4]—blocks a packet from being transferred to the outgoing port of the network segment
- Block + Notify—blocks a packet from being transferred, writes a record to the Block log, and notifies all selected contacts of the blocked packet
- Block + Notify + Trace—blocks a packet from being transferred, writes a record to the Block log, notifies all selected contacts of the blocked packet, and logs all information about the packet according to the packet trace settings
- Permit + Notify—permits a packet to be transferred to the outgoing port of the network segment, writes a record to the Alert log, and notifies all selected contacts of the packet
- Permit + Notify + Trace—permits a packet to be transferred, writes a record to the Alert log, notifies all selected contacts of the packet, and logs all information about the packet according to the packet trace settings.

The following types of notification contacts can be configured:

- Remote System Log—sends messages to a syslog server on the management network
- Management Console—sends messages to the LSM
- Email or SNMP—sends messages to the email address or specified SNMP server on the management network.

Each "Block" action can optionally specify that a TCP Reset occur, which results in the TOE resetting the TCP connection for the source or destination IP address when the Block action executes.

In addition to the Block and Permit action sets described above, the TOE supports Rate Limit and Quarantine action sets.

A Rate Limit action set defines a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth. For example, if filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps action set, then both "Echo Requests" and "Redirect Undefined Codes" filters share the 10 Mbps "pipe" as opposed to each filter getting a dedicated 10Mbps pipe. The supported rates are subject to restrictions based on the device model. Any of these listed rates can be used as long as it does not exceed 25% percent of the total bandwidth of the product.

A Quarantine action set allows the TOE to block or permit packets based on the IP addresses in the packet that triggers the filter. When a filter with a quarantine option is triggered, the TOE installs a block for the quarantined IP address and quarantines the IP address based on the instructions in the action set. If the quarantine action is combined with a Block action, the flow is blocked. The quarantine action can also be combined with a Permit action, in which case the flow is permitted while the IP address is placed in quarantine.

6.1.3.2 System Data Review (IDS_RDR.1)

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 Block and Alert logs once authenticated to the TOE.

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 be accessed either 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 log data is displayed in a manner suitable for the user to interpret the information.

[4] This option should not be used in the evaluated configuration, since alarms will not be written to the Block log or sent to configured notification contacts, meaning IDS_RCT.1 is not satisfied.

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 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 clear the System data logs.

6.1.3.3 System Data Storage (IDS_STG.1, IDS_STG.2)

The TOE 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.

As discussed in Section 6.1.1 in relation to the Audit logs, the TOE maintains a historical log file and a current log file for both the Block log and the Alert log. Whenever either current log file becomes full an alarm is sent.

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 is created takes the form of an email alarm that is sent to a specified user. The TOE also writes a new log record to the Alert log when new log files are created.

Notification contacts for alarms (syslog, email, SNMP, LSM) can be created in the Management Interface.

6.1.4 Traffic Management

In addition to IPS filtering described in Section 6.1.3, the TSE component provides traffic management filters that can be applied to traffic on selected segments, allowing the TOE to enforce an information flow control policy and operate as a firewall. Traffic management filters are managed within the context of a Traffic Management Profile that identifies the segment to which the Profile applies.

6.1.4.1 Information Flow Control Policy and Functions (FDP_IFC.1, FDP_IFF.1)

Traffic management filters are specified in terms of the following attributes of network packets:

- Source address and port—the source IP address and source port for traffic managed by the filter.
- Destination address and port—the destination IP address for traffic managed by the filter
- Protocol—specifies the protocol the filter checks for. It can have the following values: IP; ICMP; TCP; and UDP
- Action—defines how the TOE will handle traffic that triggers the filter. The possible actions are:
    - Block—traffic that satisfies the filter criteria is blocked
    - Allow—traffic that satisfies the filter criteria is allowed; such traffic is still subjected to IPS filtering
    - Rate Limit—traffic that meets the filter criteria is limited to a specified rate; such traffic is still subjected to IPS filtering
    - Trust—traffic that meets the filter criteria is passed through the TOE without IPS filtering.

IP addresses can be specified in Classless Inter Domain Routing (CIDR) format or as 'any'. Ports can be specified as a specific port number or as 'any'. A traffic management filter comprises a prioritized list of one or more rules specifying the values for the information attributes to be checked against and the action to take if a network packet matches all the values in the rule. When a traffic management filter is configured for a network segment, all traffic arriving at the TOE from that segment is compared against each rule in the filter, in priority order, until a match is found or all rules have been checked. A network packet that matches all of the criteria specified in a rule is handled based on the Action specified in the rule (Block, Allow, Rate Limit, or Trust). If a network packet does not trigger any of the rules specified in the traffic management filter, it is allowed to continue on but is subject to IPS filtering.

On the S6100N, S5100N and S2500N models, the Superuser and Administrator can configure inspection bypass rules, which can allow traffic to pass through the TOE without being subject to either traffic management or IPS filtering. Rules can be specified in terms of source address and port, destination address and port, and protocol.

Source and destination IP addresses can be specified in CIDR format. Inspection bypass rules can be specified for specific network segments and ports on the TOE appliance, or for all segments and ports.

The section titled "Traffic Management Profiles" in Chapter 4 of *TippingPoint Local Security Manager User's Guide* describes how to create and manage traffic management profiles and filters.

6.1.5 Security Management

6.1.5.1 Security Management Roles (FMT_SMR.1)

The TOE implements the following security roles:

- Superuser—has full access to the TOE. This role is able to manage the users of the TOE and to view and modify the configuration of the TOE and the logs
- Administrator—has full access to most functions of the TOE. This role is able to view and 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 and clearing the Audit log)
- Operator—has read-only access to the TOE. This role is able to view the System data logs (but not the Audit logs) and the configuration of the TOE, but is not permitted to modify any information other than his or her own password.

The TOE provides two interfaces by which administrative users can access and manage the TOE: the Local Security Manager (LSM), a web-based GUI; and a Command Line Interface (CLI). These interfaces together comprise the Management Interface component of the TOE.

A user account cannot be created without an associated role—if this is attempted, the action is denied and the Security Management security function 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.

The SFRs in the IDSSPP and this ST specify the following security roles that must, as a minimum, be maintained by the TOE: authorized System administrator; authorized administrator. The following table shows how the roles implemented by the TOE map to these specified roles.

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

Table 9: Mapping of TOE-implemented Roles to PP-defined Roles

6.1.5.2 Security Management Functions (FMT_SMF.1)

The Security Management security function provides the capability to manage: user accounts; audit data and audit configurations; security configuration data, such as password Security Level, Max Login Attempts, and Failed Login Action; traffic management filters; and System data collection analysis and reaction. The management capabilities are provided by the TippingPoint Operating System and are accessed through the Management Interface.

6.1.5.3 Management of Security Functions, Security Attributes, and TSF Data (FMT_MOF.1, FMT_MTD.1)

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 (equivalent to the authorized System administrator role defined in the IDSSPP). 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

(equivalent to the authorized administrator role defined in the IDSSPP) only have the ability to view the security policies that affect how the System data is analyzed, displayed, and reacted to.

The Security Management security function enforces the following restrictions on security 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 (including traffic management filters and inspection bypass rules)	Administrator or Superuser
Manage user accounts	Superuser
Select auditable events	Superuser
View and clear the Audit log and define users to receive alarm emails	Superuser

Table 10: Management Functions and Role Restrictions

The Management Interface controls access to the security functions provided by the TOE. 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.

6.1.6 TSF Protection

6.1.6.1 Reliable Time Stamps (FPT_STM.1)

The TOE maintains time internally using a CMOS clock and this internal time is used as the source for the timestamp recorded in each audit record and collected System data record.

6.1.7 Trusted Path

6.1.7.1 Trusted Path (FTP_TRP.1)

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

The TOE uses SSLimSecure 2.2.0 from TeamF1 for its SSL support. This library is based on OpenSSL 0.9.8b and was ported by TeamF1 to run under vxWorks. The TOE uses SSHield 2.2.0 from TeamF1 for its SSH support. This library is based on OpenSSH 3.5p1 and was ported by TeamF1 to run under vxWorks.

The TOE supports two modes of FIPS operation—crypto and full. When configured in either FIPS mode, the TOE will allow only FIPS 140-2 approved cryptographic algorithms to be used. When configured in 'full' FIPS mode, the following additional restrictions are enforced: http and telnet access cannot be enabled; only passwords that meet security level 1 or security level 2 are allowed; the debug shell cannot be enabled; restoring snapshots taken when the TOE was not in Full FIPS mode is not allowed; and restoring an older OS that is non FIPS-compliant is not allowed.

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

The TOE has a set list of supported algorithms and bit lengths for SSL. The client negotiates with the TOE to find a match that it also supports—this occurs without administrator intervention. Note that algorithms marked with a '+' are not available in FIPS mode:

- Symmetric:
    - AES (128-bit, 256-bit)
    - DES (56-bit)+
    - 3DES (168-bit)
    - RC2 (variable)+
    - RC4 (variable)+
- Asymmetric:
    - RSA
    - DSA.

The TOE has a set list of supported algorithms and bit lengths for SSH. The client negotiates with the TOE to find a match that it also supports—this occurs without administrator intervention. Note that algorithms marked with a '+' are not available in FIPS mode:

- 3DES (168-bit)
- Blowfish (variable)+
- AES (128-bit, 192-bit, 256-bit).

The TOE requires the client to provide the same capability in order to access the TOE via HTTPS or SSHv2.

7. Protection Profile Claims

The TOE conforms to the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007. In addition, HP Networking has chosen to pursue a more rigorous assurance level, as presented in Section 1.2, Conformance Claims.

Section 1.3 of the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007 states "…STs that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance…". This ST is a suitable solution to the generic security problem described in the PP. Following are the changes to the PP defined security problem definition, security objectives, and security requirements.

This Security Target includes all of the assumptions, threats, and organizational security policies specified in the security problem definition in the IDSSPP, without modification.

This Security Target includes all of the security objectives for the TOE and the TOE operational environment specified in the IDSSPP. Note, however, that PD-0097 removed O.EXPORT from the PP. Hence, it has not been included in this Security Target. The Security Target adds one TOE security objective (O.TRAFFIC) and one security objective for the operational environment (OE.CONFID). The rationale for these security objectives is provided in Section 8.1.

This Security Target includes the Security Functional Requirements from the IDSSPP, with tailoring as identified in **Table 11**.

PP Requirement	ST Tailoring
FAU_GEN.1	Changed the PP wording to be compliant with CC v3.1, Revision 2. Removed the auditable event for FAU_SAR.2 from Table 2. The TOE does not provide unauthorized users with an interface to attempt to read information from the audit records, so there is no auditable event for unsuccessful read attempts. In addition, auditable events associated with SFRs added to the ST but not specified in the PP have been included in Table 2, with the exception of FDP_IFF.1. This is in accordance with PD-0024, since the PP does not specify an objective that all security relevant events must be auditable at the basic level of auditing—the objectives and supporting rationale identify only "data accesses and the use of the System functions" (O.AUDITS), neither of which relate to the information flow capability specified by FDP_IFF.1.
FAU_SAR.1	*Assignment*—completed the assignment.
FAU_SAR.2	No changes.
FAU_SAR.3	Changed the PP wording to be compliant with CC v3.1, Revision 2.
FAU_SEL.1	Changed the PP wording to be compliant with CC v3.1, Revision 2.
FAU_STG.2	*Selection*—completed the selection. *Assignment*—completed the assignment. Changed the PP wording to be compliant with CC v3.1, Revision 2.
FAU_STG.4	*Selection*—completed the selection. *Assignment*—completed the assignment. In addition, the PP indicates this operation as a selection, when in fact the operation is an assignment. The ST author has indicated the correct operation performed.
FDP_IFC.1, FDP_IFF.1	*Added*—these requirements were added to the Security Target to specify security functionality provided by the TOE but not required by the PP. They specify the behavior of traffic management filters and inspection bypass rules implemented by the TOE that enable the TOE to operate as a firewall in addition to its primary function as an IPS device. Further rationale is provided in Section 8.2.

PP Requirement	ST Tailoring
FIA_AFL.1	*Added*—the PP specifies a refinement of this requirement to address external IT products. It was removed from the PP since the IDS System TOE does not require access from external IT products (see PD-0097). However, the TOE specified in this Security Target does satisfy the requirement as it is defined in CC Part 2, and so it is included in its original form. As such, it is associated with the Identification and Authentication security function and does not affect PP conformance. Further rationale is provided in Section 8.2.
FIA_ATD.1	*Assignment*—completed the assignment.
FIA_SOS.1	*Added*—this requirement was added to the Security Target to specify security functionality provided by the TOE but not required by the PP. It is associated with the Identification and Authentication security function and does not affect PP conformance. Further rationale is provided in Section 8.2.
FIA_UAU.1	*Assignment*—completed the assignment.
FIA_UID.1	*Assignment*—completed the assignment.
FMT_MOF.1	No changes.
FMT_MTD.1	*Assignment*—completed the assignment.
FMT_SMF.1	*Added*—this requirement was added to the Security Target to satisfy dependencies of FMT_MOF.1 and FMT_MTD.1. This requirement was originally included by International Interpretation RI#65 that was adopted in CC Part 2, v2.3 and is included in CC v3.1. This requirement specifies that security functions actually be present in addition to being protected if they are present, and therefore does not impact PP conformance. Further rationale is provided in Section 8.2.
FMT_SMR.1	*Assignment*—completed the assignment.
FPT_ITA.1, FPT_ITI.1, FPT_ITC.1	*Removed*—the TOE does not communicate with IDS System components outside the TOE, and therefore these requirements have been removed from the PP. Reference PD-0097. Since the TOE is not a distributed system, it is also not necessary to include FPT_ITT.1, as discussed in PD-0097.
FPT_STM.1	Changed the PP wording to be compliant with CC v3.1, Revision 2.
FTP_TRP.1	*Added*—this requirement was added to the Security Target to specify the capabilities provided by the TOE to support secure remote administration of the TOE using HTTPS to access the LSM and SSHv2 to access the CLI. In ensuring remote administrators are able to communicate with and manage the TOE securely, it contributes to the security objective that the TOE protects itself from unauthorized modifications and access to its functions and data (O.PROTCT). As such, it does not affect PP conformance. Further rationale is provided in Section 8.2.
IDS_ANL.1	*Selection*—completed the selection. *Assignment*—completed the assignment.
IDS_RCT.1	*Assignment*—completed the assignment.
IDS_RDR.1	*Assignment*—completed the assignment.
IDS_SDC.1	*Selection*—completed the selection. *Assignment*—completed the assignment.
IDS_STG.1	*Selection*—completed the selection *Assignment*—completed the assignment.
IDS_STG.2	*Selection*—completed the selection.

PP Requirement	ST Tailoring
EAL3	*Added*—the PP requires only EAL2, augmented with ALC_FLR.2. However, this Security Target has adopted the EAL3, augmented with ALC_FLR.2, security assurance requirements. Further rationale is provided in Section 8.3.

Table 11: Modification of Security Functional and Security Assurance Requirements

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification
- PP Claims.

8.1 Security Objectives Rationale

The U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments (IDSSPP) provides rationale for the security objectives demonstrating that security objectives are suitable to cover the intended environment. The rationale (provided in Sections 6.1 and 6.2 of the IDSSPP) is valid for the PP objectives reproduced in this ST and is not further discussed.

This ST includes an additional TOE security objective, O.TRAFFIC (The TOE must provide a capability to filter network traffic based on combinations of protocol, IP address and port). This additional objective contributes to satisfying P.ANALYZ, by applying analytical processes (traffic management filters) to derive conclusions about intrusions (invalid network addresses, ports or protocols) and taking appropriate actions in response (Block, Allow, Rate Limit, or Trust).

The ST includes an additional security objective for the operational environment, OE.CONFID (The IT Environment will provide the capability to protect the confidentiality of data communicated by the administrative users to the TOE). This additional objective contributes to satisfying P.PROTCT, by ensuring that communications between the administrative user and the TOE can be protected from disclosure, including user passwords submitted during the identification and authentication process.

8.2 Security Functional Requirements Rationale

Section 6.3 of the IDSSPP provides rationale for the security functional requirements, demonstrating that the security functional requirements are suitable to address the TOE security objectives. This rationale is valid for the PP requirements reproduced in the ST and is not further discussed.

This ST includes the following security functional requirements not included in the IDSSPP: FDP_IFC.1; FDP_IFF.1; FIA_AFL.1; FIA_SOS.1; FMT_SMF.1; and FTP_TRP.1. The following table maps these requirements to applicable TOE security objectives described in Section 4. Supporting rationale for these mappings is provided following the table.

	O.EADMIN	O.TRAFFIC	O.PROTCT	O.IDAUTH
FDP_IFC.1		X		
FDP_IFF.1		X		
FIA_AFL.1				X
FIA_SOS.1				X
FMT_SMF.1	X			
FTP_TRP.1			X	

Table 12: Objectives to Requirement Correspondence

8.2.1.1 O.EADMIN

The TOE must include a set of functions that allow effective management of its functions and data.

The following security functional requirements contribute to satisfying this security objective:

- FMT_SMF.1—the ST includes FMT_SMF.1 to specify the security management functions that are required to provide the capabilities for effective management of the TOE's functions and data

8.2.1.2 O.TRAFFIC

The TOE must provide a capability to filter network traffic based on combinations of protocol, IP address and port.

The following security functional requirements contribute to satisfying this security objective:

- FDP_IFC.1—the ST includes FDP_IFC.1 to specify the scope of control of the Traffic Management information flow control SFP. This SFP mediates the passing of traffic through the TOE between unauthenticated external IT entities. When activated on a network segment, it is applied to traffic before the IPS filtering capabilities and enables the TOE to behave as a firewall as well as an IPS device.
- FDP_IFF.1—the ST includes FDP_IFF.1 to specify the information flow functionality to be provided by the Traffic Management SFP. The TOE will act on traffic triggered by filters, based on the presumed source and destination addresses, ports and protocol of the traffic and will perform the specified filter action: Block; Allow; Rate Limit; or Trust.

8.2.1.3 O.PROTCT

The TOE must protect itself from unauthorized modifications and access to its functions and data.

The following security functional requirement contributes to satisfying this security objective:

- FTP_TRP.1—the ST includes FTP_TRP.1 to specify that the TOE will provide a trusted path for remote users to access the TOE that is able to protect TSF data from disclosure and undetected modification. The trusted path is invoked by the remote user and required for initial authentication and all remote administrative actions.

8.2.1.4 O.IDAUTH

The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

The following security functional requirement contributes to satisfying this security objective:

- FIA_AFL.1—the ST includes FIA_AFL.1 to specify that the TOE can detect when a configured number of consecutive unsuccessful attempts to authenticate have been made, and the TOE behavior when this occurs. This provides a means of protecting the identification and authentication function from a brute-force attack.

- FIA_SOS.1—the ST includes FIA_SOS.1 to specify minimum requirements for passwords chosen as user authentication data. This also contributes to protecting the identification and authentication function from direct attack by ensuring users cannot choose easily guessable passwords.

8.3 Security Assurance Requirements Rationale

The IDSSPP provides rationale for the security assurance requirements, demonstrating that they are sufficient given the statement of security environment and security objectives. The rationale is provided in Section 6.4 of the IDSSPP and is valid for this ST as no new security environment statements were added and the new security objectives are traced to existing OSPs.

This ST increases the assurance claim in the IDSSPP to EAL3 augmented with ALC_FLR.2. This entails the following changes to the set of assurance requirements specified in the PP: ADV_FSP.3 replaces ADV_FSP.2; ADV_TDS.2 replaces ADV_TDS.1; ALC_CMC.3 replaces ALC_CMC.2; ALC_CMS.3 replaces ALC_CMS.2; ALC_DVS.1 and ALC_LCD.1 are added; ATE_COV.2 replaces ATE_COV.1; and ATE_DPT.1 is added. The sponsor has chosen to increase the assurance claim due to the requirements of its customers, who are requesting EAL3 TOEs for their environments.

8.4 Requirement Dependency Rationale

The dependency requirements rationale is presented in Section 6.7 of the IDSSPP. The IDSSPP requirements have been evaluated and it has been determined that all dependencies have been satisfactorily addressed in the IDSSPP.

This ST includes the following security functional requirements not included in the IDSSPP: FDP_IFC.1; FDP_IFF.1; FIA_AFL.1; FIA_SOS.1; FMT_SMF.1; and FTP_TRP.1. The following table demonstrates how the dependencies of each of these additional SFRs are satisfied in the ST.

ST Requirement	CC Dependencies	ST Dependencies
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 and FMT_MTD.1 (see rationale below)
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_SOS.1	None	None
FMT_SMF.1	None	None
FPT_TRP.1	None	None

Table 13: Requirement Dependencies

CC Part 2 defines a dependency of FDP_IFF.1 (Simple security attributes) on FMT_MSA.3 (Static attribute initialization) to specify the nature of default values of security attributes used to enforce the SFP defined by FDP_IFF.1. However, the Traffic Management SFP defined by FDP_IFF.1 does not provide for default security attributes. The information security attributes are created outside the TOE boundary and the TOE has no control over whether they are restrictive, permissive, or some other quality. The TOE's ability to control information flow is defined by traffic management filters and their rules, specified in terms of information security attributes (i.e., protocol, source address, source port, destination address, and destination port). Restrictions on the management of these filters are specified by FMT_MTD.1, which therefore is shown to satisfy the dependency of FDP_IFF.1.

8.5 TOE Summary Specification Rationale

Section 6, the TOE Summary Specification, describes how the security functions of the TOE meet the claimed SFRs. The following table provides a mapping of the SFRs to the security function descriptions to support the TOE Summary Specification.

	Security Audit	Identification and Authentication	Intrusion Detection & Prevention	Traffic Management	Security Management	TSF Protection	Trusted Path
FAU_GEN.1	X						
FAU_SAR.1	X						
FAU_SAR.2	X						
FAU_SAR.3	X						
FAU_SEL.1	X						
FAU_STG.2	X						
FAU_STG.4	X						
FDP_IFC.1				X			
FDP_IFF.1				X			
FIA_AFL.1		X					
FIA_ATD.1		X					
FIA_SOS.1		X					
FIA_UAU.1		X					
FIA_UID.1		X					
FMT_MOF.1					X		
FMT_MTD.1					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
FPT_STM.1						X	
FTP_TRP.1							X
IDS_ANL.1			X				
IDS_RCT.1			X				
IDS_RDR.1			X				
IDS_SDC.1			X				
IDS_STG.1			X				
IDS_STG.2			X				

Table 14: Security Functions vs. Requirements Mapping

8.6 PP Claims Rationale

See Section 7, Protection Profile Claims.