TippingPoint Technologies, Inc.
UnityOne™ Version 1.2
Security Target

Document Version 2.3

August 14, 2003

Prepared for:

TippingPoint Technologies, Inc.
7501B North Capital of Texas Highway
Austin, Texas 78731
(512) 681-8000

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
(703) 267-6050

Table of Contents

List of Tables

List of Figures

1 Security Target Introduction

The Security Target (ST) introduction section presents introductory information on the Security Target, the Target of Evaluation (TOE) referenced in this Security Target, and a basic introduction to the TOE. It also contains document management information.

1.1 Security Target and TOE Identification

Table 1 – ST and TOE Identification

ST Title	TippingPoint Technologies, Inc. UnityOne™ Version 1.2 Security Target August 14, 2003
ST Version	2.3
Author	Corsec Security Inc.
TOE Identification	TippingPoint UnityOne™ Version 1.2
Common Criteria (CC) Identification	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999; Parts 2 and 3 Interpretations from the Interpreted CEM as of October 25, 2002, are included and interpretations used in this ST are as follows: • FAU_GEN.1-NIAP-0347 • FAU_STG.1-NIAP-0422 • FIA_AFL.1-NIAP-0425 • FMT_SMF.1-INTERP-065
PP Identification	Intrusion Detection System Analyzer Protection Profile, Version 1.1, December 10, 2001; Intrusion Detection System Scanner Protection Profile, Version 1.1, December 10, 2001; Intrusion Detection System Sensor Protection Profile, Version 1.1, December 10, 2001; and Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002.
Assurance Level	Evaluation Assurance Level (EAL) 2
Keywords	Intrusion Detection System (IDS), Vulnerability Assessor, Information Flow Control, Signature Analysis, Network Security, Security Target

1.2 Security Target Overview

It is important to note that this TOE is claiming conformance to four Protection Profiles in this Security Target. While the three IDS component PPs are very similar to one another as well as the IDS System PP, the four PPs are not identical. The System PP serves to incorporate most of the assumptions, objectives, threats, organizational policies, and security functional requirements that are present in the three component PPs. As such, the System PP is used as a baseline in this document. Any deviation between the System PP and any component PP is noted appropriately.

The Target of Evaluation is the TippingPoint Technologies, Inc. UnityOne™ version 1.2 (referred to as either "the TOE", the "TippingPoint UnityOne™", or the "UnityOne™"), a network-based intrusion prevention system (IPS). Networks and the hosts connected to them are potential points of attack by an adversary. The services running on a host or even the network itself may be subject to assault using a variety of known vulnerabilities. The UnityOne™ v1.2 is meant to provide a defense against network-based attacks on hosts and networks.

The network-based intrusion prevention system is used to monitor a network for potentially malicious and anomalous traffic. This system identifies such traffic through rules and algorithms designed to distinguish normal data flows from suspect ones. The UnityOne™ is also used to identify and scan hosts on a network for information gathering purposes in an attempt to identify potentially vulnerable hosts.

The Local Security Manager (LSM) agent interlinks TOE capabilities in a Web-based configuration and management console. The LSM agent handles internal communication between the TOE's components and external communication between the TOE's components and the remote management console (either a web browser or a separate appliance).

This ST describes the requirements for the TippingPoint UnityOne™ v1.2 and specifies how the TOE meets those requirements. This specific ST is based on four Intrusion Detection System Protection Profiles issued by the National Security Agency (NSA). Because conformance to all four IDS Protection Profiles is claimed, the reader will see references throughout this document made to the TOE, the System, the Analyzer, the Scanner, and the Sensor. IDS component (i.e. Analyzer, Scanner, and Sensor) functionality is specifically addressed in order to meet the requirements outlined in the IDS component PPs. "Multiple conformance notes" are used to provide additional clarity so that the reader may fully understand the similarities and differences between the IDS System and IDS component PP requirements as well as how the UnityOne™ does indeed meet the requirements of all four IDS Protection Profiles.

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the UnityOne™ v1.2 product meets in order to mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- TOE Security Environment (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its supporting environment.
- IT Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) met by the TOE.
- Assurance Requirements (Section 6) – Presents the Security Assurance Requirements (SARs) met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 8) – Presents the rationale concerning compliance of the ST with any claims of Protection Profile (PP) conformance.
- ST Rationale (Section 9) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

1.3 Common Criteria (CC) Conformance Claims

The Assurance and other Common Criteria-required documentation, specifically this ST, conform to the Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (aligned with ISO 15408).

The TippingPoint Unity One v1.2 conforms to four protection profiles:

1. Intrusion Detection System Analyzer Protection Profile, Version 1.1, December 10, 2001;
2. Intrusion Detection System Scanner Protection Profile, Version 1.1, December 10, 2001;
3. Intrusion Detection System Sensor Protection Profile, Version 1.1, December 10, 2001; and
4. Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002.

This ST claims conformance to CC Version 2.1 Part 2 extended.

This ST claims conformance to CC Version 2.1 Part 3.

Interpretations from the Interpreted CEM as of October 25, 2002, are included and interpretations used in this ST are as follows:

- FAU_GEN.1-NIAP-0347
- FAU_STG.1-NIAP-0422
- FIA_AFL.1-NIAP-0425
- FMT_SMF.1-INTERP-065

1.4 Conventions and Terminology

1.4.1 Conventions

There are several font variations within this ST. The conventions used in this ST are consistent with those used in the four Protection Profiles to which the TOE claims conformance. Selected presentation choices are discussed here to aid the Protection Profile user.

The CC allows several operations to be performed on security requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this ST.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by underlined text.

The **iteration** operation is used when a component is repeated with varying operations. Iterations are noted by the text "iteration #", followed by a numeral, in parenthesis following the requirement.

1.4.2 Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following are a subset of those definitions. They are listed here to aid the user of the ST.

User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Human user – Any person who interacts with the TOE.

External IT entity – Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Role – A predefined set of rules establishing the allowed interactions between a user and the TOE.

Identity – A representation (e.g., a string) uniquely identifying an authorized user, which can be either the full or abbreviated name of that user or a pseudonym.

Authentication data – Information used to verify the claimed identity of a user.

From the above definitions given by the Common Criteria, the following terms can be derived:

Authorized external IT entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized Administrator – A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Additional terms and abbreviations are used throughout the body of this ST. They are listed in Section 10: Glossary of Terms to aid the user of the ST.

2 TOE Description

The TOE description provides context for the evaluation. It describes the TOE as an aid to understanding the security requirements for the TOE.

2.1 UnityOne™ v1.2 Architecture

The UnityOne™ v1.2 is functionally a combination of an IPS, firewall and network discovery functionality (although, for the purposes of this evaluation, the firewall capabilities of the UnityOne™ are not being evaluated). The purpose of the TOE is to defend against network-based attacks by identifying and blocking these attacks.

The UnityOne™ v1.2 is composed of four main elements:

- **Intrusion Prevention System (IPS)**[1] – performs the intrusion prevention functionality of the TOE;
- **Firewall** – performs the traffic filtering functionality of the TOE (but not part of this evaluation);
- **Network Discovery (ND)** – performs the reconnaissance-gathering functionality of the TOE; and
- **Local Security Manager (LSM) Agent** – coordinates communication between the other components of the TOE and is responsible for local administration, configuration, and reporting.

The **intrusion prevention system (IPS)** component of the TOE monitors network data flows for inappropriate, incorrect, or anomalous activity. It uses two detection techniques: static signatures and anomaly algorithms. Signatures are used to detect indications of known attacks. Anomaly algorithms detect types of attacks rather than known implementations of the attack. The IPS also compensates for various techniques used to bypass an IPS, such as TCP packet fragmentation.

The **firewall** component of the UnityOne™ is a stateful, full-packet inspection firewall but this functionality is not part of the evaluated configuration of the TOE. The firewall permits and blocks traffic based on a rule set. When used in combination with the IPS component, the firewall will be configured dynamically by the IPS in response to attacks. Note, however, that this functionality is outside the scope of this evaluation.

The **network discovery (ND)** component of the TOE is used to collect information on a network, including detecting active hosts, the services running on those hosts, and identifying the hosts' operating systems. This is essentially an IDS Scanner. The IPS can be dynamically configured based on the findings of the ND.

The IPS and ND interact with each other through a central component, the Local Security Manager (LSM) agent. The two components report their findings to the LSM agent and the LSM agent is able to react upon these findings as configured. The LSM agent will pass this information along to the LSM console, through which the authorized administrator is able to monitor everything that is happening in real time. If configured to automatically react to new information (such as attacks or a newly detected host), the LSM agent is able to modify the IPS rules based on the newly gathered information.

[1] Please note that TippingPoint Technologies, Inc. uses the term "IPS" (intrusion prevention system) to describe its products, specifically the model 2000. That usage is distinct from the usage here, describing an architectural component of the TOE. **All** further occurrences of "IPS" should be read as a reference to the model 2000 product and not to an architectural component of the TOE unless otherwise noted.

Using the centralized LSM console, an authorized administrator is able to monitor the components of the TOE and their findings. Additionally, an authorized administrator can configure the TOE through the centralized console.

2.2 Physical Scope and Boundaries

***MULTIPLE CONFORMANCE NOTE**: The physical TOE boundary described below applies for evaluation against each and all of the four IDS PPs.*

The TippingPoint UnityOne™ v1.2 software can reside in one of four hardware models. The security functions performed are the same across all four models; the differences between models are hardware-related and result in four different levels of scalability and throughput. Three of these models are identified as appliances and one is identified as a system. These models are identified as follows:

- UnityOne™-400 Appliance (intrusion prevention performed at 400 Megabits per second);
- UnityOne™-1200 Appliance (intrusion prevention performed at 1.2 Gigabits per second);
- UnityOne™-2400 Appliance (intrusion prevention performed at 2.4 Gigabits per second); and
- UnityOne™-2000 System (intrusion prevention performed at 2.0 Gigabits per second).

The physical interfaces are functionally identical across all of the models. The 400/1200/2400 appliance models have a fixed set of 4 data segments (contiguous port pairs on the Multi-Zone Defense Module, which is further described below). The 2000 system model has a variable ("bladed") set of 5 data segments per blade with a capacity of up to 4 blades, allowing 20 data segments. The blades on the UnityOne™ 2000 provide a user with a field replacement capability; but there is no other particular function that they provide and the blades do not affect or differentiate the security functions of the UnityOne™ v1.2 in any way.

A firmware switch controls the speed at which a particular appliance model will operate. This "switch" is a parameter in the hardware that controls the maximum output rate of the (aggregate) data layer. At boot-up, the software references internal information to determine which model it is and sets the parameter accordingly (e.g., to 400Mbps if it is a Model 400).

The software build on all four UnityOne™ models is identical – the build for each of the four models is built from the same source code tree. The underlying OS has been modified to accommodate the different hardware platforms for the UnityOne™ platform models. Different device drivers (which are subcomponents of the OS) corresponding to the different hardware platforms of the four UnityOne™ models. The UnityOne™ OS kernel has a different "board support package" for each model, and the different drivers are used to address the differences between using fixed segments and blades in the UnityOne™ chassis.

The TOE's hardware components for the UnityOne™-400, -1200, and -2400 appliances comprise a two rack unit (RU) chassis which acts as the physical boundary for the UnityOne™ v1.2 when operated from an appliance chassis. Each model is rack-mountable on a 19- or 23-inch rack and contains a power supply and fans.

Figure 1 – UnityOne™-400, UnityOne™-1200 and UnityOne™-2400 Intrusion Prevention Appliances (IPAs)

The TOE's hardware components for the UnityOne™-2000 comprise a four rack unit (RU) chassis that uses a front-access, eight-slot multi-port architecture. This 4RU chassis is the physical boundary of the UnityOne™ v1.2 (2000 model), and it contains all components of the TOE. It is rack-mountable on a 19- or 23-inch rack and contains redundant power supplies and fans.

At a minimum, the TOE (IPA/IPS) is equipped with the following components:

- One Management Processor (MP)
- One Threat Suppression Engine (TSE)
- One Multi-Zone Defense Module (MZDM)
- One power supply module
- One Power Entry Module (PEM)

Figure 2 – UnityOne™-2000 Intrusion Prevention System (IPS)

The **Management Processor** is the central processing and control system for the UnityOne™ v1.2. The LSM agent is executed on the MP, and the MP also contains all software required to perform the following tasks:

- Control
- Configuration
- Management
- Performance monitoring
- Status
- Alarm reporting

The MP is an x86 card that supports a standard Compact-PCI bus, running 32 bits at 33 MHz. It runs at 700 MHz with 256 MB of DRAM and hard drive capacity of 30 GB. Acting as a simple Level 2 switch, it supports a PCI interface and two 10/100 Ethernet ports for configuration purposes and can aggregate and redirect traffic to and from the Threat Suppression Engine (TSE).

The core of the UnityOne™ v1.2 is the **Threat Suppression Engine**. The TSE provides full threat detection and suppression. The IPS[2] and ND components of the TOE are all executed on the TSE. The TSE supports a standard Compact-PCI bus with cPCI and Z-pack (GHz frequency) connectors.

The Threat Suppression Engine:

- Performs deep packet inspection on data it receives from MZDM module and redirects it as necessary
- Processes up to OC-48 of traffic.

The **Multi-Zone Defense Module (MZDM)** is a 6U interface card that supports up to 10 Gigabit Ethernet ports over copper or fiber. Untrusted traffic from a Local Area Network (LAN) or Wide Area Network (WAN) flows to the MZDM module where it is directed to the TSE for traffic assessment. If the TSE determines that the traffic will not harm the network, it passes the data back to the MZDM module and out on the LAN or WAN.

[2] In this instance, the term "IPS" refers to an architectural component of the TOE and not the model 2000 product.

2.3 Logical Scope and Boundary

The logical boundary of the TOE encompasses all of the components that reside within the physical boundary of the TOE. Note that this boundary remains the same when considering the TOE against the requirements of any and all of the four IDS Protection Profiles. The six logical components of distinction are the Network Discovery, the IPS[3], the Local Security Manager (LSM), the Command Line Interface (CLI), the UnityOne™ OS (operating system), and the UnityOne™ hardware.

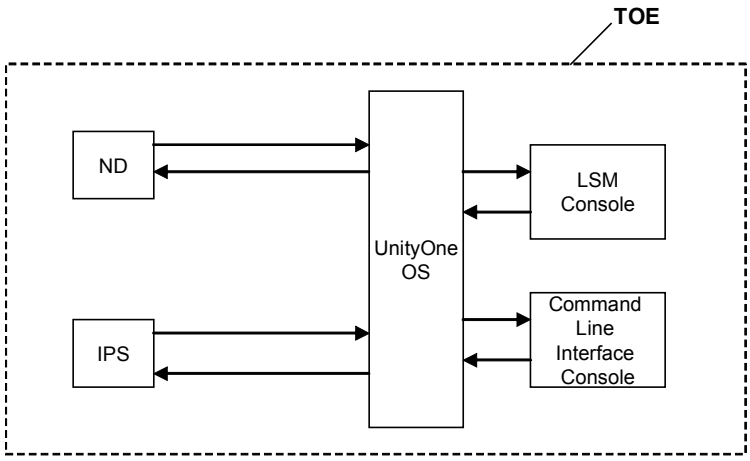


Figure 3 – TOE Boundary and Logical Interaction between UnityOne™ Components

The **UnityOne™ operating system**, based on a third-party embedded real-time operating system, provides the basic execution environment for the UnityOne™ product software. The UnityOne™ application relies on the following services the OS provides:

- Boot processing and system initialization;
- File system services;
- Process scheduling services;
- POSIX library implementation;
- Network and other hardware device drivers; and
- Network (TCP/IP, HTTPS) protocol implementations.

The TOE resides on a network as depicted in Figure 4 below. Traffic flows through the TOE between internal and external networks where it is analyzed and filtered. **Note that, while the SMS and the Threat Management Center (TMC) are depicted in the figure below, they are not a part of this evaluation and should be disregarded. Two Instances of the TOE are depicted inside dashed-line boxes.**

[3] In this instance and in the Figure 3 below, the term "IPS" refers to an architectural component of the TOE and not the model 2000 product.

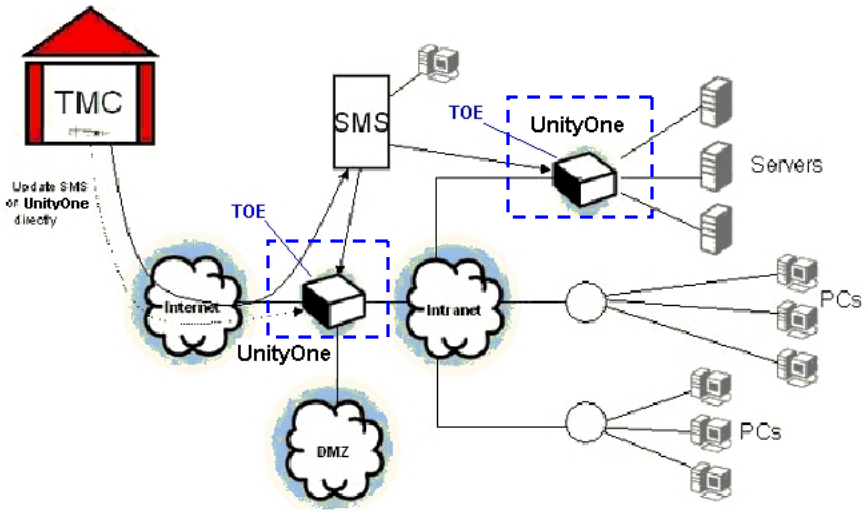


Figure 4 – Deployment of the UnityOne™ in a Network

The system that the TOE monitors is composed of the TOE, the hosts that the TOE is configured to protect and all of the traffic flowing through the TOE.

Management of the TOE occurs through shell access over a single serial port or Ethernet using Secure Shell v2.0 (SSH), and via a Microsoft Internet Explorer v5.0 (or greater) web browser using Secure Sockets Layer (SSL).

3 TOE Security Environment

This section describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

MULTIPLE CONFORMANCE NOTE: *This security environment remains the same for evaluation against each and all of the four IDS PPs except where deviation or refinement is specifically noted in the subsections below.*

To ensure that all assumptions, threats, and policies in this Security Target address all four IDS Protection Profiles, assumptions, threats, and policies have been modified where necessary. If an assumption, threat, or policy has been modified, the following format is used. The first assumption, threat, or policy has been taken directly from the IDS System PP. These statements will be identified with an asterisk (e.g. A.ACCESS*). The assumption, threat, or policy immediately following has been modified to incorporate all of the information contained for that respective assumption, threat, or policy in all of the four IDS PPs. A rationale for the change immediately follows the modified assumption, threat, or policy.

Not every assumption, threat, or policy is present in each of the four IDS PPs, however, and this is also noted (where applicable) immediately following the respective assumption, threat, or policy.

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 function*s*.

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

The Analyzer PP refers to 'resources' as opposed to 'data', so this modified assumption statement includes both.

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

This assumption refers to only the IDS Scanner and IDS System PPs.

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

This assumption refers to only the IDS System and IDS Scanner PPs.

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

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.

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

The IDS Analyzer, IDS Scanner and IDS Sensor PPs include this threat but the wording differs slightly. The Analyzer PP threat refers to a 'person' rather than a 'user' as well as data 'analyzed' as opposed to 'collected'. The Scanner and Sensor PP threats limit data to data collected, not produced, by the TOE. This new statement incorporates all of the T.COMINT TOE threats from the four IDS PPs.

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

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

The IDS Analyzer, IDS Scanner and IDS Sensor PPs include this threat but the wording differs slightly. The Analyzer PP refers to a 'person' rather than a user, and the data that is the subject of this threat is the data analyzed as opposed to the data collected by the TOE. The Scanner and Sensor PP threats limit data to data collected, not produced, by the TOE. This new statement incorporates all of the T.COMDIS TOE threats from the four IDS PPs.

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

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

The IDS Analyzer, IDS Scanner and IDS Sensor PPs include this threat but the wording differs slightly. The IDS Analyzer PP refers to a 'person' rather than a 'user' as well as data analyzed as opposed to data collected. The IDS Scanner and Sensor PPs limit the threat to data collected, not produced by the TOE. This new statement incorporates all of the T.LOSSOF TOE threats from the four IDS PPs.

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

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

The IDS Analyzer, IDS Scanner and IDS Sensor PPs include this threat but the wording differs slightly. The IDS Analyzer PP refers to a 'person' rather than a 'user'. The IDS Analyzer PP also refers to the TOE's analysis functionality rather than the System's and limits this functionality to analysis (collection functionality is omitted). The IDS Scanner and IDS Sensor PPs refer to the Scanner's and Sensor's functionality, respectively, as opposed to the System. Analysis functionality is omitted from the threat in both of these PPs (i.e. functionality is limited to collection). This new statement incorporates all of the T.NOHALT TOE threats from the four IDS PPs.

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

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE, making the TOE susceptible to improper configuration by an authorized or unauthorized person, causing potential intrusions to go undetected.

From the IDS System and IDS Scanner PPs.

The IDS Analyzer and IDS Sensor PPs include this threat but the wording differs slightly. The Analyzer and Sensor PPs includes this threat as follows:

> *"The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected." The modified threat incorporates the T.IMPCON threats from all of the four IDS PPs.*

3.2.2 IT System/Analytical Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources. Note that these threats are referred to as 'Analytical Threats' in the IDS Analyzer PP while they are referred to as 'System Threats' in the IDS Scanner, IDS Sensor, and IDS System PPs.

The following three threats are present in the IDS System and IDS Analyzer PPs:

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.

The following three threats are present in the IDS System and IDS Scanner PPs:

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.

The following three threats are present in the IDS System and IDS Sensor PPs (note that the threats in the IDS Sensor PP do not specify the IT System to be one that "the TOE monitors").

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 Organization 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 IDS family of Protection Profiles.

3.3.1 OSPs

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

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

Note that the P.Manage OSP is slightly modified in the IDS Sensor PP; the text in this PP reads that the TOE shall "be manageable only…" as opposed "only be managed…". The intent of the OSP is not affected by this wording change.

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.

The IDS Scanner PP includes an abbreviated version of this threat that is worded as follows:

> *"Status configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System must be collected."*

The IDS Sensor PP includes an abbreviated version of this threat that is worded

as follows:

> *"All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected."*

The IDS Analyzer PP does not include this OSP.

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.

This OSP is only included in the IDS Analyzer and IDS System PPs.

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

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

The IDS Analyzer, IDS Scanner and IDS System PPs include this OSP but the wording differs slightly from the OSP above. The Analyzer PP refers to data that is 'analyzed and generated' rather than 'collected and produced'. The Scanner and Sensor PPs restrict the OSP to data collected by the TOE, as opposed to collected and produced by the TOE. This new OSP incorporates all of the component OSPs.

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

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

The IDS Analyzer, IDS Scanner and IDS System PPs include this OSP but the working differs slightly from the OSP above. The Analyzer PP refers to the data that is 'analyzed and generated' rather than 'collected and produced'. The Scanner and Sensor PPs restrict the OSP to data collected by the TOE, as opposed to collected and produced by the TOE. This new OSP incorporates all of the component OSPs.

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

P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of the following: analysis and response activities, collection activities, and TOE data and functions.

The IDS Analyzer, IDS Scanner and IDS System PPs include this OSP but the wording differs slightly from the OSP above (taken from the IDS System PP). The Analyzer PP refers to disruptions of 'analysis and response activities' and the Scanner and Sensor PPs refer to 'collection activities' as opposed to 'TOE data and functions'. This new OSP incorporates all of the component OSPs.

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.

To ensure that all security objectives in this Security Target address all four IDS Protection Profiles, security objectives have been modified where necessary. If a security objective has been modified, the following format is used. The first security objective will be taken directly from the IDS System PP. This statement will be identified with an asterisk (e.g. O.FLOWS*). The security objective immediately following will be modified to incorporate all of the information contained for that respective security objective in all of the four IDS PPs. A rationale for the change immediately follows the security objective.

Not every security objective is present in each of the four IDS PPs, however, and this is also noted (where applicable) immediately following the respective security objective.

4.1 Information Technology (IT) Security Objectives

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

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.RESPON The TOE must respond appropriately to analytical conclusions.

This objective is present only in the IDS Analyzer and IDS System PPs.

O.IDSCAN &

O.IDACTS 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.

The O.IDSCAN objective is present only in the IDS Scanner and IDS System PPs. Note, however, that this same objective is instead named "O.IDACTS" and included in the IDS Scanner PP.

O.IDSENS &

O.IDACTS 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.

The O.IDSENS objective is present only in the IDS System PP. Note, however, that the O.IDSENS objective is renamed O.IDACTS and included in the IDS Sensor PP.

O.IDANLZ &

O.IDACTS 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).

The O.IDANLZ objective is present only in the IDS System PP. Note, however, that this same objective is renamed O.IDACTS and included in the IDS Analyzer PP.

O.OFLOWS* The TOE must appropriately handle potential audit and System data storage overflow*s*.

O.OFLOWS The TOE must appropriately handle potential audit and Analyzer, Scanner, Sensor, and System data storage overflows.

This objective is included in all four IDS PPs. The Analyzer, Scanner, and Sensor PPs do not refer to 'System data' in the objective, however, but rather Analyzer, Scanner and Sensor data, respectively. This new OSP incorporates all of the OSPs from the component PPs.

O.AUDITS* The TOE must record audit records for data accesses and use of the System functions.

O.AUDITS The TOE must record audit records for data accesses and use of the Analyzer, Scanner, Sensor, and System functions.

This objective is included in all four IDS PPs. The Analyzer, Scanner, and Sensor PPs do not refer to 'System functions' in the objective, however, but rather Analyzer, Scanner and Sensor functions, respectively. This new OSP incorporates all of the OSPs from the component PPs.

O.INTEGR* The TOE must ensure the integrity of all audit and System data.

O.INTEGR The TOE must ensure the integrity of all audit and Analyzer, Scanner, Sensor, and System data.

This objective is included in all four IDS PPs. The Analyzer, Scanner, and Sensor PPs do not refer to 'System data' in the objective, however, but rather Analyzer, Scanner and Sensor data, respectively. This new OSP incorporates all of the OSPs from the component PPs.

O.EXPORT* When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.

O.EXPORT When any IDS component or the TOE makes its data available to another IDS component, the TOE will ensure the confidentiality of the Analyzer, Scanner, Sensor, and System data.

This objective is included in all four IDS PPs although the wording differs slightly between the System PPs and the three component PPs. All three component PPs begin with "When the TOE…" rather than "When any IDS component…". Each of the three component PPs also refer to their own data, respectively, as opposed to 'System data'. This new OSP incorporates all of the OSPs from the component PPs.

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

O.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.

O. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.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.

O.PERSON* Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Analyzer, Scanner, Sensor, and System.

This objective is included in all four PPs, but the wording differs slightly between the IDS System PP and the three IDS component PPs. Each component PP refers to the "proper operation of the [component]", respectively, rather than the "proper operation of the System". This objective has been modified to incorporate all of the objectives stated in each of the component PPs.

O.INTROP* The TOE is interoperable with the IT System it monitors.

O.INTROP The TOE is interoperable with the IT System it monitors and other IDS components within the IDS.

This objective is included in all four IDS PPs, but it has been augmented in each of the three IDS component PPs to read as follows:

> *"The TOE is interoperable with the IT system it monitors and other IDS components within the IDS."*

This new OSP incorporates the components' augmented OSPs.

5 IT Security Requirements

This section defines the functional requirements for the TOE. Functional requirements in this ST were drawn from Part 2 Extended of the CC. These requirements are relevant to supporting the secure operation of the TOE. This Security Target also responds to explicitly stated requirements that are present in the four IDS PPs. These new requirements are indicated in bold text and contain the text (EXP) in the title.

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

Table 2 – Functional Requirements for the TOE Mapped to ST Operations

Functional Component	Description	ST Operation
FAU_GEN.1	Audit data generation	Refinement
FAU_SAR.1	Audit review	Assignment and iteration
FAU_SAR.2	Restricted audit review	None
FAU_SAR.3	Selectable audit review	None
FAU_SEL.1	Selective audit	Assignment
FAU_STG.2	Guarantees of audit data availability	Assignment and selection
FAU_STG.4	Prevention of audit data loss	Selection
FIA_UAU.1	Timing of authentication	Assignment
FIA_AFL.1	Authentication failure handling	Refinement
FIA_ATD.1	User attribute definition	Assignment
FIA_UID.1	Timing of identification	Assignment
FMT_MOF.1	Management of security functions behavior	Refinement
FMT_MTD.1	Management of TSF data	Assignment and refinement
FMT_SMF.1	Specification of management functions	Assignment
FMT_SMR.1	Security roles	Assignment and refinement
FPT_ITA.1	Inter-TSF availability within a defined availability metric	Assignment and refinement
FPT_ITC.1	Inter-TSF confidentiality during transmission	None
FPT_ITI.1	Inter-TSF detection of modification	Assignment
FPT_RVM.1	Non-bypassability of the TSP	None
FPT_SEP.1	TSF domain separation	None
FPT_STM.1	Reliable time stamps	None
IDS_SDC.1 IDS_SCN.1 IDS_COL.1	System Data Collection Scanner Data Collection Sensor Data Collection	Assignment and selection
IDS_ANL.1	Analyzer analysis	Assignment, selection and refinement
IDS_RCT.1	Analyzer react	Assignment and refinement
IDS_RDR.1	Restricted Data Review	Assignment and refinement
IDS_STG.1	Guarantee of TOE Data Availability	Assignment, Selection and refinement
IDS_STG.2	Prevention of TOE Data Loss	Selection and refinement

The following sections present the IT Security Functional Requirements (SFRs) with any ST operations performed on them based on the requirements from the four PPs to which the TOE claims conformance.

SECURITY AUDIT (FAU)

5.1.1.1.1 FAU_GEN.1-NIAP-0347 Audit data generation

MULTIPLE CONFORMANCE NOTE: Each of the 4 IDS PPs call out for the ability to access the Analyzer, Scanner, Sensor and System as well as Analyzer, Scanner, Sensor and System data, respectively. This requirement has been refined to call out the ability to access the TOE and TOE data. The means by which audit events are generated is identical whether the TOE is configured as an Analyzer, Scanner, Sensor, or System. This modified requirement is applicable to this TOE claiming compliance against all 4 IDS PPs because the TSF that is maintaining the TOE and TOE audit functions does not change among the PPs.

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 *TOE* and access to the *TOE* data.

Table 3 – Auditable Events

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to TOE	
FAU_GEN.1	Access to the TOE data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FAU_STG.4	Actions taken due to storage failure	
FIA_UAU. 1	All use of the authentication mechanism	User identity, location, method
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	User identity, location, method
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_ITI.1	The action taken upon detection of modification of transmitted TSF data	

FAU_GEN.1.2-NIAP-0347 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 3 – Auditable Events**[4].

MULTIPLE CONFORMANCE NOTE: This requirement is also present in each of the three IDS component PPs. In the Analyzer, Scanner and Sensor PPs, all System references in FAU_GEN.1.1 above are referenced as Analyzer, Scanner and Sensor, respectively.

5.1.1.1.2 FAU_SAR.1 Audit review (iteration #1)

FAU_SAR.1.1 The TSF shall provide [superusers] with the capability to read [all audit information in Table 3] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.1.3 FAU_SAR.1 Audit review (iteration #2)

FAU_SAR.1.1 The TSF shall provide [administrators and operators] with the capability to read [Actions taken due to storage failure] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.1.4 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.1.5 FAU_SAR.3 Selectable audit review

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

5.1.1.1.6 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

[4] Table 3 – Auditable Events – in this ST relates to Table 2 in the IDS System PP to which this ST claims conformance.

a) event type;

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

5.1.1.1.7 FAU_STG.2-NIAP-0422 Guarantees of audit data availability

FAU_STG.2.1-NIAP-0422 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2-NIAP-0422 The TSF shall be able to detect unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [all audit events contained in an audit or system log prior to audit storage exhaustion minus the oldest record(s) that may have been overwritten to accommodate new audit records generated to note audit storage exhaustion or attack of that log] audit records will be maintained when the following conditions occur: audit storage exhaustion, attack.

5.1.1.1.8 FAU_STG.4 Prevention of audit data loss

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

IDENTIFICATION AND AUTHENTICATION (FIA)

5.1.1.2.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [SSL/TLS and SSH session establishment[5]] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.2.2 FIA_AFL.1-NIAP-0425 Authentication failure handling

FIA_AFL.1.1-NIAP-0425 The TSF shall detect when an authorized administrator-configurable **positive** integer of unsuccessful authentication attempts occur related to **external IT products attempting to authenticate**.

FIA_AFL.1.2-NIAP-0425 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **prevent the offending external IT product from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT product in question**.

[5] Please note that the evaluation laboratory did not evaluate the cryptography related to these session establishments.

5.1.1.2.3 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity;

b) Authentication data;

c) Authorizations; and

d) [Password expiration information and lockout parameters].

5.1.1.2.4 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [SSL/TLS and SSH session establishment[6]] 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.

SECURITY MANAGEMENT (FMT)

5.1.1.3.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions **of *TOE* data collection, review, analysis and reaction** to authorized ***TOE*** administrators.

MULTIPLE CONFORMANCE NOTE: Each of the 4 IDS PPs call out for the ability to modify the behavior of Analyzer, Scanner, Sensor and System functions, respectively. This requirement has been refined to call out the ability to modify the behavior of functions of TOE data. This modified requirement is applicable to this TOE claiming compliance against all 4 IDS PPs because the TSF that is maintaining users' security roles and corresponding modification abilities does not change among the PPs.

See the Multiple Conformance Note for FMT_SMR.1 (Section 5.1.1.3.4 - Security Roles) below for guidance on understanding the meaning and use of the "authorized TOE administrator" role in FMT_MOF.1.1.

5.1.1.3.2 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to query **and add *TOE* and audit data, and shall restrict the ability to query and modify all other TOE data** to [superusers and administrators].

MULTIPLE CONFORMANCE NOTE: Each of the 4 IDS PPs call out for the ability to query and add Analyzer, Scanner, Sensor and System data, respectively. This requirement has been refined to call out the ability to query and modify TOE data. This modified requirement is applicable to this TOE claiming compliance against all 4 IDS PPs because the TSF that is maintaining users' security roles and corresponding modification abilities does not change among the PPs.

[6] Please note that the evaluation laboratory did not evaluate the cryptography related to these session establishments.

5.1.1.3.3 FMT_SMF.1-INTERP-065 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [access control, authentication].

5.1.1.3.4 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the **following** roles*:* ***superuser*, *administrator*, and** [operator].

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

MULTIPLE CONFORMANCE NOTE: In each of the 4 IDS PPs, the FMT_SMR.1 requirement calls out the specific security role of authorized Analyzer administrator, authorized Scanner administrator, authorized Sensor administrator, or authorized System administrator, respectively. In this ST, these roles have been combined into the role of "administrator". This modified requirement is applicable to this TOE claiming compliance against all 4 IDS PPs because the TSF that is maintaining these security roles does not change among the PPs. It should also be noted that the UnityOne™ Administrator role that the TOE maintains maps directly to the "authorized Analyzer/Scanner/Sensor/System administrator" role defined in each of the 4 IDS PPs, respectively; they are one and the same. The "authorized administrator" role identified in FMT_SMR.1.1 in each of the 4 IDS PPs maps directly to the UnityOne™ Superuser role; they are one and the same. These roles are further described in Section 7.1.3.4 below.

PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

5.1.1.4.1 FPT_ITA.1 Inter-TSF availability within a defined availability metric

FPT_ITA.1.1 The TSF shall ensure the availability of **audit and *TOE* data** provided to a remote trusted IT product within [60 seconds] given the following conditions: [normal traffic on the communication network, IT products are operational and available].

MULTIPLE CONFORMANCE NOTE: Each of the 4 IDS PPs call out for the maintenance of the availability of Analyzer, Scanner, Sensor and System data, respectively. This requirement has been refined to call out the availability of TOE data. This modified requirement is applicable to this TOE claiming compliance against all 4 IDS PPs because the TSF that is maintaining these security roles does not change among the PPs.

5.1.1.4.2 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

5.1.1.4.3 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [one detected message authentication code (MAC) error within a transmission].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [resending of the data in the case of errors due to protocol issues or session dropping in the case of errors indicative of an attack] if modifications are detected.

5.1.1.4.4 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.1.4.5 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.1.4.6 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

IDS COMPONENT REQUIREMENTS (IDS)

The EXP notation following the IDS functional requirements indicates that the IDS PPs have explicitly stated requirements. These new requirements are indicated in bold text as well.

5.1.1.5.1 IDS_SDC.1 System data collection (EXP)

IDS_SCN.1 Scanner data collection (EXP)

IDS_COL.1 Sensor data collection (EXP)

MULTIPLE CONFORMANCE NOTE: The IDS_SDC.1 requirement is partially contained in both the IDS Scanner (IDS_SCN.1) and IDS Sensor (IDS_COL.1) PPs. The IDS_SCN.1 requirement refers to the Scanner's functionality, static configuration information and encompasses only the items 'detected malicious code' through detected known vulnerabilities' listed in IDS_SDC.1.1 below. The IDS_COL.1 requirement refers to the Sensor's functionality and encompasses only the items 'start-up and shutdown' through 'data introduction' listed in IDS_SDC.1.1 below. IDS_SCN.1.2 and IDS_COL.1.2 also refer to Scanner and Sensor actions and events, respectively (as opposed to System actions and events). This requirement is not present in the IDS Analyzer PP.

IDS_SDC.1.1 **The System shall be able to collect the following information from the targeted IT System resource(s):**

a) Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities**; and**

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

IDS_SDC.1.2 **At a minimum, the System shall collect and record the following information:**

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

b) The additional information specified in the *Details* column of Table 4 – IDS Scanner, Sensor and System Events. (EXP)

IDS_SCN.1.1 **The Scanner shall be able to collect the following information from the targeted IT System resource(s):**

a) detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities**; and**

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

IDS_SCN.1.2 **At a minimum, the Scanner 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 4 – IDS Scanner, Sensor and System Events. (EXP)

IDS_COL.1.1 **The Sensor shall be able to collect the following information from the targeted IT System resource(s):**

a) Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction**; and**

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

IDS_COL.1.2 **At a minimum, the Sensor 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 4 – IDS Scanner, Sensor and System Events. (EXP)

Table 4 – IDS Scanner, Sensor and System Events

Component	Event ID	Event[7]	Details
IDS_SDC.1 IDS_COL.1	1	Start-up and shutdown	**none**
IDS_SDC.1 IDS_COL.1	2	Identification and authentication events	**User identity, location, source address, destination address**
IDS_SDC.1 IDS_COL.1	3	Data accesses	**Object IDS, requested access, source address, destination address**
IDS_SDC.1 IDS_COL.1	4	Service requests	**Specific service, source address, destination address**
IDS_SDC.1 IDS_COL.1	5	Network traffic	**Protocol, source address, destination address**
IDS_SDC.1 IDS_COL.1	6	Security configuration changes	**Source address, destination address**
IDS_SDC.1 IDS_COL.1	7	Data introduction	**Object IDS, location of object, source address, destination address**
IDS_SDC.1 IDS_SCN.1	8	Start-up and shutdown of audit functions	**none**
IDS_SDC.1 IDS_SCN.1	9	Detected malicious code	**Location, identification of code**
IDS_SDC.1 IDS_SCN.1	10	Access control configuration	**Location, access settings**
IDS_SDC.1 IDS_SCN.1	11	Service configuration	**Service identification (name or port), interfaces, protocols**
IDS_SDC.1 IDS_SCN.1	12	Authentication configuration	**Account names for cracked passwords, account policy parameters**
IDS_SDC.1 IDS_SCN.1	13	Accountability policy configuration	**Accountability policy configuration parameters**
IDS_SDC.1 IDS_SCN.1	14	Detected known vulnerabilities	**Identification of the known vulnerability**

5.1.1.5.2 IDS_ANL.1 Analyzer analysis (EXP)

MULTIPLE CONFORMANCE NOTE: This requirement appears in a modified form in the IDS Analyzer PP. Instead of referring to the System, the Analyzer PP requirement refers to the TSF. This requirement is not present in the IDS Scanner and IDS Sensor PPs.

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

a) signature**; and**

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

[7] Events identified with a number 1 through 7 do **not** apply to the Scanner PP and events identified with a number 8 through 14 do **not** apply to the Sensor PP.

IDS_ANL.1.2 **The *TSF or* System shall record within each analytical result at least the following information:**

a. Date and time of the result, type of result (message, policy ID, signature ID, and classification), identification of data source; and

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

5.1.1.5.3 IDS_RCT.1 Analyzer react (EXP)

MULTIPLE CONFORMANCE NOTE: This requirement appears in a modified form in the IDS Analyzer PP. Instead of referring to the System, the Analyzer PP requirement refers to the TSF. This requirement is not present in the IDS Scanner and IDS Sensor PPs.

IDS_RCT.1.1 **The *TSF or* System shall send an alarm to [**an email address or to the Alert or Block log in the form of a log entry**] and take [**drop the packet and terminate the session, allow the packet to flow through**] when an intrusion is detected. (EXP)**

5.1.1.5.4 IDS_RDR.1 Restricted data review (EXP)

IDS_RDR.1.1 **The *TOE* shall provide [**superuser, administrator, and operator roles**] with the capability to read [**all TOE data**] from the *TOE* data. (EXP)**

IDS_RDR.1.2 **The *TOE* shall provide the *TOE* data in a manner suitable for the user to interpret the information. (EXP)**

IDS_RDR.1.3 **The *TOE* shall prohibit all users read access to the *TOE* data, except those users that have been granted explicit read-access. (EXP)**

MULTIPLE CONFORMANCE NOTE: This requirement appears in a modified form in the IDS Analyzer, IDS Scanner and IDS Sensor PPs. Rather than "System" and "System data", the Analyzer, Scanner, and Sensor PPs refer to the Analyzer, Scanner, or Sensor and that component's data, respectively. This requirement has been further modified from that contained in the IDS System PP and calls out the "TOE" and "TOE data" rather than the "System" and "System data", respectively. Each of the four IDS PPs calls out the ability for the IDS component or IDS system to provide TOE data to authorized users in a suitable manner. The means by which data is provided and presented is identical whether the TOE is configured as an Analyzer, Scanner, Sensor, or System. This modified requirement is thereby applicable to this TOE claiming compliance against all 4 IDS PPs.

5.1.1.5.5 IDS_STG.1 Guarantee of TOE data availability (EXP)

IDS_STG.1.1 **The *TOE* shall protect the stored *TOE* data from unauthorized deletion. (EXP)**

IDS_ STG.1.2 **The *TOE* shall protect the stored *TOE* data from modification. (EXP)**

IDS_ STG.1.3 **The *TOE* shall ensure that [*all*] *TOE* data will be maintained when the following conditions occur: *TOE*** data storage exhaustion, attack**. (EXP)**

MULTIPLE CONFORMANCE NOTE: This requirement appears in a modified form in the IDS Analyzer, IDS Scanner and IDS Sensor PPs. Rather than "System" and "System data", the Analyzer, Scanner, and Sensor PPs refer to the Analyzer, Scanner, or Sensor and that component's data, respectively. This requirement has been further modified from that contained in the IDS System PP and calls out the "TOE" and "TOE data" rather than the "System" and "System data", respectively. Each of the four IDS PPs calls out the ability for the IDS component or

IDS system to protect data from unauthorized deletion and modification, and to protect this data in the event of data storage exhaustion and/or attack. The means by which data is stored and protected is identical whether the TOE is configured as an Analyzer, Scanner, Sensor, or System. This modified requirement is thereby applicable to this TOE claiming compliance against all 4 IDS PPs.

5.1.1.5.6 IDS_STG.2 Prevention of TOE data loss (EXP)

IDS_STG.2.1 **The *TOE* shall** overwrite the oldest stored ***TOE*** data **and send an alarm if the storage capacity has been reached. (EXP)**

MULTIPLE CONFORMANCE NOTE: This requirement appears in a modified form in the IDS Analyzer, IDS Scanner and IDS Sensor PPs. Rather than "System" and "System data", the Analyzer, Scanner, and Sensor PPs refer to the Analyzer, Scanner, or Sensor and that component's data, respectively. This requirement has been further modified from that contained in the IDS System PP and calls out the "TOE" and "TOE data" rather than the "System" and "System data", respectively. Each of the four IDS PPs calls out the ability for the IDS component or IDS system to overwrite the oldest stored TOE data and send an alarm if storage capacity has been reached. The means by which data is overwritten and alarms are sent is identical whether the TOE is configured as an Analyzer, Scanner, Sensor, or System. This modified requirement is thereby applicable to this TOE claiming compliance against all 4 IDS PPs.

6 TOE Security Assurance Requirements

This section specifies the Security Assurance Requirements (SARs) for the TOE. Table 5 – Security Assurance Requirements for the TOE below provides a complete listing of the Assurance Requirements for the TOE at EAL2 with no augmentation. Assurance requirements are taken from the CC Part 3.

Table 5 – Security Assurance Requirements for the TOE

Assurance Class	Assurance Components	
ACM: Configuration Management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

6.1.1 Configuration Management (ACM)

CONFIGURATION ITEMS (ACM_CAP.2)

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a Configuration Management (CM) system.

ACM_CAP.2.3D The developer shall provide CM documentation.

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

6.1.2 Delivery and Operation (ADO)

DELIVERY PROCEDURES (ADO_DEL.1)

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

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

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

INSTALLATION, GENERATION, & START-UP PROCEDURES (ADO_IGS.1)

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

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

6.1.3 Development (ADV)

INFORMAL FUNCTIONAL SPECIFICATION (ADV_FSP.1)

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

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

DESCRIPTIVE HIGH-LEVEL DESIGN (ADV_HLD.1)

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

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces of the subsystems of the TSF are externally visible

INFORMAL CORRESPONDENCE DEMONSTRATION (ADV_RCR.1)

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

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

6.1.4 Guidance Documents (AGD)

ADMINISTRATOR GUIDANCE (AGD_ADM.1)

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

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

USER GUIDANCE (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non- administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

6.1.5 Tests (ATE)

EVIDENCE OF COVERAGE (ATE_COV.1)

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

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

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, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

INDEPENDENT TESTING (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.

6.1.6 Vulnerability Assessment (AVA)

STRENGTH OF TOE SECURITY FUNCTION EVALUATION (AVA_SOF.1)

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

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level of SOF-basic.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength metric of SOF-basic.

DEVELOPER VULERABILITY ANALYSIS (AVA_VLA.1)

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities

AVA_VLA.1.1C The documentation shall show, for all intended vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

.

7 TOE Summary Specification

This section provides a high-level definition of the IT Security Functions and the Assurance Measures provided by the TOE to meet the SFRs and SARs specified in this ST.

The TOE provides the following five Security Functions:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions
- IDS-Specific Functionality (IDS Component Requirements)

MULTIPLE CONFORMANCE NOTE: The subtle differences between the security functions performed by the IDS System and the security functions performed by the IDS Analyzer, Scanner, and/or Sensor have been identified in *Section 5: IT Security Requirements* and are not re-identified in this section except in explanatory text that describes how the TOE meets each functional requirement.

7.1 TOE Security Functions

7.1.1 Security Audit (FAU)

Audit data generation

The TOE has five types of audit data logs: the Fault Log, the Alert Log, the System Log, the Block Log, and the Audit Log. These logs are accessible to the roles defined in FMT_SMR.1. Only the superuser and administrator roles are able to modify the logs, with only the superuser role being able to view/clear the audit log (audit records). The operator has read-only access to the fault, alert, system, and block logs and no access to the audit log. Logs can be accessed via the CLI (using the `show log ?` command) or the LSM (via the Logs page), but only the LSM may be used to view logs in the CC-evaluated version as the LSM was designed to facilitate log viewing and comprehension.

The TOE audits all information described in Table 6 – Auditable Events, the startup and shutdown of the TOE, and access to the Analyzer, Scanner, Sensor, System, as well as TOE, Analyzer, Scanner, Sensor and System data as configured by the authorized administrators.

The **Fault Log** contains alerts arising from hardware issues.

The **Alert Log** contains alerts triggered by signatures.

The actions taken due to storage failure are logged to the **System Log**.

The **Block Log** contains a list of packets that were blocked by the TOE.

Where the Fault, Alert, System, and Block logs indicate state changes (e.g., software/hardware fault, blocked packet, or alert), the **Audit Log** indicates user access changes (e.g., updates to the system via a configuration command). All attempts to authenticate to the TOE are logged to the Audit Log. As configured by the authorized administrator (via signatures), the TOE is able to log access to Analyzer, Scanner, Sensor, and System data. The audit records generated by the TOE also include a timestamp, the event being logged, the subsystem triggering the log, and the outcome of the event (if applicable). The Audit Log contains the following additional fields: interface (web, telnet, or serial), IP address (where appropriate), and success/failure of the audited event.

Meets Functional Requirements: FAU_GEN.1.1, FAU_GEN.1.2

Table 6 – Auditable Events

Component	Event	Details	Log Type
FAU_GEN.1	Start-up and shutdown of audit functions		Audit
FAU_GEN.1	Access to TOE		Audit
FAU_GEN.1	Access to the TOE data	Object IDS, Requested access	Audit[8]
FAU_SAR.1	Reading of information from the audit records		Audit
FAU_SAR.2	Unsuccessful attempts to read information from the audit records		Audit
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating		Audit
FAU_STG.4	Actions taken due to storage failure		System & Audit
FIA_UAU. 1	All use of the authentication mechanism	User identity, location, method	Audit
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	User identity, location, method	Audit
FMT_MOF.1	All modifications in the behavior of the functions of the TSF		Audit
FMT_MTD.1	All modifications to the values of TSF data		Audit
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity	Audit[9]
FPT_ITI.1	The action taken upon detection of modification of transmitted TSF data		Audit

Audit review

When a request to review audit records is entered by clicking on the `Logs` tab of the LSM, the permission-enforcement API validates the user's audit accessibility and passes the request to a library, which in turn uses the system-support API to extract audit log records from disk storage. For a remote authorized superuser, these logs are either in raw data form (text with binary packet if logged) or parsed into XML. When accessed via the web or through a remote shell, the logs are in text format. XML is only available through remote TippingPoint products, which are outside the scope of this evaluation.

The TOE only allows the superuser role to access the audit data contained in the Audit Logs.

[8] The TOE does not audit reads of the TOE data, only writes of that data. This audit record is stored in the Audit Log.
[9] The notion of "groups" of users does not exist in the TOE. The Audit Log stores audit information regarding single user modification.

Administrators and operators can also view a subset of the logs maintained by the TOE as described in Table 7 below. Logs are accessible via the LSM.

Table 7 – Log Review Based on Access Role

Log Type	Superuser Access	Administrator Access	Operator Read-Only Access
Fault Log	✓	✓	✓
Block Log	✓	✓	✓
System Log	✓	✓	✓
Alert Log	✓	✓	✓
Audit Log	✓	X	X

Meets Functional Requirements: FAU_SAR.1.1 (iteration #1), FAU_SAR.1.2 (iteration #1), FAU_SAR.1.1 (iteration #2), FAU_SAR.1.2 (iteration #2)

Restricted audit review

The permission-enforcement API compares the user access level for all incoming audit review requests to the access level of the user role provided and maintained by the authorization API (see *Section 7.1.1.2 Audit review* for a description of audit access methods). 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 audit records stored by the TOE.

Audit data is stored in the Audit Log (viewable from the `Logs` page of the LSM) and only the superuser role has access to this log. An unauthorized user cannot bypass role enforcement and/or identification and authentication mechanisms to view an audit record via the LSM. Users who are logged in to the TOE as an operator- or administrator-level user do not have a link in the LSM to view the Audit Log. If the URL of an accessed Audit Log is pasted into the Web browser the user (operator or administrator-level) is immediately returned to the LSM login screen and an audit record is generated to the Audit Log.

Meets Functional Requirements: FAU_SAR.2.1

Selectable audit review

The capability for selective review of audit records is implemented in the Web browser. When an authorized user makes a selective request for audit records by clicking on an audit record parameter heading in the `Logs` section of the LSM (i.e. Log Entry Time, Username, Interface, Component, Action, or Result), the Web server sorts the records according to the specific request. The Web server sends the page that contains the Javascript instructions for sorting.

The superuser role, using shell access, is able to select audit logs based on information contained in the logs, including timestamp, user identity, event type, interface type (web, Command Line Interface (CLI), serial), IP address, or outcome of the event (Pass/Fail).

Meets Functional Requirements: FAU_SAR.3.1

Selective audit

Auditable events (i.e., the auditable events for the basic level of auditing as specified in the Common Criteria) can be included or excluded from the set of audited events based on event type. A library maintains a list of auditable event types which user of the TOE can update via the CLI using the `configure` command (this selection cannot be performed via the LSM). The selection determines which events are written to the audit log, host port block log entries, and system start/stop log entries.

Only the superuser role is able to select components to audit.

It should be understood that the UnityOne™ architecture is such that a single command (e.g. `config t log audit select report`) may enable/disable audited events that correspond to more than one Common Criteria functional component and/or event type. The issue of locating log events relating to a specific functional component is resolved through post-selection sorting of the audit records (FAU_SAR.3).

A mapping that links components, event types, pre-selection audit commands and UnityOne™ log messages has been included in the document titled *Common Criteria Certified Installation and Configuration Guidelines for UnityOne™ v1.2* (specifically, Appendix C). A superuser can sort audit records alphabetically by log message after these records have been collected. Referring to this mapping table allows the administrator to locate and view exactly which audit records relate to the functional component and/or event type of interest.

Meets Functional Requirements: FAU_SEL.1.1

Guarantees of audit data availability

The TOE does not allow a user to modify audit data outside of allowing an authorized superuser to completely purge the Audit Log using the `clear` CLI command or `Reset` LSM command found on the `Logs` page. The permission-enforcement API compares the user access level for all incoming audit review requests to the access level of the user role provided and maintained by the authorization API. If the access level of the requested action is greater than the current user's access level, the requested action to purge is denied. This purge action is logged, allowing for detection of the deletion of audit records.

The only modifications that can be made to audit records within an audit log are a log "reset" or a log "rotate" that can be performed by a superuser. Resetting a log clears the log and logs that the reset has been performed, and rotating a log pushes the log data out to an older version of the log, preserving the log information but freeing space in the log. This action is also logged.

Additionally, the TOE performs resource management, especially when the module is under attack. This resource management attempts to minimize impacts to limited resources and ensure that the TOE continues to function properly under an attack. All audit events stored prior to audit storage exhaustion are maintained; overwriting logs based on FIFO priority is a last resort.

Meets Functional Requirements: FAU_STG.2.1, FAU_STG.2.2, FAU_STG.2.3

Prevention of audit data loss

Audit records are stored sequentially in a log file. When a log file reaches a watermark file size, the log is closed, a new file is created, and an alert (via an E-mail message) is sent to an authorized administrator. New audit log records will be written to the newly created log file. When the number of audit logs exceeds six, the TOE will delete the oldest log. This frees up disk space for the new audit log.

The E-mail client is responsible for sending a canned text message to a designated E-mail address whenever the Audit Log reaches capacity and rolls over.

Meets Functional Requirements: FAU_STG.4.1

7.1.2 Identification and Authentication (FIA)

Timing of authentication

Before a user is authenticated to the TOE, the user is restricted in the actions that they perform. The user is permitted only to establish an SSH or SSL session.

Part of SSH session establishment[10] is the submission of user credentials (username and password), which the SSH interface enforces using the authorization API to validate the username/password pair. Only when a valid login has been supplied is the user connected to a CLI session.

The Web server ensures that a user can only access the TOE login page before authentication. No other functions or types of access are permitted from the Web interface prior to identification and authentication. User authentication is performed in the Web session by making a call to the authorization API and the user (if authorized) is logged into the TOE. Only then are additional functions and types of access made available.

The TOE treats every user as a hostile user until that user has been successfully identified and authenticated to the TOE and thus does not permit access to any other functionality or data.

Meets Functional Requirements: FIA_UAU.1.1, FIA_UAU.1.2

Authentication Failure Handling

When five consecutive unsuccessful authentication attempts are performed by a user, the TSF disables this user's account by updating an account state attribute that is stored by the authorization API. This disabling prevents the offending external IT product from successfully authenticating until an authorized superuser re-enables the account. While the default number of unsuccessful authentication attempts for a user is five, this number can be set by a superuser to any integer between 1 and 10 (inclusive) from the `Admin` screen of the LSM.

Any account disabling is audited.

Meets Functional Requirements: FIA_AFL.1.1, FIA_AFL.1.2

User attribute definition

The authorization API maintains a list of security attributes in the form of individual records that belong to a particular user. These attributes are the user identity, authentication data, authorizations (roles), password expiration information and lockout parameters. These attributes can be modified by an authorized superuser from the `Admin` and `Configure` pages of the LSM or using the `user` command of the CLI.

Meets Functional Requirements: FIA_ATD.1.1

Timing of identification

Before a user is identified to the TOE, the user is restricted in the actions that they perform. The user is permitted only to establish an SSH or SSL session[11].

[10] Please note that the evaluation laboratory did not evaluate the cryptography related to these session establishments.
[11] Please note that the evaluation laboratory did not evaluate the cryptography related to these session establishments.

Part of SSH session establishment is the submission of user credentials (username and password), which the SSH interface enforces using an API to validate the username/password pair. Only when a valid login has been supplied is the user connected to a CLI session.

The Web server ensures that a user can only access the TOE login page before identification. No other functions or types of access are permitted from the Web interface prior to identification and authentication. User authentication is performed in the Web session by making a call to the authorization API and the user (if authorized) is logged into the TOE. Only then are additional functions and types of access made available.

The TOE treats every user as a hostile user until that user has been successfully identified and authenticated to the TOE and thus does not permit access to any other functionality or data.

Meets Functional Requirements: FIA_UID.1.1, FIA_UID.1.2

7.1.3 Security Management (FMT)

Management of security functions behavior

The permission-enforcement API compares the user access level for all incoming requests to the access level of the user role provided and maintained by the authorization API. 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 the ability to modify the behavior of the functions of analysis and reaction; only superuser and administrator roles are able to perform these modifications (modifying filters, discovery, monitoring, and updating pages/functions). These modifications can be made using the CLI (`configure` command) or the LSM (Configure, Filters, Discover and Update pages).

Meets Functional Requirements: FMT_MOF.1.1

MULTIPLE CONFORMANCE NOTE: The actions that an authorized user can perform is primarily restricted by two things – the user's role/access level and the TOE's configuration (Analyzer, Scanner, Sensor or System). When the TOE is configured as an IDS Sensor, scanning and analysis functions are unavailable since they have not yet been configured. When the TOE is configured as an IDS Scanner, an authorized user can now perform all Sensor functions as well as Scanner functions. Further configuration is necessary to set up the TOE as an IDS Analyzer and access the analysis functionality of the TOE. When the TOE is set up as an IDS Analyzer, full IDS System functionality is available to authorized users.

Management of TSF data

The permission-enforcement API compares the user access level for all incoming requests to the access level of the user role provided and maintained by the authorization API. 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 both the ability to modify or query IDS System, Analyzer, Scanner, Sensor, and audit data.

The operator role is only permitted to read TOE and Analyzer, Scanner, Sensor and System data. The administrator role is able to read and modify this data, with the restriction that they cannot view or clear the Audit Log, nor can the administrator role modify audit selection. The superuser role is able to read and modify all system data.

The ability to manage "system" data refers to the ability to schedule scans and enable/disable signatures. This scheduling can be performed via the `Discover` page of the LSM. This ability also includes clearing of Alert, Block, Fault, and System logs, which can be performed via the `Logs` page of the LSM or using the `clear` CLI command. Time management can be modified by superuser and administrator roles using the `configure` CLI command or the `Configure` page of the LSM. Queries of TOE data can be performed using the `show` and `user` CLI commands or through the Logs, Monitor and Admin pages of the LSM.

Meets Functional Requirements: FMT_MTD.1.1

Specification of Management Functions

Access to the TOE and TOE data is controlled by the authentication and access control mechanisms that the TOE provides and implements.

Meets Functional Requirements: FMT_SMF.1.1

Security roles

The authorization API maintains a list of security attributes in the form of individual records that belong to a particular user; one of these attributes is the user's role.

The following roles are defined on the TOE:

- **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. This role corresponds to the "authorized administrator" role that is called out in the FMT_SMR.1 requirement in each of the 4 IDS PPs.

- **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 clearing of the audit log). This role corresponds to the "authorized Analyzer/Scanner/Sensor/System administrator" role that is called out in the FMT_SMR.1 requirement in each of the 4 IDS PPs and the "authorized System administrator" role that is called out in Section 5.1.1.3.4.

- **Operator** – Read-only access to the TOE. This role is able to view the logs and configuration of the TOE, but is not permitted to modify any information other than his/her own password.

Each authorized user of the TOE is assigned to one and only one access level. It should also be noted that authorized Analyzer/Scanner/Sensor/System administrators possess the same privileges and access rights as users with the access role of Administrator who are not IDS-component or IDS-System specific.
A user account cannot be created without an associated role; if this is attempted, the action is denied and the interface enforces that a role be specified before proceeding with account creation.

Superusers are permitted to change their role or the roles of other users. This is accomplished using the `user` CLI command or through the `Admin` screen of the LSM. A list of all users and their associated roles can be viewed by any authorized user from the `Admin` screen of the LSM.

Table 8 – Mapping of UnityOne™-defined Roles to PP-defined Roles

UnityOne™ Role	Corresponding IDS PP-defined Role
Superuser	Authorized Administrator
Administrator	Authorized Analyzer Administrator Authorized Scanner Administrator Authorized Sensor Administrator Authorized System Administrator
Operator	Not defined in any of the IDS PPs, but this role is called out as an Assignment in the FMT_SMR.1 requirement included in Section 5.1.1.3.4.

Meets Functional Requirements: FMT_SMR.1.1, FMT_SMR.1.2

7.1.4 Protection of the TOE Security Functions (FPT)

Inter-TSF availability within a defined availability metric

Once a request for data has been made by the user, a library makes the calls necessary to the management services responsible for retrieving the requested information. Only those users that have been granted (via their roles) explicit read-access are able to view this information.

Under normal conditions, the TOE will provide alert and block no later than one minute after the information is requested by the remote trusted IT product. Information can be delayed based on retrieving older information (the delay is increased as the age of the information increases), attempting to filter data (requires a comparison of fields), or attempting to display all of the records available at once.

Filter settings can be created and modified via the Filters and Configure pages of the LSM. Configuration can also be performed using the CLI `configure` command.

Meets Functional Requirements: FPT_ITA.1.1

Inter-TSF confidentiality during transmission

SSL provides a secure channel for communications between a Web browser and the UnityOne™[12]. SSH provides a secure channel for communications between the user's client software and the CLI terminal server.

The transmitted data is encrypted and MAC'd (message authentication coded) to ensure confidentiality and integrity of the transmitted data.

Configurations related to this requirement can be performed using the `configure` CLI command or the Configure LSM page.

Meets Functional Requirements: FPT_ITC.1.1

Inter-TSF detection of modification

Communications between the TOE and a remote management console (i.e. a Web browser) are secured using SSL/TLS[13].

SSL is capable of detecting modifications to TSF data during transmission between trusted IT products and the TOE. SSL can also resend the data if modifications are detected but, if invalid MACs, timestamps, and/or other characteristics indicative of an attack are detected by the TOE, the session will be dropped. An audit record will also be generated to record that there was an encryption error with the web session.

SSH is capable of detecting modifications to TSF data during transmission between trusted IT products and the TSF[14]. SSH can also resend the data if modifications are detected but, if invalid MACs, timestamps, and/or other characteristics indicative of an attack are detected by the TOE, the session will be dropped. An audit record will also be generated to record that there was an encryption error with the SSH session.

[12] Please note that the evaluation laboratory did not evaluate the cryptography related to these SSL or SSH sessions.
[13] Please note that the evaluation laboratory did not evaluate the cryptography related to these SSL sessions.
[14] Please note that the evaluation laboratory did not evaluate the cryptography related to these SSH sessions.

Remote shell access communications with the TOE are secured using SSH. The transmitted data is encrypted and MAC'd (message authentication coded) to ensure confidentiality and integrity of the transmitted data.

Meets Functional Requirements: FPT_ITI.1.1, FPT_ITI.1.2

Non-bypassability of the TSP

The permission-enforcement API compares the user access level for all incoming requests to the access level of the user role provided and maintained by the authorization API. If the access level of the requested action is greater than the current user's access level, the requested action is denied. Traffic can come into the TOE in one of four modes. Each mode and the relevant security measures to ensure non-bypassability are described below:

Mode A: Serial port
The UnityOne™ has a serial port that is used ONLY during initial installation and configuration. It may be used in a non-operational manner for troubleshooting purposes. At all other times this interface is not connected, therefore this is not an interface used in normal operation of the device.

Mode B: Host Management interface
The UnityOne™ provides an Ethernet interface (10/100) that is to be connected only to the management network. This interface is protected at multiple levels:
1. The protocol stack is configured to ignore ICMP traffic as part of the normal installation and configuration procedures.
2. All traffic must be encrypted via either an SSH or an SSL connection.
3. All traffic is then routed as appropriate.

Mode C: Network interface - Data traffic
All data traffic enters the UnityOne™ via the Data Network interface. All traffic is monitored by the data network hardware, which implements the filters. Processing of the network traffic is performed, as required. If a host or network hardware failure occurs, the network interface will then stop passing data traffic.

Mode D: Network interface - Scanner traffic
When the UnityOne™ scans the network, it will use the Data Network interface. When the scanner is configured, communication will be controlled from the scanner to devices on the data network. Traffic destined for the scanner (based on the configured IP address) is filtered and only scanner-specific data is allowed to flow through.

The TOE further ensures that TSP enforcement functions are invoked and succeed before each function with the TSC is allowed to proceed. For example, when a remote user connects to the TOE for shell access, the TOE must first establish an SSH connection with the remote user. Next, the user must successfully log in with a valid username and password. Once these steps are completed successfully, the authorized administrator has access to functions as specified by his or her assigned role.

At all physical interfaces, the TOE intercedes to ensure non-bypassability. Traffic can only come into the TOE via three physical interfaces: the Serial Port (which is used only during initial setup and configuration of the TOE), the Host Management interface (access to which is controlled by a username a password), or the Data Network interface (where the traffic is monitored by the TOE but no actions can be executed). Unauthorized users cannot bypass the identification and authentication mechanisms, and traffic cannot bypass these three interfaces to enter the TOE.

Meets Functional Requirements: FPT_RVM.1.1

TSF domain separation

The TOE is a hardware device that executes all of its processes internally. It is accessible only via the defined interfaces and only authorized administrators are able to modify the functionality of the TOE.

The Data Network interface is a dedicated physical and logical interface that is associated with network interface ports and used to passively monitor network packets from the target IT system. It does not implement a TCP/IP protocol stack and does not have a routable IP address. It simply receives raw packets for analysis within the TOE.

This interface enforces domain separation in that any data sent to this interface (which is presumed untrusted) is logically separated from all other TOE data. It is never executed but rather is parsed for analysis.

Traffic flowing through the TOE is subject to the policies as defined by the authorized administrators.

At all physical interfaces, the TOE intercedes to ensure domain separation. Traffic can only come into the TOE via three physical interfaces: the Serial Port (which is used only during initial setup and configuration of the TOE), the Host Management interface (access to which is controlled by a username a password), or the Data Network interface (where the traffic is monitored by the TOE but no actions can be executed). Traffic and/or unauthorized users cannot bypass the identification and authentication mechanisms, preventing interference and tampering by untrusted subjects and thereby maintaining a domain for its own execution.

Meets Functional Requirements: FPT_SEP.1.1, FPT_SEP.1.2

Reliable time stamps

A system time maintained by the operating system is read by a TOE component. The operating system maintains the system time by periodically comparing its stored value to the real-time clock on the Management Processor of the TOE

The time can only be modified by an authorized superuser or administrator role using the `configure` CLI command or the `Configure` page of the LSM. It is also possible to have the TOE synchronize with a time server via SNTP but SNTP is outside the scope of this evaluation and is not used in the CC-evaluation configuration of the TOE.

Meets Functional Requirements: FPT_STM.1.1

7.1.5 IDS Component Requirements (IDS)

System data collection

Scanner data collection
Sensor data collection

The TOE contains and manages all IDS System, Analyzer, Scanner, and Sensor records. Traffic flowing through the module is monitored according to the defined policies accessible via the `Filters, Discovery` and `Configure` pages of the LSM or, in part, using the `configure` and `show` CLI commands. Logs are generated based on these policies, and these logs include timestamps, presumed source address, and the reaction to the attack. Log entries are also written to the System Log when the IDS system, analyzer, scanner, and sensor are launched or shutdown.

The Network Discovery Service (NDS) is the primary data collector for IDS system and scanner data; it is, in essence the **IDS Scanner** component. The NDS probes a targeted network through the Data Network Interface for the purpose of detecting services running on machines attached to the targeted network. The NDS utilizes the system-support API to record the collected scanner data to the IDS logs. The NDS supports the scanner data collection by scanning the hosts monitored by the device and storing the results of the scan in an internal database.

Additionally, the NDS scans the hosts monitored by the IDS in order to determine the information about those hosts that relates to IDS functionality. The results of the scans are used to populate a database, which in turn is used by the IDS to determine what signatures apply to which hosts.

The database populated by the NDS contains the following information:

- OS and version and/or detected network device (e.g., if a network printer is detected, the device type will be displayed)
- Service type
- Service port number
- IP address
- Security zone
- Date of last device scan (used for auto-tuning)

The NDS performs "normal" network discovery scans. Normal scans search for new hosts and determine which services are running on which ports on those hosts. Normal scans determine the OS, OS version number, and detected network for each service running on the machine.

A separate TOE component acts as an **IDS Sensor**. This component, along with networking hardware, inspects network traffic according to filter settings. When network traffic that matches a particular filter is sensed, this component informs the notification mechanism. This component also supports the "anomaly filters" – these are filters designed to identify and report reconnaissance activities such as port scans and host sweeps. These activities are precursors to a future intrusion or attack, and, as such, considered part of the IDS Analyzer functionality.

Meets Functional Requirements: IDS_SDC.1.1, IDS_SDC.1.2, IDS_SCN.1.1, IDS_SCN.1.2, IDS_COL.1.1, IDS_COL.1.2

Analyzer analysis

The TOE performs signature-based analysis of traffic as it flows through the UnityOne™. Analysis methodologies match specific signatures or patterns that may characterize attack attempts to characteristics of known attacks. Using scanner data, the potential threat ("severity") is further qualified. Statistical techniques are employed to identify reconnaissance activity, which may be a precursor to an intrusion.

The Unified Defense Management (UDM) component, essentially the **IDS Analyzer** component, supports the analysis of collected data by supplying the information necessary to further qualify the severity of an attack. Specifically, an attack is downgraded in its severity if the NDS database notes that the target address of the attack packet is offline or if the service running on the attacked port is not vulnerable to the attack.

The UDM also installs signature-based rules into the sensor component, together with the action (Allow or Deny) as defined by the security policy. The UDM utilizes the system-support API to record the analytical results to the applicable logs.

Within each analytical result, the following information is stored:

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

Analysis settings are configured via the `Filters` page of the LSM.

Meets Functional Requirements: IDS_ANL.1.1, IDS_ANL.1.2

Analyzer react

The UDM (i.e. the IDS Analyzer component of the TOE) supports the analyzer reaction by receiving alerts that particular signatures have been triggered and executing the configured reaction alert. Analysis settings are configured via the `Filters` page of the LSM.

The UnityOne™ v1.2 is capable sending alerts via:

- **Log File:** Writes an alert message to the UnityOne™'s Alert or Block log file.
- **E-mail:** Sends an e-mail to a specified address.

The TOE can take the following actions when an alert is triggered:

- **Allow:** Allows the packet to pass through the UnityOne™.
- **Deny:** Causes the packet to be dropped without delivering it to the destination and terminates the session.

Packet capture, useful for performing future analysis, can be enabled in conjunction with the Allow action or the Deny action, if desired.

Meets Functional Requirements: IDS_RCT.1.1

Restricted data review

The permission-enforcement API compares the user access level for all incoming data review requests to the access level of the user role provided and maintained by the authorization API. 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 IDS analyzer, scanner, sensor, and system data stored by the TOE. These requests can be performed using the `Attacks`, `Logs`, `Monitor`, `Discover` and `Admin` pages of the LSM. Some of this data can also be accessed using the `show` CLI command.

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

For a remote authorized administrator, these logs are either in raw data form (text with binary packet if logged) or in parsed into XML. When accessed locally or through a remote shell, the logs are in text format. XML parsed logs are only available when the TOE is communicating to a remote TippingPoint Management system. Remote TippingPoint Management systems are, however, outside the scope of this evaluation.

Meets Functional Requirements: IDS_RDR.1.1, IDS_RDR.1.2, IDS_RDR.1.3

7.1.5.5 Guarantee of Analyzer, Scanner, Sensor and System data availability

The permission-enforcement API compares the user access level for all incoming data modification requests to the access level of the user role provided and maintained by the authorization API. 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 IDS system, analyzer, scanner, and sensor data. Deletion can be performed via the `Logs` or `Discover` pages of the LSM or using the `clear` CLI command.

The IDS logs are stored on the TOE. Operator roles have read-only access to the IDS logs (this does not include the Audit Log) via the `Logs` page of the LSM. Administrator and superuser roles have the ability to modify the TOE system data (this is not referring to data stored in the Audit Log).

When an attack occurs on TOE resources or storage exhaustion is eminent, the TOE resource manager attempts to compensate for the attack or exhaustion. In the worst case, the log files are FIFO, with old logs being overwritten with new ones.

Meets Functional Requirements: IDS_STG.1.1, IDS_STG.1.2, IDS_STG.1.3

7.1.5.6 Prevention of Analyzer, Scanner, Sensor and System data loss

All IDS system, analyzer, scanner, and sensor records are contained and managed by a component of the TOE. The TOE maintains multiple log files for each type of log. Each log's capacity is monitored and, when the capacity is exceeded, the oldest of the log files is deleted and an alarm is sent. This frees up space for the creation of a new file of that type. The alarm takes the form of an E-mail alert and a new audit record written to a different log than the one that has exceeded the capacity.

Additionally, log entries are written to the System Log when the IDS system, analyzer, scanner, and sensor are launched or shutdown.

Email alert contacts can be created in the Filters LSM page.

Meets Functional Requirements: IDS_STG.2.1

7.2 TOE Security Assurance Measures

This section of the ST maps the assurance requirements for a CC EAL2 level of assurance to the assurance measures used for the development and maintenance of the TOE. Table 9 provides a mapping of the appropriate documentation to the assurance requirements.

The TOE was developed with the following security assurance measures in place, which constitute a CC EAL2 level of assurance:

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documentation
- Testing
- Vulnerability Assessment

Table 9 – Assurance Measures Mapping to Security Assurance Requirements (SARs)

CC Assurance Components	TippingPoint Assurance Measures
ACM_CAP.2 Configuration items	TippingPoint UnityOne™ version 1.2 Configuration Management Description v1.4
ADO_DEL.1 Delivery procedures	TippingPoint UnityOne™ version 1.2 Secure Delivery and Installation v1.5
ADO_IGS.1 Installation, generation, and start-up procedures	*Common Criteria Certified Installation and Configuration Guidelines for UnityOne™ Version 1.2*; TECHD-0000000030; Publication Control Number 080603 which then references the following: *Quick Start UnityOne™ Intrusion Prevention System*; Part Number TECHD-0000000003; Publication Control Number 062603 *UnityOne™ Model 400/1200/2400 Intrusion Prevention Appliance Installation and Configuration Guide Version*

CC Assurance Components	TippingPoint Assurance Measures
	1.2; Part Number TECHD -00000000015; Publication Control Number 030503 *UnityOne™ Model 2000 Intrusion Prevention System Installation and Configuration Guide Version 1.2*; Part Number TECHD -00000000004; Publication Control Number 021303 *UnityOne™ Command Line Interface Reference Version 1.2*; Part Number TECHD-0000000013; Publication Control Number 062503 *UnityOne™ Local Security Manager User Guide Version 1.2*; Part Number TECHD-00000000014; Manufacturing Revision A07; Publication Number 021903 *Licensing V1.2*; Part Number TECHD-0000000005
ADV_FSP.1 Informal functional specification	TippingPoint UnityOne™ version 1.2 Functional Specification v1.9 *UnityOne™ Command Line Interface Reference Version 1.2*; Part Number TECHD-0000000013; Publication Control Number 062503 *UnityOne™ Local Security Manager User Guide Version 1.2*; Part Number: TECHD-0000000014; Manufacturing Revision:A07; Publication Control Number: 021903 *Common Criteria Certified Installation and Configuration Guidelines for UnityOne™ Version 1.2*; TECHD-0000000030; Publication Control Number 080603 *UnityOS™ Draft High Level Design Document*; Pub Number: Not Assigned; Revision unpub 2002-10-28.
ADV_HLD.1 Descriptive high-level design	TippingPoint UnityOne™ version 1.2 High-Level Design v1.5 *UnityOS™ Draft High Level Design Document; Pub Number: Not Assigned; Revision unpub 2002-10-28.* TippingPoint Technologies, Inc. UnityOne™ Version 1.2 Functional Specification v1.9
ADV_RCR.1 Informal correspondence demonstration	TippingPoint UnityOne™ version 1.2 Informal Correspondence Analysis v1.3
AGD_ADM.1 Administrator guidance	*UnityOne™ Command Line Interface Reference Version 1.2*; Part Number TECHD-0000000013; Publication Control Number 062503 *UnityOne™ Local Security Manager User Guide Version 1.2*; Part Number: TECHD-0000000014; Manufacturing Revision:A07; Publication Control Number: 021903 *Common Criteria Certified Installation and Configuration Guidelines for UnityOne™ Version 1.2*; TECHD-0000000030; Publication Control Number 080603

CC Assurance Components		TippingPoint Assurance Measures
AGD_USR.1	User guidance	*UnityOne™ Command Line Interface Reference Version 1.2*; Part Number TECHD-0000000013; Publication Control Number 062503 *UnityOne™ Local Security Manager User Guide Version 1.2*; Part Number: TECHD-0000000014; Manufacturing Revision:A07; Publication Control Number: 021903
ATE_COV.1	Evidence of coverage	UnityOne v1.2 CC test package - June 26 2003.zip.pgp
ATE_FUN.1	Functional testing	UnityOne v1.2 CC test package - June 26 2003.zip.pgp which includes: TippingPoint Technologies, Inc. UnityOne Version 1.2 Functional Specification Manifest Document Version 1.7
ATE_IND.1	Independent testing	Cable & Wireless Test Report
AVA_SOF.1	Strength of TOE security function evaluation	TippingPoint UnityOne™ version 1.2 Vulnerability Assessment v1.3
AVA_VLA.1	Developer vulnerability analysis	TippingPoint UnityOne™ version 1.2 Vulnerability Assessment v1.3

7.3 TOE Strength of Function Claims

The TOE (specifically, the TOE's password mechanism) minimum strength of function claim is SOF-basic. The TOE incorporates user defined authentication tokens (i.e., passwords) that can be analyzed via probabilistic or permutational means. The TOE requires that the minimum password length used to authenticate an entity acting in the Super-User role be equal to or greater than 8 characters. The password must contain at least two alphabetic characters, one numeric character, and one special character.

8 Protection Profile Claims

This ST conforms to the following Protection Profiles:

1. Intrusion Detection System Analyzer Protection Profile, Version 1.1, December 10, 2001;
2. Intrusion Detection System Scanner Protection Profile, Version 1.1, December 10, 2001;
3. Intrusion Detection System Sensor Protection Profile, Version 1.1, December 10, 2001; and
4. Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002.

9 Rationale

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

9.1 RATIONALE FOR IT SECURITY OBJECTIVES

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose this ST. Table 10 demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

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

The O.INTROP objective ensures the TOE has the needed access.

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

The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will be managed appropriately.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitor*s*.

The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

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

The O.PHYCAL provides for the physical protection of the TOE hardware and software.

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

The O.PHYCAL provides for the physical protection of the TOE.

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

The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

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.

The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

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

The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

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.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self- protection.

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

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection.

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

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self- protection.

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.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt 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.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

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

The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

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

The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

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

The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

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

The O.IDSCAN objective counters this threat by requiring a TOE that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change.

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.

The O.IDSCAN objective counters this threat by requiring a TOE that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.

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

The O.IDSCAN objective counters this threat by requiring a TOE that contains a Scanner to collect and store static configuration information that might be indicative of a vulnerability.

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

The O.RESPON objective ensures the TOE reacts to analytical conclusions about 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.

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a 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.

The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

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.

The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data.

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.

The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.

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

The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.

The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

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

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.

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

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.

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

The O.INTEGR objective ensures the protection of data from modification.

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

The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications.

9.2 RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

MULTIPLE CONFORMANCE NOTE: This table is taken from the IDS System PP but the relationship between these security environment parameters and objectives is the same for all four IDS PPs, even though each of these objectives/threats/assumptions/policies may not be present in each of the component PPs.

Table 10 – Relationship of Security Environment to Objectives

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP
A.ACCESS																	X
A.DYNMIC																X	X
A.ASCOPE																	X
A.PROTCT														X			
A.LOCATE														X			
A.MANAGE																X	
A.NOEVIL													X	X	X		
A.NOTRST														X	X		
T.COMINT	X						X	X			X						
T.COMDIS	X						X	X				X					
T.LOSSOF	X						X	X			X						
T.NOHALT		X	X	X			X	X									
T.PRIVIL	X						X	X									
T.IMPCON						X	X	X					X				
T.INFLUX									X								
T.FACCNT										X							
T.SCNCFG		X															
T.SCNMLC		X															
T.SCNVUL		X															
T.FALACT					X												
T.FALREC				X													
T.FALASC				X													
T.MISUSE			X							X							
T.INADVE			X							X							
T.MISACT			X							X							
P.DETECT		X	X							X							
P.ANALYZ				X													
P.MANAGE	X					X	X	X					X		X	X	
P.ACCESS	X						X	X									
P.ACCACT								X		X							
P.INTGTY											X						
P.PROTCT									X					X			

Because the security objectives for the environment are not IT in nature, they need only be mapped to security assurance requirements (SARs). They do not need to be mapped to security functional requirements (SFRs). Security objectives for the environment are:

- O.INSTAL
- O.PHYCAL
- O.CREDEN
- O.PERSON
- O.INTROP

These objectives are satisfied by procedural or administrative measures. Thereby, each of these objectives is addressed through the TOE Administrator and User Guidance (AGD_ADM and AGD_USR) security assurance measures.

9.3 RATIONALE FOR SECURITY REQUIREMENTS

This section demonstrates that the functional components selected for this ST provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

MULTIPLE CONFORMANCE NOTE: This table is taken from the IDS System PP but the relationship between these security functional requirements and objectives is the same for all four IDS PPs, even though these objectives and security functional requirements may not be present in each of the component PPs or may be included in a form that is slightly modified from what is contained in the IDS System PP.

Table 11 – Mapping of Functional Requirements to Objectives

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT
FAU_GEN.1-NIAP-0347										X		
FAU_SAR.1						X						
FAU_SAR.2							X	X				
FAU_SAR.3						X						
FAU_SEL.1						X				X		
FAU_STG.2-NIAP-0422	X						X	X	X		X	
FAU_STG.4									X	X		
FIA_UAU.1							X	X				
FIA_AFL.1-NIAP-0425								X				
FIA_ATD.1								X				
FIA_UID.1							X	X				
FMT_MOF.1	X						X	X				
FMT_MTD.1	X						X	X			X	
FMT_SMF.1							X	X				
FMT_SMR.1								X				
FPT_ITA.1												X
FPT_ITC.1											X	X
FPT_ITI.1											X	X
FPT_RVM.1	X					X		X		X	X	
FPT_SEP.1	X					X		X		X	X	
FPT_STM.1										X		

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT
IDS_SDC.1 IDS_COL.1 IDS_SCN.1		X	X									
IDS_ANL.1				X								
IDS_RCT.1					X							
IDS_RDR.1						X	X	X				
IDS_STG.1	X						X	X	X		X	
IDS_STG.2									X			

The following discussion provides detailed evidence of coverage for each security objective.

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

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2-NIAP-0422]. The Analyzer, Scanner, Sensor and System are required to protect the Analyzer, Scanner, Sensor and System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer, Scanner, Sensor and System may query and add Analyzer, Scanner, Sensor and System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1].

The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

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.

A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC.1, IDS_SCN.1, IDS_COL.1].

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.

A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_SDC.1, IDS_SCN.1, IDS_COL.1].

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).

The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

O.RESPON The TOE must respond appropriately to analytical conclusions.

The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].

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

The TOE must provide the ability to review and manage the audit trail of the Analyzer, Scanner, Sensor and System [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The Analyzer, Scanner, Sensor and System must provide the ability for authorized administrators to view all Analyzer, Scanner, Sensor and System data collected and produced [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer, Scanner, Sensor and System are required to restrict the review of Analyzer, Scanner, Sensor and System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2-NIAP-0422]. The Analyzer, Scanner, Sensor and System are required to protect the Analyzer, Scanner, Sensor and System data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1, FMT_SMF.1]. Only authorized administrators of the Analyzer, Scanner, Sensor and System may query and add Analyzer, Scanner, Sensor and System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_SMF.1].

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

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer, Scanner, Sensor and System are required to restrict the review of Analyzer, Scanner, Sensor and System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2-NIAP-0422]. The Analyzer, Scanner, Sensor and System are required to protect the Analyzer, Scanner, Sensor and System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1, FMT_SMF.1]. The TOE will monitor the number of unsuccessful authentication attempts and, when the defined limit of unsuccessful attempts has been reached, prevent successful authentication for that entity until an authorized administrator takes some action to make authentication possible [FIA_AFL.1-NIAP-0425]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer, Scanner, Sensor and System may query and add Analyzer, Scanner, Sensor and System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMF.1, FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

O.OFLOWS The TOE must appropriately handle potential audit and Analyzer, Scanner, Sensor and System data storage overflow*s*.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2-NIAP-0422]. The TOE must prevent the loss of audit data in the event its audit trail is full [FAU_STG.4]. The Analyzer, Scanner, Sensor and System are required to protect the Analyzer, Scanner, Sensor and System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The Analyzer, Scanner, Sensor and System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2].

O.AUDITS The TOE must record audit records for data accesses and use of the Analyzer, Scanner, Sensor and System functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1-NIAP-0347]. The TOE must provide the capability to select which security-relevant events to audit [FAU_SEL.1]. The TOE must prevent the loss of collected data in the event that its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

O.INTEGR The TOE must ensure the integrity of all audit and Analyzer, Scanner, Sensor and System data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2-NIAP-0422]. The Analyzer, Scanner, Sensor and System are required to protect the Analyzer, Scanner, Sensor and System data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the Analyzer, Scanner, Sensor and System may query or add audit and Analyzer, Scanner, Sensor and System data [FMT_MTD.1]. The Analyzer, Scanner, Sensor and System must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1].

O.EXPORT When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the Analyzer, Scanner, Sensor and System data.

The TOE must make the collected data available to other IT products [FPT_ITA.1]. The TOE must protect all data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1].

9.4 RATIONALE FOR TOE SUMMARY SPECIFICATION

The following table represents a mapping between the security functions in this ST to their related TOE security functional requirements and provides a rationale for how each security function meets the corresponding security functional requirement.

Table 12 – Mapping of Security Functional Requirements to TOE Security Functions

Functional Requirement:	TOE Security Functions:	Rationale:
Functional Requirements for the TOE		
FAU_GEN.1	Audit Data Generation	The Audit Data Generation function satisfies this requirement by providing audit data generation for the UnityOne™ components.

Functional Requirement:	TOE Security Functions:	Rationale:
FAU_SAR.1	Audit Review	The Audit Review function satisfies this requirement by providing the capability for UnityOne™ superusers to view the TOE's audit data.
FAU_SAR.2	Restricted Audit Review	The Restricted Audit Review function satisfies this requirement by prohibiting unauthorized users access to audit records.
FAU_SAR.3	Selectable Audit Review	The Selectable Audit Review function satisfies this requirement by providing authorized users with the ability to perform sorting of audit data based on various parameters.
FAU_SEL.1	Selective Audit	The Selective Audit function satisfies this requirement by allowing authorized users to include or exclude auditable events from the set of auditable events.
FAU_STG.2	Guarantees of Audit Data Availability	The Guarantees of Audit Data Availability function satisfies this requirement by protecting audit records from unauthorized deletion, detecting modification to audit records, and maintaining audit records in the event of storage exhaustion or attack.
FAU_STG.4	Prevention of Audit Data Loss	The Prevention of Audit Data Loss function satisfies this requirement by overwriting the oldest stored audit records and sending an alarm if the audit trail is full.
FIA_UAU.1	Timing of Authentication	The Timing of Authentication function satisfies this requirement by allowing the initiation of the login process to be provided to a user prior to being authenticated using the password-based authentication mechanism, and by not allowing any other actions to be performed prior to successful authentication.
FIA_AFL.1	Authentication Failure Handling	The Authentication Failure Handling function satisfies this requirement by tracking the number of unsuccessful authentication attempts a user has tallied and, if this number reaches a pre-set limit, locking out this account until it is unlocked by an authorized superuser.
FIA_ATD.1	User Attribute Definition	The User Attribute Definition function satisfies this requirement by maintaining a list of security attributes for each user of the TOE.
FIA_UID.1	Timing of Identification	The Timing of Identification function satisfies this requirement by requiring each user to be successfully identified before allowing the user to perform any other action.
FMT_MOF.1	Management of Security Functions Behavior	The Management of Security Functions Behavior function satisfies this requirement by restricting access to modify the behavior of or change the configurations of the security functions for authorized TOE administrators.
FMT_MTD.1	Management of TSF Data	The Management of TSF Data function satisfies this requirement by restricting access to query and add IDS Analyzer, Scanner, Sensor and System data to superusers and administrators.
FMT_SMF.1	Specification of Management Functions	The Specification of Management Functions function satisfies this requirement by requiring the ST author to identify the security management functions that the TSF is capable of performing.
FMT_SMR.1	Security Roles	The Security Roles function satisfies this requirement by providing roles and associating each user to a role.
FPT_ITA.1	Inter-TSF Availability within a Defined Availability Metric	The Inter-TSF Availability within a Defined Availability Metric function satisfies this requirement by ensuring that requested audit and IDS Analyzer, Scanner, Sensor and System data is provided to a remote trusted IT product within 60 seconds under normal operating conditions.

Functional Requirement:	TOE Security Functions:	Rationale:
FPT_ITC.1	Inter-TSF Confidentiality During Transmission	The Inter-TSF Confidentiality During Transmission function satisfies this requirement by restricting the disclosure of information in transit through the use of SSH and SSL.
FPT_ITI.1	Inter-TSF Detection of Modification	The Inter-TSF Detection of Modification function satisfies this requirement by detecting the modification of information in transit through the use of a message authentication code (MAC). Additionally, if a modification is detected within a session then the data is retransmitted.
FPT_RVM.1	Non-bypassability of the TSP	The Non-bypassability of the TSP function satisfies this requirement by ensuring that TSP enforcement functions (e.g. identification & authentication procedures) are invoked and succeed before each function is allowed to proceed.
FPT_SEP.1	TSF Domain Separation	The TSF Domain Separation function satisfies this requirement by ensuring that the TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. The TSF also enforces separation between the security domains of subjects in the TSC.
FPT_STM.1	Reliable Time Stamps	The Reliable Time Stamps function satisfies this requirement by ensuring that the TOE has access to a reliable time stamp that is maintained by the operating system and can be changed only by authorized superusers.
Explicitly Stated Requirements for the TOE		
IDS_SDC.1	System Data Collection	The System Data Collection function satisfies this requirement by performing IDS System data collection for the UnityOne™.
IDS_SCN.1	Scanner Data Collection	The Scanner Data Collection function satisfies this requirement by performing IDS Scanner data collection for the UnityOne™.
IDS_COL.1	Sensor Data Collection	The Sensor Data Collection function satisfies this requirement by performing IDS Sensor data collection for the UnityOne™.
IDS_ANL.1	Analyzer Analysis	The Analyzer Analysis function satisfies this requirement by performing signature analysis functions on all IDS data received. Additionally, other information is recorded within each analytical result.
IDS_RCT.1	Analyzer React	The Analyzer React function satisfies this requirement by sending and Email alert when an intrusion is detected.
IDS_RDR.1	Restricted Data Review	The Restricted Data Review function satisfies this requirement by only allowing authorized users to read IDS Analyzer, Scanner, Sensor and System data in a suitable format.
IDS_STG.1	Guarantee of Analyzer, Scanner, Sensor and System Data Availability	The Guarantee of Analyzer, Scanner, Sensor and System Data Availability function satisfies this requirement by protected stored IDS data from unauthorized deletion or modification.
IDS_STG.2	Prevention of Analyzer, Scanner, Sensor and System Data Loss	The Prevention of Analyzer, Scanner, Sensor and System Data Loss function satisfies this requirement by overwriting the oldest stored IDS data and sending an alarm if storage capacity is reached.

9.5 RATIONALE FOR ASSURANCE REQUIREMENTS

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software

engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the IDS Analyzer, Scanner, Sensor, and System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the IDS Analyzer, Scanner, Sensor, and System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The chosen assurance level was also selected for conformance with the Intrusion Detection System family of Protection Profiles and to meet the vendor's customer requirements.

Configuration Management – The Configuration Management documentation provides a description of automation tools used to control the configuration items and how they are used at the TippingPoint and vendor support development facilities. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

Delivery and Operation – The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by TippingPoint to protect against TOE modification during product delivery. The Installation Documentation provided by TippingPoint details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

Development – The UnityOne™ Design documentation consist of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Correspondence Demonstration

Guidance Documentation – The TippingPoint Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The Administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. TippingPoint provides single versions of documents which address the Administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

Tests – There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. TippingPoint's Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

Vulnerability and TOE Strength of Function Analyses – A Vulnerability Analysis is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Strength of TOE Security Function evaluation
- Developer Vulnerability Analysis

9.6 RATIONALE FOR EXPLICITLY STATED REQUIREMENTS

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

The TOE is claiming conformance to four U.S. Government-certified Protection Profiles. Because these PPs are certified, the writers of this ST operate with the assumption that the rationales presented in each of these PPs are valid and complete. The writers of this ST consequently trust that the assurance requirements presented in each of the four PPs are applicable and appropriate to support any explicitly stated TOE SFRs that appear within these PPs.

9.7 RATIONALE FOR STRENGTH OF FUNCTION

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in Section 4.

9.8 RATIONALE FOR SATISFYING ALL DEPENDENCIES

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 13 lists each requirement from the four Protection Profiles to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 13 – Functional Requirements Dependencies

Functional Component	Dependency	Included
FAU_GEN.1-NIAP-0347	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1-NIAP-0347	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1-NIAP-0347 and FMT_MTD.1	Yes
FAU_STG.2-NIAP-0422	FAU_GEN.1-NIAP-0347	Yes
FAU_STG.4	FAU_STG.2-NIAP-0422	Yes
FIA_UAU.1	FIA_UID.1	Yes
FIA_AFL.1	FIA_UAU.1[15]	Yes
FMT_MOF.1	FMT_SMF.1 and FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1 and FMT_SMR.1	Yes
FMT_SMR.1	FIA_UID.1	Yes

[15] FIA_UAU.1 (timing of authentication) is dependent on FIA_UID.1 (timing of identification). Both requirements are met.

10 Glossary of Terms

CC	Common Criteria
CLI	Command line interface
CM	Configuration management
FIFO	First in, first out
FTP	File transfer protocol
HTTPS	Secure hypertext transfer protocol
IDS	Intrusion detection system
IP	Internet protocol
IT	Information technology
LAN	Local area network
LSM	Local Security Manager
MAC	Message authentication code
MP	Management processor
MZDM	Multi-zone defense module
ND	Network Discovery
NIPS	Network-based intrusion prevention system
NSA	National Security Agency
OS	Operating system
PEM	Power entry module
PP	Protection Profile
RU	Rack-unit
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMTP	Simple mail transfer protocol
SSH	Secure Shell
SSL	Secure sockets layer

ST	Security Target
TCP	Transmission control protocol
TOE	Target of Evaluation
TLS	Transport layer security
TPT	TippingPoint Technologies, Inc.
TSE	Threat suppression engine
TSF	Target of Evaluation (TOE) security function
TSP	Target of Evaluation (TOE) security policy

Appendix A: Interpretations

From the Common Criteria Evaluation and Validation Scheme (CCEVS) Web site (http://niap.nist.gov/cc-scheme/PUBLIC/thequeue.html):

"One of the responsibilities of the NIAP Interpretations Board (NIB) is the development of NIAP interpretations (NIs) of the Common Criteria (CC) and the Common Evaluation Methodology (CEM). The sources of NIs include (1) issues that are raised from interim decisions produced by CCEVS for individual evaluations (called Observation Decisions), and (2) sections of the CC and CEM that the NIB has found to be confusing based on its review during NIB meetings. As part of the NI development process, the NIB distributes the proposed NIs for public review and comment."

Approved NIs (and other publicly available NIB database entries) are available at the following site:

http://niap.nist.gov/cc-scheme/PUBLIC/index.html

Several interpretations have been applied within this Security Target. This Appendix serves to identify those relevant interpretations and their effects.

FAU_GEN.1-NIAP-0347

ISSUE:
In the FIA_UID family, the CC specifically calls for the inclusion of the user identity in the audit record, even though it is possible that a user, confused by the I&A protocol, provides a password when the user identity is requested. There may be other instances in the CC where the audit requirement either explicitly or implicitly requires data to be logged that might be sensitive. Yet, the example given in CC Part 2, Annex C, paragraph 558, under FAU_GEN, suggests that the CC's intention was to allow the PP/ST author to exclude sensitive data from the required data to be logged. However, this paragraph is in a non-normative portion of the CC. Please clarify.

STATEMENT:
The CC should allow PP/ST authors to selectively exempt specific sensitive attribute data from being placed into audit records while still being able to claim compliance with one of the three levels of selecting security-relevant audit events (minimum, basic, detailed).

SPECIFIC INTERPRETATION:
To address this interpretation, the following changes are made to CC v2.1, Part 2:

FAU_GEN.1-NIAP-0410 is relabeled as FAU_GEN.1-NIAP-0347. Unless otherwise noted in these changes, all normative and informative material associated with FAU_GEN.1-NIAP-0410 is incorporated unchanged into FAU_GEN.1-NIAP-0347, and all references to FAU_GEN.1-NIAP-0410 in the CC, CEM, or other Common Criteria documentation are changed to refer to FAU_GEN.1-NIAP-0347.

Subclause 3.2, FAU_GEN.1, is changed as follows:
FAU_GEN.1.2-NIAP-0410-0347 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 timetype, based on the auditable event definitions of the functional components included in the PP/ST, [selection: [assignment: other audit relevant information, excluding sensitive fields], "no other information"]

The following paragraph is added in Subclause C.2, after paragraph 561:

A PP/ST author may also decided that certain information called out in the audit section for a functional component may be sensitive information, due to the design of the system or usage patterns. The PP/ST author should provide justification for any information called out for auditing in the component that has been removed for sensitivity reasons.

The following changes are made to Subclause C.2, paragraph 569:

For FAU_GEN-NIAP-0410-0347.1.1b, the PP/ST author should assign, for each auditable events included in the PP/ST, a list of other audit relevant information to be included in audit event records. Sensitive information may be excluded with a convincing justification.

FAU_STG.2-NIAP-0422

ISSUE:

There is a confusion introduced with the Part 2 usage of the term "Audit Records", as opposed to the term "Audit Trail". The Part 2 Annex, Section C.6, clarifies by implication that the term "Audit Records" refers to the records in the audit trail, as the application notes refer almost exclusively to the "audit trail" or the records in the trail. The problem with the use of the term "audit records" is that audit records may appear outside the audit trail, for example, after they have been retrieved through a selection.

STATEMENT:

In the .1 and .2 elements of the FAU_STG.1 and FAU_STG.2 components, the phrase "audit records" refers to audit records stored in the "audit trail," as described in the Part 2 Annex. However, the use of the phrase "audit records" in this way does not preclude the actions specified as acceptable in FAU_STG.2.3, FAU_STG.3, and FAU_STG.4.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to the CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

FAU_STG.1 is relabeled as FAU_STG.1-NIAP-0422. Unless otherwise noted in these changes, all normative and informative material associated with FAU_STG.1 is incorporated unchanged into FAU_STG.1-NIAP-0422, and all references to FAU_STG.1 in the CC, CEM, or other Common Criteria documentation is changed to refer to FAU_STG.1-NIAP-0422.

The elements in FAU_STG.1 are replaced with the following elements:

FAU_STG.1.1-NIAP-0422: The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2-NIAP-0422: The TSF shall be able to [selection: prevent, detect] modifications to the audit records in the audit trail.

FAU_STG.2 is relabeled as FAU_STG.2-NIAP-0422. Unless otherwise noted in these changes, all normative and informative material associated with FAU_STG.2 is incorporated unchanged into FAU_STG.2-NIAP-0422, and all references to FAU_STG.2 in the CC, CEM, or other Common Criteria documentation is changed to refer to FAU_STG.2-NIAP-0422.

Elements FAU_STG.2.1 and FAU_STG.2.2 are replaced with the following elements:

FAU_STG.2.1-NIAP-0422: The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2-NIAP-0422: The TSF shall be able to [selection: prevent, detect] modifications to the audit records in the audit trail.

FIA_AFL.1-NIAP-0425

ISSUE:

In element FIA_AFL.1.1, the PP/ST author should specify the default number of unsuccessful authentication attempts that, when met or surpassed, will cause the TSF to perform some action or actions. Part 2, Subclause G.1, paragraph 958 states that the PP/ST author may specify that the number is: "an authorised administrator configurable number". However, the wording used in element FIA_AFL.1.1 ("[assignment: number]") does not allow a phrase to be inserted.

STATEMENT:
The number of unsuccessful authentication attempts is permitted to be specifiable by an administrator.

SPECIFIC INTERPRETATION:
To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

FIA_AFL.1 is relabeled as FIA_AFL.1-NIAP-0425. Unless otherwise noted in these changes, all normative and informative material associated with FIA_AFL.1 is incorporated unchanged into FIA_AFL.1-NIAP-0425, and all references to FIA_AFL.1 in the CC, CEM, or other Common Criteria documentation is changed to refer to FIA_AFL.1-NIAP-0425.

FIA_AFL.1.1 is replaced by the following:

> FIA_AFL.1.1-NIAP-0425: The TSF shall detect when [selection: [assignment: positive integer number], "an authorised administrator configurable integer"] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

In Subclause G.1, FIA_AFL.1, Operations, the following is added before the "Assignment" operation:

> Selection:
> In FIA_AFL.1.1-NIAP-0425, the PP/ST author should select either the assignment of a positive integer, or the phrase "an authorised administrator configurable integer".

In Subclause G.1, FIA_AFL.1, Operations, paragraph 958 (the first "Assignment") is replaced with the following:

> In FIA_AFL.1.1-NIAP-0425, if the assignment of a positive integer is selected, the PP/ST author should specify the default number (positive integer) of unsuccessful authentication attempts that, when met or surpassed, will trigger the events. The PP/ST author may specify that the number is: "an authorised administrator configurable number".

Annex G.1, Paragraph 959 is modified to reference FIA_AFL.1.1-NIAP-0425, instead of FIA_AFL.1.1.

FMT_SMF.1-INTERP-065

Final Interpretation for RI # 65 - No component to call out security function management
Effective Date: July 31, 2001

Issue
The CC words for the FMT class specify restrictions on roles that may perform security management functions, but fail to provide explicit requirements that the TSF provide the security management functions upon which the restrictions apply. A common argument is that restricting the functions implicitly requires that they be provided.

Interpretation
A new family is added to the FMT Class in CC Part 2 that allows specification of management functions to be provided by the TOE.

Specific Changes
To address this interpretation, the following changes are made to CC Part 2:

The following family is added to Clause 8, Class FMT:

8.x Specification of Management Functions (FMT_SMF)

Family Behaviour

This family allows the specification of the management functions to be provided by the TOE. Management functions provide TSFI that allow administrators to define the parameters that control the operation of security-related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes. Management functions also include those functions performed by an operator to ensure continued operation of the TOE, such as backup and recovery. This family works in conjunction with the other components in the FMT class: the component in this family calls out the management functions, and other families in FMT restrict the ability to use these management functions.

Component Levelling

FMT_SMF.1 Specification of Management Functions requires that the TSF provide specific management functions.

Management: FMT_SMF.1

There are no management activities foreseen for this component.

Audit: FMT_SMF.1

The following events should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Use of the management functions.

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

Dependencies: No Dependencies

The following subclause is added to Annex H, Security Management:

H.x Specification of Management Functions (FMT_SMF)

This family allows the specification of the management functions to be provided by the TOE. Each security management function that is listed in fulfilling the assignment is either security attribute management, TSF data management, or security function management.

FMT_SMF.1 Specification of Management Functions

This component specifies the management functions to be provided.

Application Note

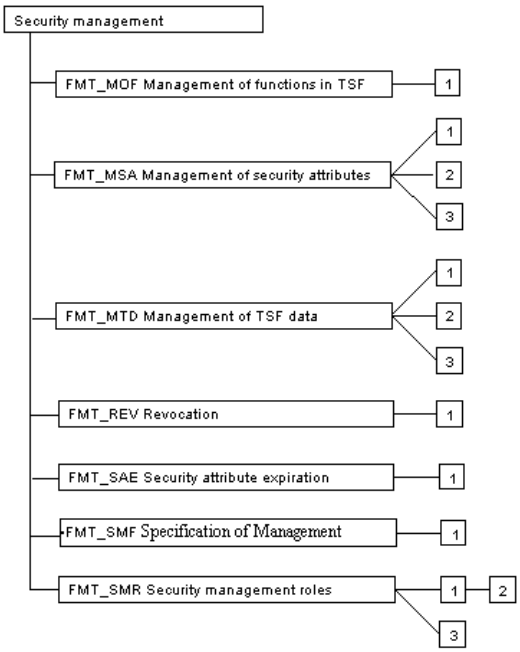
PP/ST authors should consult the “Management” sections for components included in their PP/ST to provide a basis for the management functions to be listed via this component.

Operations

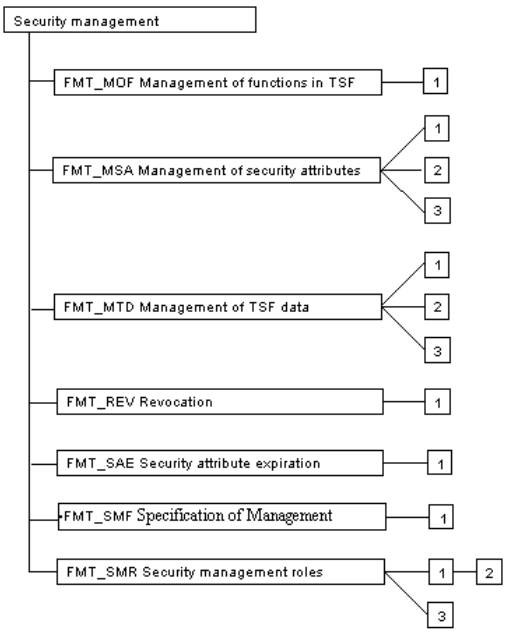
Assignment:

In FMT_SMF.1, the PP/ST author should specify the management functions to be provided by the TSF, either security attribute management, TSF data management, or security function management.

Clause 8, Figure 8.1, is modified to show an additional family, FMT_SMF Specification of Management Functions, with one component.



Clause H, Figure H.1, is modified to show an additional family, FMT_SMF Specification of Management Functions, with one hierarchical component.



The following dependency is added to FMT_MOF.1: FMT_SMF.1 Specification of Management Functions

The following dependency is added to FMT_MSA.1: FMT_SMF.1 Specification of Management Functions

The following dependency is added to FMT_MTD.1: FMT_SMF.1 Specification of Management Functions