Security Target

McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5

Document Version 1.1

September 9, 2011

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ST Revision	1.1
ST Publication Date	September 9, 2011
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
TOE Type	Intrusion Prevention System (IPS)

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by *italicized* text.
- 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**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by underlined text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the terms and acronyms used in this document:

TERM	DEFINITION
Agent(s)	Agent(s) refer to the HIP software for systems running the Windows operating system.
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CM	Configuration Management
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
Exception	Defines a set of attributes that instructs the Agent to not enforce a rule or policy, resulting in an Event not being generated.
GB	Giga-Byte
GUI	Graphical User Interface
HIP	Host Intrusion Prevention
I&A	Identification and Authentication

TERM	DEFINITION
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
JRE	Java Runtime Environment
MB	Mega-Byte
NIAP	National Information Assurance Partnership
OS	Operating System
OSP	Organizational Security Policy
PC	Personal Computer
PD	Precedent Decision
PDC	Primary Domain Controller
Policy File	Each Signature is assigned a Security Level. The Policy File defines the Reaction to take for a specific Security Level. Each Policy File entry includes the Reaction to take if a signature of that severity level occurs.
PP	Protection Profile
RAM	Random Access Memory
Reaction	A Reaction is defined in a Policy File. It defines the action (Prevent, Log, or Ignore) the Agent is to take per Event Severity Level (High, Medium, Low, Information).
Severity Level	The available Severity Levels available are: High, Medium, Low, or Information.
SFR	Security Functional Requirement
Signature	Signatures are patterns that indicate a potential security violation.
Signature File	Agents are installed with a Signature File that contains a list of Signatures. The Agents intercept operating system calls and network packets and compare them to the Signatures File
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
VGA	Video Graphics Array

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

The TOE is a host-based intrusion prevention system designed to protect system resources and applications, and includes a host based management system that provides management and monitoring functionality. HIP works to intercept system calls prior to their execution and network traffic prior to their processing. If the HIP Agent determines that a call or packet is symptomatic of malicious code, the call or packet can be blocked and/or an audit log created; if it determines that a call or packet is safe, it is allowed.

McAfee Agent and HIP software is installed on the host to be protected. HIP software is operating system specific; only the Windows version is included in this evaluation.

ePO distributes and manages agents that reside on client systems. A centralized but distributed architecture allows the HIP software to be centrally managed and yet decrease network traffic required to manage clients. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

Based upon per-user permissions, users may configure the policies to be enforced on individual systems (executing the HIP software).

1.7 TOE Description

1.7.1 HIP Agent

The HIP Agent for Windows (hereafter referred to as Agent) provides a protection layer that identifies and prevents malicious attempts to compromise a host. Agent software is installed on the host to be protected. Agents are operating system specific; only the Windows Agent is included in this evaluation.

1.7.2 ePolicy Orchestrator (ePO)

In addition to the Agent, the TOE includes ePolicy Orchestrator (ePO). ePO distributes and manages agents that reside on client systems. A centralized but distributed architecture allows the Agent software to be centrally managed and yet decrease network traffic required to manage clients. ePO provides:

- the management interface and functionality for the administrators of the TOE
- centralized audit collection and review functionality
- provides HIP-specific functions for policy management.

The TOE does include McAfee Host Intrusion Prevention for Desktops as well as McAfee Host Intrusion Prevention for Servers. Both are the same software/code base; the latter provides SQL and IIS protection when a server operating system is detected during install

1.7.3 McAfee Agent

The McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed system. It provides common communication functionality between ePO and all of McAfee's product-specific agents (such as HIP).

1.7.4 Physical Boundary

The TOE is a software TOE and includes:

1. The ePO application executing on a dedicated server

2. The McAfee Agent and HIP software on each system to be protected

Note specifically that the hardware, operating systems and third party support software (e.g. DBMS) on each of the systems are excluded from the TOE boundary.

In order to comply with the evaluated configuration, the following hardware and software components should be used:

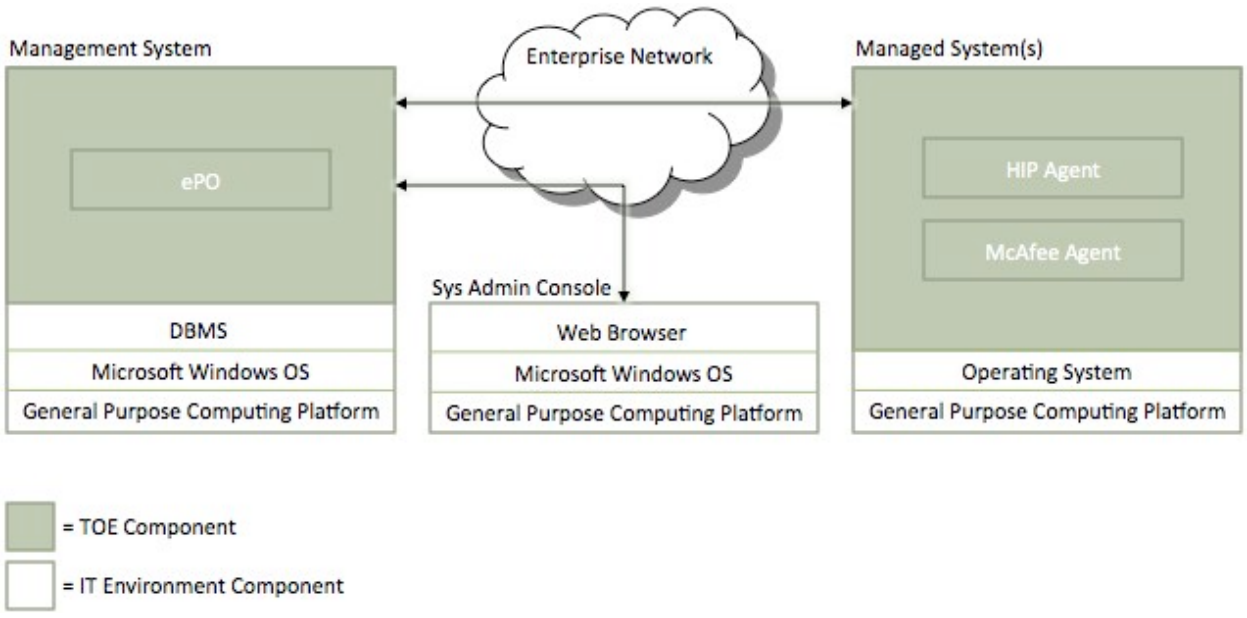
TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	HIP Agent 8.0 (for Servers and for Desktops) ePolicy Orchestrator 4.5 Patch 3 McAfee Agent 4.5[1] Patch 2 Database Capacity Monitor Extension 1.0
IT Environment	Specified in the following: • Table 4 – Management System Component Requirements • Table 5 – Supported Agent Platforms • Table 6 – Agent Platform Hardware Requirements

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration consists of a single instance of the management system (with ePO) and one or more instances of managed systems (with McAfee Agent and the HIP Agent).

ePO supports both ePO authentication and Windows authentication of user account credentials. The evaluated configuration requires the use of ePO authentication only.

The following figure presents an example of an operational configuration. The shaded elements in the boxes at the top of the figure represent the TOE components.



[1] McAfee Agent 4.5 is shipped/packaged with ePO 4.5. From a clean installation, no additional steps are necessary to install McAfee Agent 4.5.

Figure 1 – TOE Boundary

The functionality not included in the evaluation is itemized below:

1. Firewall functionality (some government users require firewall functionality to be disabled unless it has been evaluated against one of the firewall PPs at EAL4 or Medium Robustness). Application Blocking functionality is associated with the firewall functionality and is also excluded.
2. Custom signatures and policies.
3. Importing configurations.
4. HIP Solaris Agents.
5. HIP Linux Agents.

1.7.5 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

The platform on which the ePO software is installed must be dedicated to functioning as the management system. ePO operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients). The TOE requires the following hardware and software configuration on this platform.

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium III-class or higher; 1GHz or higher
Memory	1 GB RAM
Free Disk Space	1 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2003 Enterprise with Service Pack 2 or later Windows Server 2003 Standard with Service Pack 2 or later Windows Server 2003 Web with Service Pack 2 or later Windows Server 2003 R2 Enterprise with Service Pack 2 or later Windows Server 2003 R2 Standard with Service Pack 2 or later Windows Server 2008 Enterprise Windows Server 2008 Standard
DBMS	SQL Server 2005 SQL 2005 Express SQL 2008 SQL 2008 Express
Additional Software	Firefox 3.0 Microsoft Internet Explorer 7.0 or 8.0

COMPONENT	MINIMUM REQUIREMENTS
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network

Table 4 – Management System Component Requirements

The McAfee Agent and HIP Agent execute on one or more managed systems. The supported platforms for these components are:

SUPPORTED AGENT OS	PLATFORM
Windows XP Professional with SP2, SP3	X86 platforms
Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (all editions)	X86 and X64 platforms
Windows Vista SP1 (Business, Enterprise, Ultimate editions)	X86 and X64 platforms
Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (all editions)	X86 and X64 platforms
Windows 7 (Professional, Enterprise, Ultimate editions)	X86 and X64 platforms

Table 5 – Supported Agent Platforms

The minimum hardware requirements for the agent platforms are specified in the following table:

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
Memory	20MB RAM
Free Disk Space	80MB
Network Card	Ethernet, 10Mb or higher

Table 6 – Agent Platform Hardware Requirements

The management system is accessed from remote systems via a browser. The supported browsers are Microsoft Internet Explorer 6.0 with Service Pack 1 or later or Microsoft Internet Explorer 7.0.

1.7.6 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Audit	The TOE generates audit records upon detection of a potential security violation or system configuration events. The audit records can be viewed by an authorized user. The TOE audit functionality includes the ability to configure what auditable events generate audit records.
Identification and Authentication	The TOE requires administrative users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.

TSF	DESCRIPTION
Management	The TOE's Management Security Function provides administrator functionality that enables a human user to configure and manage TOE components. Configuration functionality includes enabling a user to modify TSF Data. Management functionality includes invocation of TOE functions that effect security functions and security function behavior.
System Protection	The Agents are host based intrusion prevention systems designed to protect system resources and applications from attacks. The Agents accomplish this by intercepting operating system calls and comparing them to signatures symptomatic of known attacks and behavioral rules. The Agents also inspect network traffic by comparing packets to signatures symptomatic of known attacks. If a potential security violation is detected, the system call or network traffic may be allowed to proceed or be blocked. An audit event may also be generated.

Table 7 – Logical Boundary Descriptions

1.7.7 TOE Data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information. Security attributes enable the TOE to enforce the security policy. Authentication data enables the TOE to identify and authenticate users.

TSF Data	Description	AD	UA	GE
Application Protection Lists	List of processes that are explicitly enabled or disabled for performing user-level hooking			✓
Audit Filter Configuration	A list of audits that are filtered (not generated) by the TOE.			✓
Contacts	A list of email addresses that ePolicy Orchestrator uses to send email messages to specified users in response to events.			✓
Dashboards	Collections of chart-based queries that are refreshed at a user-configured interval.			✓
Email Server	SMTP server name and port used to send email messages for notifications. Credentials may optionally be specified for authenticated interactions.			✓
ePO User Accounts	ePO user name, authentication configuration, enabled status, Global Administrator status and permission sets for each user authorized to access TOE functionality on the management system.	✓		
Event Filtering	Specifies which events are forwarded to the server from the agents on the managed systems.			✓
Exceptions	Mechanism to refine the signature matches to eliminate false positives			✓
Global Administrator Status	Individual ePO user accounts may be configured as Global Administrators, which means they have read and write permissions and rights to all operations.		✓	

TSF Data	Description	AD	UA	GE
Groups	Node on the hierarchical System Tree that may contain subordinate groups or systems.			✓
IPS Options	Per-Agent mode for operation of the IPS processing, may be ON for normal operation or configured for Adaptive mode			✓
IPS Policies	Used to configure the reaction to signature matches			✓
IPS Protection Policies	Per-Agent reaction specified for each of the severity levels that can be specified in signatures.			
Notification Rules	Rules associated with groups or systems used to generate alerts upon receipt of specified events			✓
Permission	A privilege to perform a specific function.		✓	
Permission Set	A group of permissions that can be granted to any users by assigning it to those users' accounts.		✓	
Queries	Configurable objects that retrieve and display data from the database.			✓
Server Settings	Control how the ePolicy Orchestrator server behaves.			✓
Signatures	Collection of system call events or network traffic indicative of malicious code			✓
System Event Audit Configuration	Configuration to determine which actions create audit events			✓
System Information	Information specific to a single managed system (e.g. internet address) in the System Tree.			✓
System Tree	A hierarchical collection of all of the systems managed by ePolicy Orchestrator.			✓
Trusted Applications	Mechanism to refine the signature matches to eliminate false positives			✓

Table 8 – TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied operating systems.

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to direct the system calls and network packets to the TOE for examination.

The TOE is implemented with well-defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any

actions within the TOE. The TOE tracks multiple users by sessions and ensures the access privileges of each are enforced.

The server hardware provides virtual memory and process separation, which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Communication between the components relies upon cryptographic functionality provided by the OS or third party software (operational environment) to protect the information exchanged from disclosure or modification.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile Conformance Claim

The TOE claims strict conformance to the *U.S. Government Protection Profile Intrusion Detection System - System for Basic Robustness Environments*, Version 1.7, dated July 25, 2007.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 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.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
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.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

Table 9 – Threats Addressed by the TOE

The following table identifies threats to the managed systems that may be indicative of vulnerabilities in or misuse of IT resources:

THREAT	DESCRIPTION

THREAT	DESCRIPTION
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
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.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
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.

Table 10 – Threats Addressed by the IT Environment

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 11 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment

only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
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.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Table 12 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

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

Table 13 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.INTROP	The TOE is interoperable with the IT System it monitors

OBJECTIVE	DESCRIPTION
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

Table 14 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE / THREAT / ASSUMPTION	O.ACCESS	O.AUDITS	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.CREDEN	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL	OE.PROTECT	OE.SD_PROTECTION	OE.TIME
A.ACCESS																✓					
A.ASCOPE																✓					
A.DYNMIC																✓	✓				
A.LOCATE																		✓			
A.MANAGE																	✓				
A.NOEVIL														✓	✓			✓			
A.NOTRUST														✓				✓			
A.PROTCT																		✓			
P.ACCACT		✓			✓								✓								✓
P.ACCESS	✓				✓					✓		✓								✓	
P.ANALYZ				✓																	
P.DETECT		✓				✓	✓														✓
P.INTGTY								✓													
P.MANAGE	✓		✓		✓					✓				✓	✓		✓				
P.PROTCT									✓									✓	✓		
T.COMDIS	✓				✓					✓									✓		
T.COMINT	✓				✓			✓		✓									✓		
T.FACCNT		✓																			
T.FALACT											✓										

OBJECTIVE / THREAT / ASSUMPTION	O.ACCESS	O.AUDITS	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.CREDEN	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL	OE.PROTECT	OE.SD_PROTECTION	OE.TIME
T.FALASC				✓																	
T.FALREC				✓																	
T.IMPCON	✓		✓		✓										✓						
T.INADVE							✓														
T.INFLUX									✓											✓	
T.LOSSOF	✓				✓			✓		✓											
T.MISACT							✓														
T.MISUSE							✓														
T.NOHALT	✓			✓	✓	✓	✓														
T.PRIVIL	✓				✓					✓											
T.SCNCFG						✓															
T.SCNMLC						✓															
T.SCNVUL						✓															

Table 15 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.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 OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
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 OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRUST	The TOE can only be accessed by authorized users. The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
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 OE.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.AUDIT_SORT objective supports this policy by providing a mechanism for administrators to effectively review the audit logs.
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 OE.AUDIT_PROTECTION and OE.SD_PROTECTION objectives counter this threat via IT Environment protections of the audit trail. The O.PROTCT objective addresses this policy by providing TOE self-protection.
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.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. The OE.TIME objective supports this policy by providing a time stamp for insertion into the audit records.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
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.MANAGE	The TOE shall only be managed by authorized users. The OE.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 OE.INSTAL objective supports the OE.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 OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.
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 OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment.
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.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
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. The OE.PROTECT objective supports the TOE protection from the IT Environment.
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.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.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
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.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.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.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.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE to collect Sensor data.
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. The OE.SD_PROTECTION objective counters this threat via IT Environment protections of the audit trail.
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.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE to collect Sensor data.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE to collect Sensor data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
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.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 to 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 to 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 to collect and store static configuration information that might be indicative of a vulnerability.

Table 16 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 IDS Class of SFRs

All of the components in this section are taken from the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This class of requirements is taken from the IDS System PP to specifically address the data collected and analysed by an IDS scanner and analyzer. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of system data and provide for requirements about collecting, reviewing and managing the data.

5.1.1 IDS_SDC.1 System Data Collection

Management: IDS_SDC.1

The following actions could be considered for the management functions in FMT:

a) Configuration of the events to be collected

Audit: IDS_SDC.1

There are no auditable events foreseen.

IDS_SDC.1 System Data Collection

Hierarchical to:	No other components
Dependencies:	No dependencies
IDS_SDC.1.1	The System shall be able to collect the following information from the targeted IT System resource(s): a) [selection: *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) [assignment: *other specifically defined events*].
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 the table below:

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Startup and shutdown	None
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, source address, destination address
IDS_SDC.1	Startup and shutdown of audit functions	None
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Table 17 – System Data Collection Events and Details

Application Note: The rows in this table must be retained that correspond to the selections in IDS_SDC.1.1 when that operation is completed. If additional events are defined in the assignment in IDS_SDC.1.1, then corresponding rows should be added to the table for this element.

5.1.2 IDS_ANL.1 Analyzer Analysis

Management: IDS_ANL.1

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed

Audit: IDS_ANL.1

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

a) Minimal: Enabling and disabling of any of the analysis mechanisms

IDS_ANL.1 Analyzer Analysis

Hierarchical to:	No other components
Dependencies:	No dependencies
IDS_ANL.1.1	The System shall perform the following analysis function(s) on all IDS data received: a) [selection: *statistical, signature, integrity*]; and b) [assignment: *other analytical functions*].
IDS_ANL.1.2	The System shall record within each analytical result at least the following information: a. Date and time of the result, type of result, identification of data source; and b. [assignment: *other security relevant information about the result*]. (EXT)

5.1.3 IDS_RCT.1 – Analyzer React

Management: IDS_RCT.1

The following actions could be considered for the management functions in FMT:

a) Configuration of the reaction operations to be performed

Audit: IDS_RCT.1

The following actions could be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Enabling and disabling of any of the reaction mechanisms

IDS_RCT.1 Analyzer React

Hierarchical to:	No other components
Dependencies:	No dependencies
IDS_RCT.1.1	The System shall send an alarm to [assignment: *specified location*] and take [assignment: *specified actions*] when an intrusion is detected.

5.1.4 IDS_RDR.1 Restricted Data Review (EXT)

Management: IDS_RDR.1

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the system data records.

Audit: IDS_RDR.1

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

a) Basic: Attempts to read system data that are denied.

b) Detailed: Reading of information from the system data records.

Application Note: The audit event definition is consistent with CCEVS Policy Letter #15, which states that only access failures are auditable at the Basic level of audit.

IDS_RDR.1 Restricted Data Review

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
IDS_RDR.1.1	The System shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of System data*] from the System data.	
IDS_RDR.1.2	The System shall provide the System data in a manner suitable for the user to interpret the information.	
IDS_RDR.1.3	The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.	

5.1.5 IDS_STG.1 Guarantee of System Data Availability

Management: IDS_STG.1

The following actions could be considered for the management functions in FMT:

b) maintenance of the parameters that control the system data storage capability.

Audit: IDS_STG.1

There are no auditable events foreseen.

IDS_STG.1 Guarantee of System Data Availability

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
IDS_STG.1.1	The System shall protect the stored System data from unauthorized deletion.	
IDS_ STG.1.2	The System shall protect the stored System data from modification. *Application Note: Authorized deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.*	
IDS_ STG.1.3	The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*].	

5.1.6 IDS_STG.2 Prevention of System Data Loss

Management: IDS_STG.2

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of actions to be taken in case system data storage capacity has been reached.

Audit: IDS_STG.2

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

a) Basic: Actions taken if the storage capacity has been reached.

IDS_STG.2 Prevention of System data loss

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis

IDS_STG.2.1 The System shall [selection: *'ignore System data', 'prevent System data, except those taken by the authorized user with special rights', 'overwrite the oldest stored System data '*] and send an alarm if the storage capacity has been reached.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.4	Prevention of Audit Trail Data Loss
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of Identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of Security Functions	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
IDS Component Requirements	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
	IDS_RCT.1	Analyzer React
	IDS_RDR.1	Restricted Data Review
	IDS_STG.1	Guarantee of System Data Availability
	IDS_STG.2	Prevention of System Data Loss

Table 18 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the basic level of audit; and

c) **Access to the System and access to the TOE and System data**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,** *the information detailed in the following table*.

Application Note: The auditable events for the basic level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and System data	Object IDs, Requested access
FAU_SAR.1	Reading of information from the audit records.	
FAU_SAR.2	Note: Unsuccessful attempts to read information from the audit records do not occur because the TOE does not present that capability to users that are not authorized to read the audit records.	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FAU_STG.4	Note: Since new audit records are discarded when storage space is exhausted, an audit record and alert are generated in response to audit storage failure.	
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated.	
FIA_UAU. 1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
IDS_ANL.1	None (the analysis function is always enabled)	
IDS_RDR.1	None (the user is not given the option of accessing unauthorized system data)	

COMPONENT	EVENT	DETAILS
IDS_STG.2	Note: Since new audit records are discarded when storage space is exhausted (system data and audit records are stored in the same database), an audit record is recorded and an alarm sent to the administrator in response to storage failure.	

Table 19 – Audit Events and Details

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *users with the "View audit log" or "View and purge audit log" permission or Global Administrators* with the capability to read *all information* 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.

6.1.1.3 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.

6.1.1.4 FAU_SEL.1 Selective audit

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

a) event type*;*

b) *no additional attributes*.

6.1.1.5 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the authorized user with special rights and *send an alarm* if the audit trail is full.

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_ATD.1 User Attribute Definition

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

a) User Identity;

b) Authentication Data;

c) Authorizations;

d) *Enabled or disabled*;

e) *Authentication configuration (must be configured for ePO)*;

Application Note: User identity is the ePO User name. Authentication data is the password. Authorizations are the permission sets and Global Administrator status.

6.1.2.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

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

6.1.2.3 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified.

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

Application Note: Authorized System Administrators in this context are users with the HIP IPS Policy "View and modify settings" permission and/or the HIP General Policy "View and modify settings" permission, or Global Administrators.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

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

Application Note: Authorized System Administrators in this context are users with the HIP IPS Policy "View and modify settings" permission and/or the HIP General Policy "View and modify settings" permission, or Global Administrators.

6.1.3.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query **and add System and audit data, and shall restrict the ability to query and modify all other TOE data** the *TSF data identified in the following table* to *a user with the permissions identified in the following table or a Global Administrator*.

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Application	HIP IPS Policy: View settings	Query

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Protection Lists	HIP IPS Policy: View and modify settings	Query and modify
Contacts	Create and edit contacts	Query, create, delete and modify
	Use contacts	Use
Dashboards	Use public dashboards	Query and use public dashboards
	Use public dashboards; create and edit personal dashboards	Query and use public dashboards; create and modify personal dashboards
	Use public dashboards; create and edit personal dashboards; make personal dashboards public	Query and use public dashboards; create, delete and modify personal dashboards; make personal dashboards public
	The owner of a personal dashboard has the implicit permission to change the owner of the dashboard (making it a personal dashboard of the new owner).	Modify the owner
Email Servers	View notification rules and Notification Log	Query
	Create and edit notification rules; view Notification Log	Query
	Create and edit notification rules; view and purge Notification Log.	Query, create, delete and modify
ePO User Accounts	n/a (only allowed by a Global Administrator)	Query, create, delete and modify
Event Filtering	n/a (only allowed by a Global Administrator)	Query and modify
Exceptions	HIP IPS Policy: View settings	Query
	HIP IPS Policy: View and modify settings	Query and modify
Global Administrator Status	n/a (only allowed by a Global Administrator)	Query and modify
Groups	n/a (only allowed by a Global Administrator)	Query, create, delete and modify
IPS Options	HIP IPS Policy: View settings	Query
	HIP IPS Policy: View and modify settings	Query and modify
IPS Policies	HIP IPS Policy: View settings	Query

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	HIP IPS Policy: View and modify settings	Query and modify
IPS Protection Policies	HIP IPS Policy: View settings	Query
	HIP IPS Policy: View and modify settings	Query and modify
Notification Rules	View notification rules and Notification Log	Query
	Create and edit notification rules; view Notification Log	Query, create, delete and modify
	Create and edit notification rules; view and purge Notification Log	Query, create, delete and modify
Permission Set	n/a (only allowed by a Global Administrator)	Query, create, delete, modify, and assign (to a user) permissions
Queries	Use public queries	Query and use public queries
	Use public queries; create and edit personal queries	Query and use public queries; create and modify personal queries
	Edit public queries; create and edit personal queries; make personal queries public	Query, delete, modify and use public queries; create, delete and modify (including make public) personal queries
Server Settings	n/a (only allowed by a Global Administrator)	Query and modify
Signatures	HIP IPS Policy: View settings	Query
	HIP IPS Policy: View and modify settings	Query and modify
System Event Audit Configuration	n/a (only allowed by a Global Administrator)	Query and modify
System Information	Access to the specific group node in the tree	Query
	“View System Tree tab”, access to the specific group node in the tree, and “Edit System Tree groups and systems”	Query, create, delete and modify
System Tree	View System Tree tab and access to the specific group node in the tree	Query

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	"View System Tree tab", access to the specific group node in the tree, and "Edit System Tree groups and systems"	Query, create, delete and modify
Trusted Applications	HIP General Policy: View settings	Query
	HIP General Policy: View and modify settings	Query and modify

Table 20 – TSF Data Access Permissions

6.1.3.3 FMT_SMF.1 Specification of Management Functions

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

a) ePO User Account management,

b) Permission Set management,

c) Audit Log management,

d) Event Log management,

e) Notification management,

f) Event Filtering management,

g) System Tree management,

h) Query management,

i) Dashboard management,

j) HIP IPS Policy management,

k) HIP General Policy management

6.1.3.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the **following** roles: **authorized System Administrators, and** *Global Administrators and Users users assigned any of the following permissions*:

a) Create and edit contacts

b) Create and edit notification rules; view and purge Notification Log;

c) Create and edit notification rules; view Notification Log

d) Edit public queries; create and edit personal queries; make personal queries public

e) *Edit System Tree groups and systems*

f) *HIP General Policy: View and modify settings*

g) *HIP General Policy: View settings*

h) *HIP IPS Policy: View and modify settings*

i) *HIP IPS Policy: View settings*

j) *System permissions (to specific nodes)*

k) *Use contacts*

l) *Use public dashboards*

m) *Use public dashboards; create and edit personal dashboards*

n) *Use public dashboards; create and edit personal dashboards; make personal dashboards public*

o) *Use public queries*

p) *Use public queries; create and edit personal queries*

q) *View notification rules and Notification Log*

r) *View System Tree tab.*

Application Note: The "authorized administrator" role specified in the PP has been deleted since the only reference to it (other than this SFR) is in FIA_AFL.1, which has been deleted from the ST per NIAP PD-0097.

Application Note: Authorized System Administrators in this context are users with the HIP IPS Policy "View and modify settings" permission and/or the HIP General Policy "View and modify settings" permission, or Global Administrators.

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

6.1.4 Protection of the TSF (FPT)

6.1.4.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

Application Note: This SFR requires the TOE to use IT Environment-provided functionality to protect communication between TOE components. Having the functionality in the IT Environment is not sufficient since the TOE is not necessarily utilizing it.

6.1.5 IDS Component Requirements (IDS)

6.1.5.1 IDS_SDC.1 System Data Collection

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

a) detected malicious code and

b) *no other events.*

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 the table below**.

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Start-up and shutdown	None
IDS_SDC.1	Detected malicious code	Location, identification of code

Table 21 – System Data Collection Events and Details

6.1.5.2 IDS_ANL.1 Analyzer analysis

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

a) signature*;* and

b) *behavioral intrusion prevention functions.*

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

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

b) *Severity level.*

6.1.5.3 IDS_RCT.1 Analyser react

IDS_RCT.1.1 The System shall send an alarm to *the audit log* and ~~take~~ *optionally block the system call or network packet from proceeding (if configured to do so)* when an intrusion is detected.

6.1.5.4 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The System shall provide *Global Administrators and users with System permissions* with the capability to read *the system data listed in the table below* from the System data.

USER TYPE	ACCESS
Global Administrators	Full access
Users with System permissions	System Data originating from systems the users have been granted permission to

Table 22 – System Data Access

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

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.1.5.5 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion **via interfaces within the TSC**.

IDS_ STG.1.2 The System shall protect the stored System data from modification **via interfaces within the TSC**.

Application Note: Authorized deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 The System shall ensure that *the full number of the currently stored* System data will be maintained when the following conditions occur: System data storage exhaustion.

Rationale for refinement: The TOE is only able to restrict access to the database from within the TSC. Access to the database from outside the TSC is addressed by OE.SD_PROTECTION.

6.1.5.6 IDS_STG.2 Prevention of System data loss

IDS_STG.2.1 The System shall prevent System data, except those taken by the authorized user with special rights and send an alarm if the storage capacity has been reached.

6.2 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ADV_TDS.1: Basic Design	Basic Design: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_FLR.2 Flaw Reporting Procedures	Flaw Reporting Procedures: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ATE_FUN.1: Functional Testing	Security Testing: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5

Table 23 – Security Assurance Measures

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied by the operational environment (OE.TIME). This approach is acceptable per NIAP PD-0152.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_SEL.1	No other components.	FAU_GEN.1, FMT_MTD.1	Satisfied Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied by the operational environment (OE.AUDIT_PROTECTION)
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.1	No other components.	FIA_UID.1	Satisfied
FIA_UID.1	No other components.	None	n/a
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied
FPT_ITT.1	No other components.	None	n/a
IDS_SDC.1	No other components.	FPT_STM.1	Satisfied by the operational environment (OE.TIME). This approach is acceptable per NIAP PD-0152.
IDS_ANL.1	No other components.	None	n/a
IDS_RCT.1	No other components.	None	n/a
IDS_RDR.1	No other components.	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied
IDS_STG.1	No other components.	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied
IDS_STG.2	No other components.	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied

Table 24 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

SFR \ OBJECTIVE	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.IDANLZ	O.IDSCAN	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON
FAU_GEN.1		✓									
FAU_SAR 1			✓								
FAU_SAR.2	✓			✓							
FAU_SEL.1		✓	✓								
FAU_STG.4		✓							✓		
FIA_ATD.1				✓							
FIA_UAU.1	✓			✓							
FIA_UID.1	✓			✓							
FMT_MOF.1	✓			✓						✓	
FMT_MTD.1	✓			✓				✓		✓	
FMT_SMF.1			✓								
FMT_SMR.1				✓							
FPT_ITT.1								✓			
IDS_ANL.1					✓						
IDS_RCT.1											✓
IDS_RDR.1	✓		✓	✓							
IDS_SDC.1						✓	✓				
IDS_STG.1	✓			✓				✓	✓	✓	
IDS_STG.2									✓		

Table 25 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE

OBJECTIVE	RATIONALE
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 System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.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]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1].
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. 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 the audit trail is full [FAU_STG.4].
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 System [FAU_SAR.1, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The management functions provided by the TOE are specified [FMT_SMF.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].

OBJECTIVE	RATIONALE
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 System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.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]. 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 System may query and add 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_SMR.1]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [IDS_STG.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].
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].
O.INTEGR	The TOE must ensure the integrity of all audit and System data. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted between distributed TOE components [FPT_ITT.1].
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows. The TOE must prevent the loss of audit data in the event the its audit trail is full [FAU_STG.4]. The System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [IDS_STG.1].

OBJECTIVE	RATIONALE
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data. 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 System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [IDS_STG.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].

Table 26 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ADV_FSP.3 Functional Specification with Complete Summary	Functional Specification: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ADV_TDS.2 Architectural Design	Architectural Design: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_CMC.3 Authorization Controls	Security Measures: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_CMS.3 Implementation representation CM coverage	Security Measures: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_DVS.1 Identification of Security Measures	Security Measures: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_LCD.1 Developer defined life-cycle model	Life Cycle Model: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ALC_FLR.2 Flaw Reporting Procedures	Flaw Reporting Procedures: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ASE_CCL.1 Conformance claims	Security Target: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ASE_ECD.1 Extended components definition	Security Target: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ASE_INT.1 ST introduction	Security Target: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ASE_OBJ.2 Security objectives	Security Target: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ASE_REQ.2 Derived security requirements	Security Target: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ASE_SPD.1 Security problem definition	Security Target: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ASE_TSS.1 TOE summary specification	Security Target: Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ATE_COV.2 Analysis of Coverage	Testing Evidence Supplement: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ATE_DPT.1 Testing: Basic Design	Testing Evidence Supplement: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
ATE_FUN.1 Functional Testing	Testing Evidence Supplement: McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5

Table 27 – Security Assurance Rationale and Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. Hierarchically stronger than or the same as the assurance requirements specified in the referenced PP.
3. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented byALC_FLR.2 from part 3 of the Common Criteria

6.5 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

SFR \ TSF	AUDIT	I&A	MGMT	SYSPROT
FAU_GEN.1	✓			
FAU_SAR.1	✓			
FAU_SAR.2	✓			
FAU_SEL.1	✓			
FAU_STG.4	✓			
FIA_ATD.1		✓		
FIA_UAU.1		✓		
FIA_UID.1		✓		
FMT_MOF.1			✓	
FMT_MTD.1			✓	
FMT_SMF.1			✓	
FMT_SMR.1			✓	
FPT_ITT.1				✓
IDS_ANL.1				✓
IDS_RCT.1				✓
IDS_RDR.1	✓			
IDS_SDC.1				✓
IDS_STG.1	✓			
IDS_STG.2	✓			

Table 28 – SFR to TOE Security Functions Mapping

SFR	SF AND RATIONALE
FAU_GEN.1	**Audit** – As management events occur, the TOE generates audit records.
FAU_SAR.1	**Audit** - Authorized Console Users are given access to all the audit event records.
FAU_SAR.2	**Audit** – Audit review access is controlled by the TSF and limited to authorized users. Access is determined by the security attributes of the console user type and permissions.
FAU_SEL.1	**Audit** – Audit generation includes the ability to selectively audit based on audit event type. Filtering of specific security events is specified via the audit filter configuration file.
FAU_STG.4	**Audit** – When the space for audit records is exhausted, the TOE will prevent auditable events, except those taken by the authorized user with special rights and send an alarm.
FIA_ATD.1	**I&A** – User security attributes are associated with the user upon successful login.

SFR	SF AND RATIONALE
FIA_UAU.1	**I&A** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FIA_UID.1	**I&A** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FMT_MOF.1	**Mgmt** – The User Type identifies the privilege level of the console user. System administrators modify the behaviour of the IDS functions by determining the systems on which the TOE is installed and configuring the Agents on those systems.
FMT_MTD.1	**Mgmt** – The User Type identifies the privilege level of the console user. Appropriate privileges are provided to the various user types for management of Agents and Console Users. Note that the SFR describes management functionality in terms of querying and modifying all TOE data other than system data and audit data. Since this description does not explicitly address the ability to add or delete data (e.g., console users), the ST author interprets “modify” in this instance to include creation and deletion of TOE data where appropriate.
FMT_SMF.1	**Mgmt** – The TOE provides the management functions specified in the SFR.
FMT_SMR.1	**Mgmt** – The TOE provides the roles specified in the SFR. When a Console User Account is created or modified, the user must specify the user type of the console user.
FPT_ITT.1	**Sysprot** – Whenever information is communicated between distributed TOE components, the TOE invokes IT Environment-provided functionality to protect the information from modification and disclosure.
IDS_SDC.1	**Sysprot** – The Agents detect malicious code by examining system calls. Upon detection, an audit is generated. Agents also generate events when they are started or stopped.
IDS_ANL.1	**Sysprot** – The Agents detect malicious code by comparing system calls to signatures of known malicious attacks. Upon detection, an audit is generated.
IDS_RCT.1	**Sysprot** – The Agents detect malicious code by comparing system calls to signatures of known malicious attacks. Upon detection, an audit is generated and the system call may be blocked (as configured by the administrator).
IDS_RDR.1	**Audit** – Authorized Console Users are given access to all the system data records.
IDS_STG.1	**Audit** – The TOE does not provide any mechanism to modify or delete saved system data. If storage space for system data is exhausted, the oldest records are maintained and new records are discarded.

SFR	SF AND RATIONALE
IDS_STG.2	**Audit** – When the space for audit records is exhausted, the new system data is discarded and the TOE records and audit record and sends an alert.

Table 29 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 System Protection (SYSPROT)

The Agents are host based intrusion detection/prevention systems designed to detect malicious code and protect system resources and applications from attacks. The Agents accomplish this by intercepting operating system calls and network packets (both incoming and outgoing) and comparing them to signatures symptomatic of malicious code.

The Agent software includes Policy rules that reference a list of Signatures. Signatures are system call and network packet patterns that are symptomatic of a potential security violation. The Agents compare system calls and network packets against the Signatures referenced by Policies enabled on that Agent. If the system call or network packet matches a signature, a potential security violation has been detected.

Each Signature in the Signature File is assigned a Severity Level (Information, Low, Medium or High). Each Severity Level defines the potential danger an occurrence of the Signature poses to a host. On a match of a Signature, the reaction taken by an Agent is defined by the Agent's Protection Policy. If a potential security violation is detected, the reactions configured by the administrator for that Agent are performed automatically by the TOE. Possible reactions are:

1. Generate a security audit event
2. Block the system call or network packet
3. Allow the system call or network packet to proceed

If no signatures match, the call or packet is allowed to proceed. When multiple signatures match, the highest reaction is taken.

Exceptions and Trusted Applications may be defined for each Policy to override the Signatures. The exception feature enables administrators to weed out false positive alerts, minimize needless data flowing to the console, and ensures that the alerts are legitimate security threats. A trusted application is an application that is known to be safe in the end user environment, has no known vulnerabilities, and is allowed to perform operations that would otherwise be prevented. Application Protection may also be configured for Policies to control what applications are permitted to perform user-level process hooking. Explicit lists of permitted and blocked processes may be configured. If a process is not included in either list, then the hook is permitted if the process is a Windows service and blocked otherwise.

The Agent's IPS Options Policy defines the overall operation of the Agent. An Agent may be:

1. operating normally (On),
2. automatically generating client rules that permit all operations that would normally trigger an event (Adaptive).

An Agent is typically put into Adaptive (or Learning) mode when the Agent is first installed. This assists the Administrator in reviewing the activity on the system to customize the signatures and policies for that system. Once the customization is complete, the system is configured to operate normally. Once this activity is normalized, the TOE can analyze behavioral patterns and take action based on patterns that fall outside the normal usage patterns.

Security audit events are generated on the Agent systems and communicated to ePO, where they are saved and reviewed via the same mechanism used for audit events (see AUDIT below). Each audit events includes a timestamp, the type of event, and Agent identity. For events involving signatures, the event also identifies the matching signature, user id (if applicable), process name (if applicable), severity level, and the reaction taken.

The transfer of information between the Agent systems and ePO must be protected from disclosure and modification in order to ensure the integrity of the information exchanged between those components. The TOE invokes functionality provided by the IT Environment to protect all communication between the components.

7.2 Audit

The Audit Log maintains a record of ePO user actions. The auditable events are specified in the Audit Events and Details table in the FAU_GEN.1 section. Event filters may be configured to specify which possible events do not result in audit records being generated. Event filters for the Selective Audit function are specified in a configuration file using any text editor. The audit filter file is read whenever the TOE is started. This file is located in the "conf" directory of the ePO server. Typically this will be located at %Program Files%\McAfee\ePolicy Orchestrator\ \conf\orion\audit-filter.txt. The following audit event types can be selectively audited:

- CommonEvents
- EPO Core
- CommonEvents
- View IPS Events
- Delete Site (System)
- Move Branch Node
- Move Leaf Node
- New User
- Delete User

- Run Query
- Run Report (Dashboard)
- Set Policy Setting Value
- Set Policy User Role
- Uninstall Branch Node
- Uninstall Leaf Node
- EPO Core Startup Error
- Purge Client Events
- Purge Audit Log
- Add Dashboard
- View Audit Log
- View Audit Events
- Server Restart

The Audit Log entries may be displayed via reports. The information displayed is configurable, but is always presented in human readable form.

Audit Log entries can be queried against by a Global Administrator or users with the "View Audit Log" or "View and purge audit log" permission. The Audit Log entries are automatically purged based upon a configured age. A Global Administrator or users with the "View and purge audit log" permission may issue a command through the ePO GUI to purge all audit records older than a specified time. The audit log entries are stored in the database. Auditable events are prevented if database storage space is exhausted; the Database Capacity Monitor will fire an alarm and ePO operations can not be performed until space is made available via operational environment procedures (e.g., increasing the storage space or deleting information from the database).

7.2.1 Event Log

The Event Log maintains a record of events generated by HIP. The auditable events are specified in the IDS_SDC.1, IDS_ANL.1, and IDS_RCT.1 SFRs.

The Event Log entries may be displayed via dashboards and reports. The information displayed is configurable, but is always presented in human readable form.

Event Log information can be viewed by a Global Administrator or users with the "View Events" or "View and purge events log" permission. Global Administrators may view information originating from any

system, while users are limited to information originating on systems they have been granted permission to view.

The Event Log entries are automatically purged based upon a configured age. A Global Administrator or users with the "View and purge events" permission may issue a command through the ePO GUI to purge all event records older than a specified time.

7.3 Identification and Authentication

Users must log in to ePO with a valid user name and password supplied via a GUI before any access is granted by the TOE to TOE functions or data. The supplied credentials are validated by ePO. If validation is successful, the TOE grants access to additional TOE functionality. If the validation is not successful, an error message is displayed and the user may try to login again.

Upon successful login, the Global Administrator status and the union of all the permissions from the permission sets from the user account configuration are bound to the session, along with the user name. Those attributes remain fixed for the duration of the session (until the user logs off).

7.4 Management

The TOE's Management Security Function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE may be performed via the ePO GUI. Management permissions are defined per-user. Configuring Global Administrator status to an account implicitly grants all user permissions to that user.

The TOE provides functionality to manage the following:

1. ePO User Accounts,
2. Permission Sets,
3. Audit Log,
4. Event Log,
5. Notifications,
6. Event Filtering,
7. System Tree,
8. Queries,
9. Dashboards,
10. HIP IPS Policies,
11. HIP General Policies.

Each of these items is described in more detail in the following sections.

7.4.1 ePO User Account Management

Each user authorized for login to ePO must be defined with ePO. Only Global Administrators may perform ePO user account management functions (create, view, modify and delete). For each defined account, the following information is configured:

1. User name
2. Password
3. Enabled or disabled
4. Whether authentication for this user is to be performed by ePO or Windows (the evaluated configuration requires ePO authentication for all users)
5. Permission sets granted to the user
6. Global Administrator status

One or more permission sets may be associated with an account. Global Administrators are granted all permissions.

Permissions exclusive to global administrators (i.e., not granted via permission sets) include:

1. Change server settings.
2. Create and delete user accounts.
3. Create, delete, and assign permission sets.
4. Limit events that are stored in ePolicy Orchestrator databases.

7.4.2 Permission Set Management

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. One or more permission sets can be assigned to any users who are not global administrators (global administrators have all permissions to all products and features).

Permission sets only grant rights and access — no permission set ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks.

Global administrators may create, view, modify and delete permission sets. Each permission set has a unique name so that it can be appropriately associated with ePO users.

When a permission set is created or modified, the permissions granted via the permission set may be configured by a global administrator.

7.4.3 Audit Log Management

A global administrator may configure the length of time Audit Log entries are to be saved. Entries beyond that time are automatically purged.

The audit log may also be purged manually by a global administrator or a user with the "View and purge audit log" permission using a GUI to specify that all events older than a specified date are to be deleted. This is a one-time operation and the date specified is independent of the time period specified for automatic purging.

A global administrator or a user with either the "View audit log" or "View and purge audit log" permission may view events in the audit log.

7.4.4 Event Log Management

A global administrator may configure the length of time Event Log entries are to be saved. Entries beyond that time are automatically purged.

The event log may also be purged manually by a global administrator or a user with the "View and purge events" permission using a GUI to specify that all events older than a specified date are to be deleted. This is a one-time operation and the date specified is independent of the time period specified for automatic purging.

A global administrator or a user with either the "View events" or "View and purge events" permission may view events in the events log. Users access to event information is further restricted to information generated on systems to which they have been granted access (via System permissions).

7.4.5 Notification Management

Notifications may be specified in response to events generated by the TOE. Notifications cause alert messages to be sent to the configured recipient(s).

A global administrator or user with the "Create and edit contacts" permission may create, view, edit and delete contacts. Each contact includes a first name, last name and email address. The contacts are used in email notifications; any global administrator or user with the "Use contacts" permission may cause a notification to be sent to the specified contact for that notification.

A global administrator or user with the appropriate permissions (see below) may configure independent rules at different levels of the System Tree. The rules specify when and what type of notification should be sent under what conditions.

The permissions associated with Notification management are:

1. View notification rules and Notification Log - This permission also grants the ability to view registered executables, and external commands.
2. Create and edit notification rules; view Notification Log - This permission also grants the ability to registered servers, and external commands.

Users can configure when notification messages are sent by setting thresholds based on aggregation and throttling. Use aggregation to determine the thresholds of events at which the rule sends a notification message. Use throttling to ensure not too many notification messages are sent.

Once associated with a group or system, notification rules may be enabled and disabled by a global administrator or user with the "Create and edit contacts" permission.

7.4.6 Event Filtering Management

A global administrator may view and modify the list of auditable events that are generated.

7.4.7 System Tree Management

The System Tree organizes managed systems in units for monitoring, assigning policies, scheduling tasks, and taking actions. The System Tree is a hierarchical structure that allows systems to be organized within units called groups.

Groups have these characteristics:

1. Groups can be created by global administrators.
2. A group can include both systems and other groups.
3. Groups are modified or deleted by a global administrator.

The System Tree root includes a Lost&Found group. Depending on the methods for creating and maintaining the System Tree, the server uses different characteristics to determine where to place systems. The Lost&Found group stores systems whose locations could not be determined.

The Lost&Found group has the following characteristics:

1. It can't be deleted.
2. It can't be renamed.
3. Its sorting criteria can't be changed (although you can provide sorting criteria for the subgroups you create within it.)
4. It always appears last in the list and is not alphabetized among its peers.
5. All users with view permissions to the System Tree can see systems in Lost&Found.
6. When a system is sorted into Lost&Found, it is placed in a subgroup named for the system's domain. If no such group exists, one is created.

Child groups in the System Tree hierarchy inherit policies set at their parent groups. Inheritance is enabled by default for all groups and individual systems that you add to the System Tree. Inheritance may be disabled for individual groups or systems by a Global Administrator. Inheritance can be broken by applying a new policy at any location of the System Tree (provided a user has appropriate permissions). Users can lock policy assignments to preserve inheritance.

User permissions in the Systems category that are relevant to this information are:

1. View the “System Tree” tab
2. Edit System Tree groups and systems

Systems may be deleted or moved between groups by a Global Administrator or users with both the “View the “System Tree” tab” and “Edit System Tree groups and systems” permissions. User access to groups in the System Tree is controlled by individual check boxes in the permission sets for the System Tree.

7.4.8 Query Management

Users may create, view, modify, use and delete queries based upon their permissions. Permissions associated with queries are:

1. Use public queries — Grants permission to use any queries that have been created and made public.
2. Use public queries; create and edit personal queries — Grants permission to use any queries that have been created and made public by users with the same permissions, as well as the ability to create and edit personal queries.
3. Edit public queries; create and edit personal queries; make personal queries public — Grants permission to use and edit any public queries, create and modify any personal queries, as well as the ability to make any personal query available to anyone with access to public queries.

7.4.9 Dashboard Management

User-specific dashboards may be configured to display data of interest to each user; these chart-based displays are updated at a configured rate to keep the information current. Permissions relevant to dashboards are:

1. Use public dashboards
2. Use public dashboards; create and edit personal dashboards
3. Edit public dashboards; create and edit personal dashboards; make personal dashboards public

7.4.10 HIP IPS Policy Management

HIP IPS Policy management addresses the management of Application Protection Lists, Exceptions, IPS Options, IPS Policies, IPS Protection Policies, and Signatures.

Permissions relevant to HIP IPS Policy management are:

1. View settings
2. View and change settings

7.4.11 HIP General Policy Management

HIP General Policy management addresses the management of Trusted Applications.

Permissions relevant to HIP General Policy management are:

1. View settings

2. View and change settings