Security Target

McAfee Nitro Intrusion Prevention System 9.1

Document Version 1.3

October 30, 2013

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Ave, 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 Nitro Intrusion Prevention System 9.1. 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 Nitro Intrusion Prevention System 9.1
ST Revision	1.3
ST Publication Date	October 30, 2013
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	McAfee Nitro Intrusion Prevention System 9.1.3 Build 20121030211720

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 showing the value in square brackets, i.e. [assignment_value(s)].
- 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 *italicized* 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, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

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
ARP	Address Resolution Protocol
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
IPS	Intrusion Prevention System
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 2 – Acronyms Used in Security Target

1.6 TOE Description

1.6.1 Summary

The TOE is McAfee's Nitro Intrusion Prevention System (IPS) version 9.1.3. The TOE includes McAfee Enterprise Security Manager 9.1.3 (ESM). The evaluated configuration includes one IPS and one ESM running on a virtual machine.

The TOE provides a scalable enterprise security solution that provides intrusion prevention or intrusion detection, network event and/or flow data acquisition, network behavior analysis, and security event management that enables administrators to secure their networks with real-time threat mitigation. The TOE's IPS component can pass, drop, and log packets as they arrive, based on administrator-configurable rules. When IPS is performing intrusion detection, it is said to be operating in an "IDS mode", when performing intrusion prevention, it is said to be operating in an "IPS mode". Additionally, IPS has an alerts-only mode that is supported when it is operated in an in-line mode.

The general concept of operation of the TOE includes one or more IPS devices, each in an in-line network location operating in either an IPS mode or in an alerts-only mode. This is depicted in the figure below:

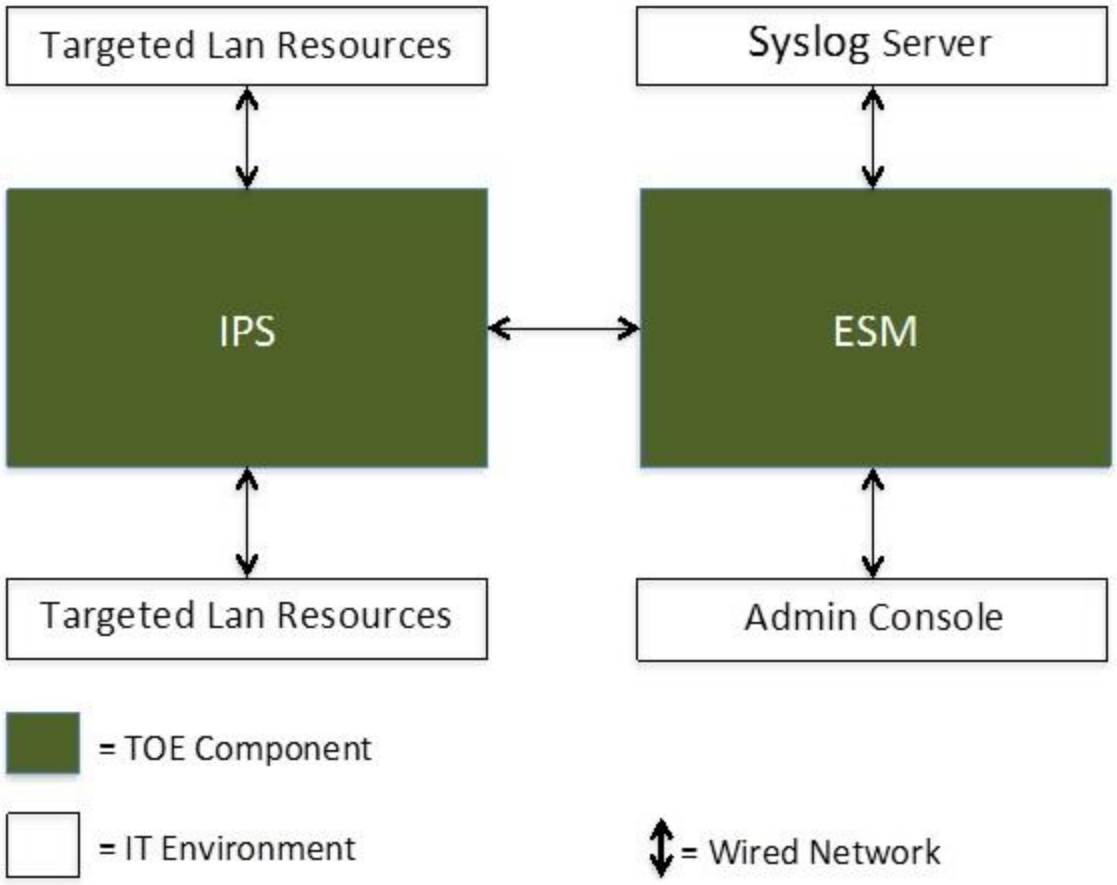


Figure 1: In-line network location of IPS and ESM

In another deployment scenario, of the operation of the TOE's IPS is in an in-tap network location operating in an IDS mode, and is depicted in the figure below:

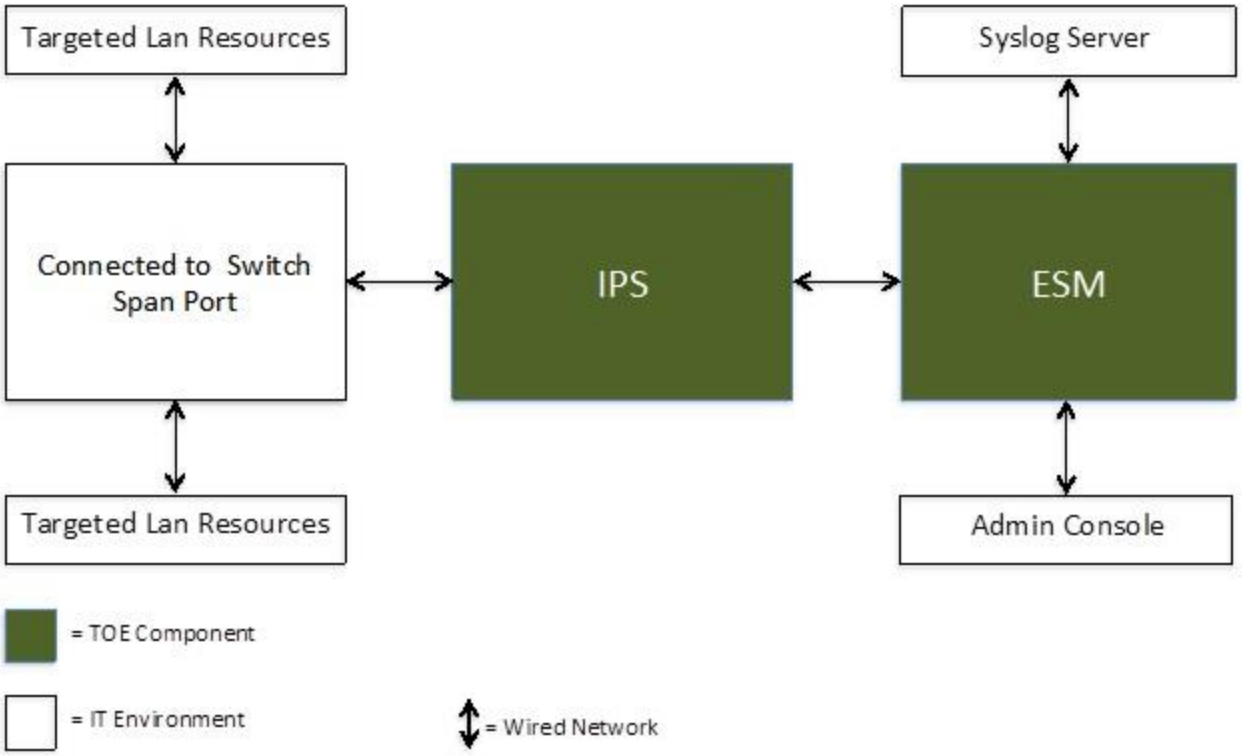


Figure 2: In-tap network location of IPS and ESM

The TOE is also capable of running in "stealth mode" whether placed in an "in-tap" or "in-line" deployment scenario. When configured to run in stealth mode, the IPS device does not require an IP address. The device will not respond to pings, trace routes, or any other high-level mechanics, nor will it respond to ARP requests or any other low level mechanics. It is extremely difficult to detect the presence of the device within a network, effectively reducing the risk of attack against the IPS device itself.

The TOE protects communications between its components. The TOE includes a FIPS 140-2 validated module, which performs cryptographic operations. Communications with the Console are protected by both the TOE and the Operational Environment.

1.6.2 TOE Functionality Overview

The TOE is not a Firewall[1]; it is an IPS that includes a firewall module and it is that module which all network traffic passes. The TOE's IPS passes, drops, and logs packets as they arrive, based on configurable rules. Each device in a TOE deployment is individually configured with rules, notification definitions, modes, variables and other parameters. Following are the three rule types the IPS supports:

- *Firewall Policy rules* - include those rules that the IPS will test against when a packet is

[1] The TOE is not a Firewall, it is an IPS. When configured in IPS mode, the rules could be defined as simple firewall flow control rules. Its integration with snort traffic analysis rules are what distinguishes this product in IPS mode from a simple Traffic Filter Firewall. No firewall functionality was evaluated.

examined. These rules correspond to iptables (these include both standard and custom firewall policy rules). The firewall policy rules are adjusted as needed to control the iptables instance running within the IPS component. There are standard firewall rules and custom firewall rules within the policy. For the standard rules, the user can adjust the parameters of the rule including enabling or disabling a rule, for custom rules, the user defines the rules and can enable and disable them.

- *Standard Policy rules* - include deep-packet inspection rules that evaluate the contents of a packet and compare them with the signatures associated with the rules.
- *Custom Policy rules* - include administrator-modified/created firewall policy rules and standard policy rules as described above.

Nitro IPS is designed using the layers of the protocol stack present in data-link and TCP/IP protocol definitions. IPS includes an implementation of Snort, which is an open source packet inspection application implementation. The IPS imposes order on packet data by overlaying data structures on the raw network traffic. These decoding routines are called, in order, through the protocol stack, from the data link layer up through the transport layer, finally ending at the application layer.

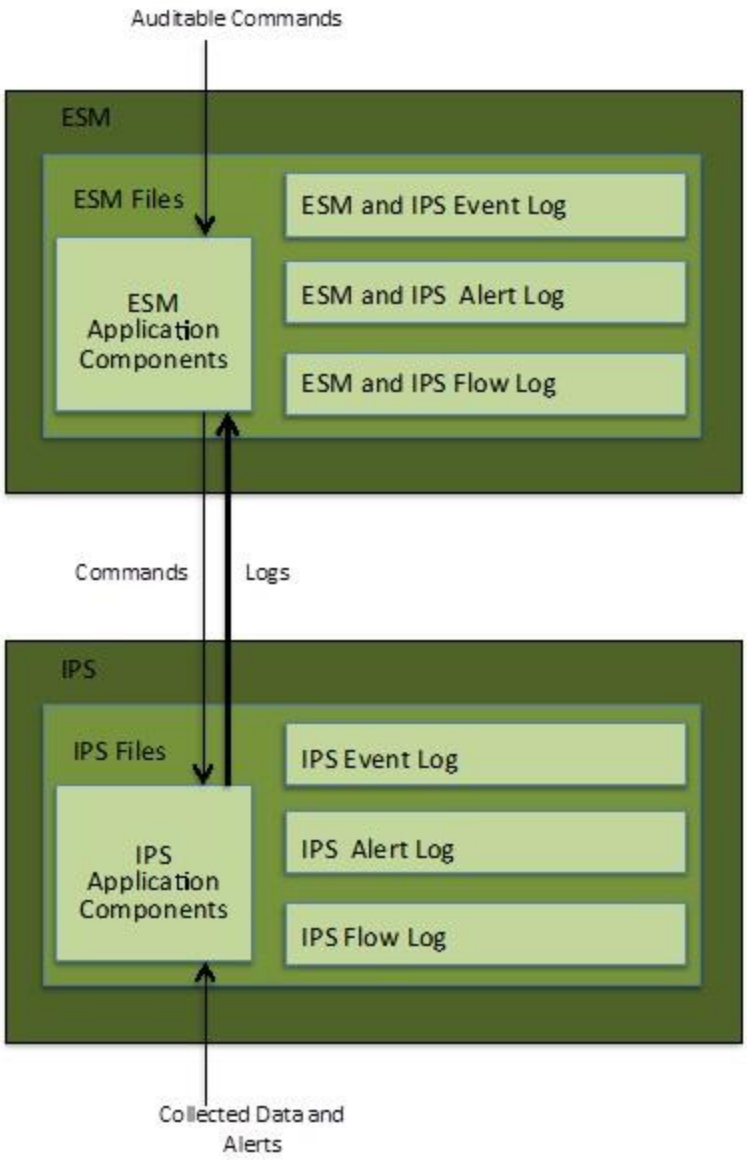


Figure 3: Command and log flow within an ESM and IPS deployment

When a network packet enters the IPS through one of its physical network interfaces, when it is either in an in-line or an in-tap network location, the packet is first inspected using Linux netfilter/iptables to look for any firewall policy rule matches (packet headers), and to gather flow data information. The first check is done by a netfilter/iptables plug-in that determines if the packet is a control channel packet from the Enterprise Security Manager (ESM) destined for IPS device. If the packet is a control channel packet it is dropped (The control channel packet is actually processed using a control channel daemon that acquires the packet from the network interface promiscuously). If the packet is NOT a control channel packet, and a match is found that will cause an alert the information is passed to a daemon in the alert module for logging to the alerts database. Additionally, the netfilter/iptables capabilities are used to acquire flow information that is passed to a daemon in the flow module for logging to the flows

database. If the packet was not dropped, IPS passes it to one, of potentially several, Snort[2] instances, each with its own set of inspection rules to be matched against a packets content, running on the IPS device. If a match is found, Snort has a custom plug-in, which enables it to send the alert to the alerts database in the alert module for logging. If the packet has gone through both firewall and deep packet inspection without being dropped, it is sent out of the IPS device through the second physical interface of that traffic path.

The evaluated configuration does not allow the use of the bypass feature that allows all traffic to pass, even malicious traffic.

1.6.3 Physical Boundary

The TOE is a software TOE and is defined as the Nitro Intrusion Prevention System 9.1. In order to comply with the evaluated configuration, the following software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER	
TOE Software	Nitro IPS	Version 9.1.3
	McAfee ESM	Version 9.1.3

Table 3 **– Evaluated Configuration for the TOE**

1.6.4 Hardware and Software Supplied by the IT Environment

The following tables identify the minimum system requirements for McAfee ESM components provided by the IT Environment:

Component	Minimum Requirement
Processor	P4 class (not Celeron) or higher (Mobile/Xeon/Core2,Corei3/5/7) AMD AM2 class or higher (Turion64/Athlon64/Opteron64,A4/6/8)
Operating system	Windows 2008 Server Windows 7 Linux (SuSe 10, Mandrake 10.2, or Fedora Core 5 recommended) Mac (limited testing on OS 9.2.2 and OS X 10.4.10)
RAM	1.5 GB
Screen resolution	1024 by 768 pixels
Browser	IE 7 or higher and FireFox 1.5.0.4 or later (must be AES enabled)
Flash Player	11.2.x.x
Virtual Machine	ESXI 5.0

Table 4 – Hardware and Software Requirements for IT Environment for IPS

Component	Minimum Requirement
Processor	P4 class (not Celeron) or higher (Mobile/Xeon/Core2,Corei3/5/7) AMD AM2 class or higher (Turion64/Athlon64/Opteron64,A4/6/8)

[2] Snort® is an Open Source network intrusion prevention and detection system (IDS/IPS). See Also: http://www.snort.org

Component	Minimum Requirement
Operating system	Windows 2008 Server Windows 7 Linux (SuSe 10, Mandrake 10.2, or Fedora Core 5 recommended) Mac (limited testing on OS 9.2.2 and OS X 10.4.10)
RAM	1.5 GB
Screen resolution	1024 by 768 pixels
Browser	IE 7 or higher and FireFox 1.5.0.4 or later (must be AES enabled)
Flash Player	11.2.x.x
Virtual Machine	ESXI 5.0

Table 5 – Hardware and Software Requirements for IT Environment for ESM

Component	Minimum Requirement
Administrator Console	General Purpose Computer
Browser	IE 7 or higher and FireFox 1.5.0.4 or later (must be AES enabled)

Table 6 – Hardware and Software Requirements for IT Environment for the Administrator Console

Component	Minimum Requirement
Syslog Server	General Purpose Computer running Syslog Server Software

Table 7 – Hardware and Software Requirements for IT Environment for the Syslog Server

1.6.5 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
Security Audit	The TOE applications; IPS and ESM generate audit records when security-relevant events occur. Auditable events generated by the IPS are sent at regular administrator-configured intervals for storage and review by the ESM appliance. Audit records are stored in an audit trail on the ESM appliance. The audit trail is physically protected by the ESM appliance hardware. The audit trail is protected from unauthorized access by restricting access to the ESM web-based GUI interface used to read from the audit trail.
Cryptographic Support	The TOE encrypts communications between the ESM and IPS components using AES 256 CBC. ESM and the Console communicate over HTTPS using either AES 125, 192 or 256 CBC. The Console uses a web browser that supports one of these algorithms.

TSF	DESCRIPTION
Identification and Authentication	The TOE cannot be accessed directly. Their system data collection interfaces are invoked upon receipt of monitored network traffic. They are managed using the ESM appliance, which can only be accessed after an authorized user successfully logs into the ESM web-based GUI interface using a valid username and password. The TOE also provides a mechanism to lock or disable a user account after a configured number of consecutive failed attempts to logon. Authentication services are handled internally (fixed passwords) . The external authentication server is considered outside the scope of the TOE.
Security Management	The ESM provides a GUI interface to administer the IPS. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction. System data consists of results from IPS scanning, sensing, and analyzing tasks. The administrator console is also used to manage audit data and user accounts. The TOE also provides the capability to see the physical locations where events have occurred in the network, which increases the ability of tracking down events through the Network Discovery function. The TOE restricts access to this function via the GUI interface. The actual function of Network Discovery is not considered security relevant from the point of view of this TOE, and was not covered by the evaluation.
TSF Protection	The TOE restricts access to its interfaces by requiring authorized users to log into the ESM using its GUI, and by encrypting commands sent from the ESM to the IPS. HTTPS is also used to protect the connection between the web browser in the operational environment and the ESM. In FIPS mode, the TOE tunnels all traffic between the ESM and IPS through a FIPS certified VPN tunnel, and uses a FIPS certified HTTPS crypto function. The FIPS certificate numbers can be found in Table 27 – Security Function, Use and Certificate
Intrusion Detection	The TOE can detect different types of intrusion attempts by performing analysis of network traffic packets depending on location within a network. The TOE supports installation in different locations in the network architecture of the TOE operational environment by providing the ability to operate in different types of IDS and IPS/alerts-only modes. The evaluated configuration does not allow the use of the bypass feature that allows all traffic to pass, even malicious traffic.

Table 8 – Logical Boundary Descriptions

1.6.6 TOE Product Documentation

The TOE includes the following product documentation:

- McAfee Enterprise Security Manager Interface 9.1.3 ESM/Event Receiver VM Users Guide
- McAfee Enterprise Security Manager Interface 9.1.3 ESMI Users Guide
- McAfee Enterprise Security Manager Interface 9.1.3 ESMI Quick Start Guide
- McAfee Enterprise Security Manager Interface 9.1.3 ESMI Setup and Installation Guide
- McAfee ESM Release 9.1.3 Release Notes

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 with ALC_FLR.2.

2.2 Protection Profile Conformance Claim

The TOE does not conform to any protection profiles, however the ST is modeled after the requirements in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007 (IDSPP). The exceptions are noted in Section 2.4.1 Protection Profile Refinements and in Section 2.4.2 Protection Profile Additions.

2.3 Package Claim

The TOE claims conformance to the Interim Basic assurance package as defined by the Consistency Instruction Manual for Interim Basic Robustness Environments and summarized in the IDSPP.

2.4 Conformance Rationale

The Security Functional Requirements are modeled after the requirements in the IDSPP. The Security Assurance Requirements are satisfied in accordance with the IDSPP and with relevant NIAP Precedents.

2.4.1 Protection Profile Refinements

The following items have been deleted for the set of SFRs in the IDSPP:

- FAU_STG.4
- IDS_STG.2 (EXT)
- FIA_AFL.1
- FPT_ITA.1
- FPT_ITC.1
- FPT_ITI.1
- O.EXPORT

2.4.2 Protection Profile Additions

This Security Target includes all of the assumptions and threats statements described in the PP, verbatim, except as noted below.

- The threat, T.PROCOM was added to address the issue of unauthorized entities modifying information sent between distributed components of the TOE.

This Security Target includes all of the Security Objectives from the PP, verbatim, except as noted below.

- The security objective, O.ENCRYPT was added to support the protection of the confidentiality of the TOE's dialogue between distributed components. The security objective counters the threat, T.PROCOM.

This Security Target includes all of the Security Objectives for the Environment from the PP, verbatim, except as noted below.

- The operational environment security objectives OE.AUDIT_PROTECTION and OE.AUDIT_SORT are not applicable to the environment for this TOE and were removed from the ST. The security objectives for the TOE provide the ability to sort the audit logs and provide protection of the audit trail.

- The security objective, OE.PROTECT was added to support the protection of the TOE from external interference or tampering. The security objective counters the threat T.PROCOM.

This Security Target includes all of the Security Functional and Security Assurance Requirements from the PP verbatim, except as noted below.

- FMT_SMF.1 was added in this Security Target to satisfy a dependency to FMT_MOF.1 and FMT_MTD.1. This requirement was originally included by International Interpretation RI#65 that was adapted in CC Part 2, v2.3 and is included in CC v3.1. This requirement simply requires that security functions actually be present in addition to being protected if they are present and therefore does not impact PP conformance.
- FPT_ITT.1 was added to protect inter-communications between the distributed TOE components.

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.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between distributed components of the TOE.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

Table 9 – Threats Addressed by the TOE

The IT System addresses the following threats:

THREAT	DESCRIPTION
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

Table 10 – Threats Addressed by the IT System

3.2 Organizational Security Policies

The following Organizational Security Policies apply to the TOE:

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

THREAT	DESCRIPTION
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

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

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.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyser must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses, use of the System functions, and the results of the TOE's detection/filtering functions[3]
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.ENCRYPT	The TOE must protect the confidentiality of its dialogue between distributed components.

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.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

[3] Objective expanded to include audit capabilities of IPS functionality

OBJECTIVE	DESCRIPTION
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.INTROP	The TOE is interoperable with the IT System it monitors.
OE.PROTECT	The Operational Environment will protect itself and the TOE from external interference or tampering.

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 / THREATS/ ASSUMPTION	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.ENCRYPT	OE.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.PROTECT
A.ACCESS																		✓	
A.DYNMIC																	✓	✓	
A.ASCOPE																		✓	
A.PROTCT															✓				
A.LOCATE															✓				
A.MANAGE																	✓		
A.NOEVIL														✓	✓	✓			
A.NOTRST															✓	✓			
T.COMINT	✓						✓	✓			✓								
T.COMDIS	✓						✓	✓											
T.LOSSOF	✓						✓	✓			✓								
T.NOHALT		✓	✓	✓			✓	✓											
T.PRIVIL	✓						✓	✓											
T.IMPCON						✓	✓	✓						✓					
T.INFLUX									✓										
T.FACCNT										✓									
T.SCNCFG		✓																	
T.SCNMLC		✓																	

OBJECTIVE / THREATS/ ASSUMPTION	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.ENCRYPT	OE.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.PROTECT
T.SCNVUL		✓																	
T.FALACT					✓														
T.FALREC				✓															
T.FALASC				✓															
T.MISUSE			✓																
T.INADVE			✓																
T.MISACT			✓																
T.PROCOM												✓							✓
P.DETECT		✓	✓							✓			✓						
P.ANALYZ				✓															
P.MANAGE	✓					✓	✓	✓						✓		✓	✓		
P.ACCESS	✓						✓	✓											
P.ACCACT								✓		✓			✓						
P.INTGTY											✓								
P.PROTCT									✓						✓				

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 OE.INTROP objective ensures the TOE has the needed access.
A.DYNMIC	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.ASCOPE	The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.PROTCT	The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.NOEVIL	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.NOTRST	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.
T.COMINT	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.COMDIS	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.
T.LOSSOF	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.NOHALT	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	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.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.IMPCON	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.INFLUX	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.FACCNT	The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNCFG	The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The Scanner/Monitoring Engine component of the TOE specifically addresses this threat.
T.SCNMLC	The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code. The Scanner/Monitoring Engine component of the TOE specifically addresses this threat.
T.SCNVUL	The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability. The Scanner/Monitoring Engine component of the TOE specifically addresses this threat.
T.FALACT	The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC	The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.MISUSE	The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.INADVE	The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.MISACT	The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.PROCOM	This threat is completely countered by • O.ENCRYPT which will protect the confidentiality of its communications between distributed TOE components. • OE.PROTECT, which will protect the Operational Environment and the TOE from external interference or tampering.
P.DETECT	The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data.
P.ANALYZ	The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.
P.MANAGE	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 and OE_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.ACCESS	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.ACCACT	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.
P.INTGTY	The O.INTEGR objective ensures the protection of data from modification.
P.PROTCT	The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

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

5 Extended Components Definition and Rationale

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

5.1 Rationale for Extended Components

The IDS class was created because the Common Criteria standard classes do not have any Security Functional Requirements (SFR) that accurately described the unique capabilities of an intrusion prevention system.

5.2 Definition of Extended Components

5.2.1 Class IDS: Intrusion Detection System

Intrusion Detection System functions provide the capability to collect, review and manage event data.

5.2.1.1 System Data Collection (EXT) IDS_SDC

Family Behavior

This family defines the requirements to select the set of system events to be collected during TOE operation from the set of all collectable events.

Component Leveling

Management: IDS_SDC.1

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

a) maintenance of the rights to view/modify the system events.

Audit: IDS_SDC.1

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

b) Minimal: All modifications to the audit configuration that occur while the system data collection functions are operating.

IDS_SDC.1 (EXT) 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*]. (EXT)

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

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

b) The additional information specified in the *Details* column of Table Table 17 – System Events**. (EXT)**

Component	Event	Details
IDS_SDC.1	Start-up 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	Start-up 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	Detection known vulnerabilities	Identification of the known vulnerability

Table 17 – System Events

5.2.1.2 Analyser Analysis (EXT) IDS_ANL

Family Behavior

This family defines requirements for automated means that analyze analyser activity looking for possible or real intrusions. This analysis may work in support of intrusion detection, or automatic response to a potential intrusion.

Component Leveling

Management: IDS_ANL.1

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

a) maintenance (deletion, modification, addition) of the subset of analyser events.

Audit: IDS_ANL.1

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

b) Minimal: Enabling and disabling of any of the analysis mechanisms;
c) Minimal: Automated responses performed by the tool.

IDS_ANL.1 (EXT) Analyser 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*]. (EXT)**

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

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

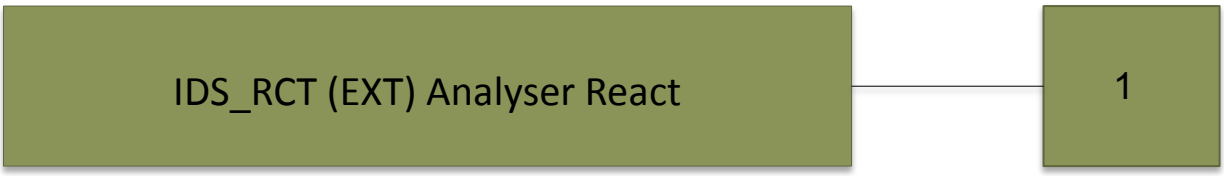
b. [assignment: *other security relevant information about the result*]. (EXT)

5.2.1.3 Analyser React (EXT) IDS_RCT

Family Behavior

This family defines the requirement the nature of the actions that must occur when an intrusion is detected.

Component Leveling



IDS_RCT.1 Analyser React, the TSF shall take actions in case an intrusion is detected.

Management: IDS_RCT.1

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

a) the management (addition, removal, or modification) of actions.

Audit: IDS_RCT.1

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

a) Minimal: Actions taken due to potential intrusions.

IDS_RCT.1 (EXT) Analyser React

Hierarchical to: No other components

Dependencies: No dependencies

IDS_RCT.1.1 The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when an intrusion is detected.

5.2.1.4 Restricted Data Review (EXT) IDS_RDR

Family Behavior

This family defines the requirements for system tools that should be available to authorized users to assist in the review of system data.

Component Leveling

IDS_RDR.1 Restricted data review, provides the capability to read information from the system records.

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.

Audit: IDS_RDR.1

The following actions should be auditable if FAU_GEN System data generation is included in the PP/ST:

a) Basic: Reading of information from the system data.

IDS_RDR.1 (EXT) Restricted Data Review

Hierarchical to: No other components

Dependencies: No dependencies

IDS_RDR.1.1 The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data. (EXT)

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

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

5.2.1.5 Management of System Data (EXT) IDS_STG

Family Behavior

This family defines the requirements for storing and protecting system data. This family identifies actions taken when the storage capacity has been reached.

Component Leveling

IDS_STG.1 Guarantee of system data availability, specifies the guarantees that the TSF maintains over the system data given the occurrence of an undesired condition.

Management: IDS_STG.1

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

a) maintenance of the parameters that control the system storage capability.

Audit: IDS_STG.1

There are no auditable events foreseen.

IDS_STG.1 (EXT) Guarantee of System Data Availability

Hierarchical to: No other components

Dependencies: No dependencies

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

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

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*]. (EXT)

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_SAR.3	Selective Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.2	Guarantees of audit data availability
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
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 the TSF	FPT_ITT.1	Basic Internal TOE TSF Data Transfer Protection
	FPT_STM.1	Reliable Time Stamps
IDS Component Requirements	IDS_SDC.1 (EXT)	System Data Collection
	IDS_ANL.1 (EXT)	Analyser Analysis
	IDS_RCT.1(EXT)	Analyser React (IDS)
	IDS_RDR.1 (EXT)	Restricted Data Review
	IDS_STG.1 (EXT)	Guarantee of System Data Availability

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;

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

d) [The events identified in Table 19 – Auditable Events]

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the additional information specified in the Details column of Table 19 – Auditable Events.

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FCS_CKM.1	Successful use of key generation function.	
FCS_CKM.4	Successful use of key destruction function.	
FCS_COP.1	Successful use of cryptographic operations.	

COMPONENT	EVENT	DETAILS
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 19 – Auditable Events

].

6.1.1.2 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [authorized administrators with permission to view reports on management actions] with the capability to read [all audit record detail identified in Table 19 – Auditable Events] 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_SAR.3– Selectable Audit Review

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

6.1.1.5 FAU_SEL. – Selective Audit

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

a) *event type*

b) [no additional attributes].

6.1.1.6 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to *detect* unauthorized modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that [the most recent, limited by available storage space] stored audit records will be maintained when the following conditions occur: *audit storage exhaustion*.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 – Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm algorithm [See Table 20 - Key Generation Algorithm in the table below] and specified cryptographic key sizes [See Key Sizes in the table below] that meet the following: [See Standards in the table below]

KEY GENERATION ALGORITHM	MODES	KEY SIZES	STANDARDS
AES	CBC	128,192, 256	FIPS 197

Table 20 - Key Generation Algorithm

6.1.2.2 FCS_CKM.4 – Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [Federal Information Processing Standard 140 requirements for key zeroization].

6.1.2.3 FCS_COP.1 – Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [AES 128- , 192- and 256-bit] that meet the following: [FIPS 197].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 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; and

d) User group memberships;

e) User assigned group permissions and group permission level].

6.1.3.2 FIA_UAU.1 – Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [no administrative 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.

6.1.3.3 FIA_UID.1 – Timing of Identification

FIA_UID.1.1 The TSF shall allow [no administrative 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.

6.1.4 Security Management

6.1.4.1 FMT_MOF.1 – Management of Security Functions Behavior

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

6.1.4.2 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]* ~~the~~ [all other TOE data] to [authorized administrators with explicit permissions to perform these actions].

6.1.4.3 FMT_SMF.1 – Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [of System data collection, analysis and reaction].

6.1.4.4 FMT_SMR.1 – Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrator, system administrator, and general user; see Section 7.5 – Security Management for more details].

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

6.1.5 Protection of the TOE Security Functions

6.1.5.1 FPT_ITT.1 – Basic Internal TSF Data Transfer Protection

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

6.1.5.2 FPT_STM.1 – Reliable Time Stamps

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

6.1.6 Traffic Analysis Component Requirements

6.1.6.1 IDS_SDC.1 – System Data Collection (EXT)

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

a) *network traffic*; and

b) [no 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 Table 21 – System Events. (EXT)

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Network traffic	Protocol, source address, destination address

Table 21 – System Events

6.1.6.2 IDS_ANL.1 – Analyser Analysis (EXT)

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

a) *Signature;* and

b) [matching to limited traffic flow rules via protocol anomaly analysis, behavioral anomaly analysis, and stateful protocol analysis].

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) [no other security relevant information about the result].

6.1.6.3 IDS_RCT.1– Analyser React (IDS Functionality)

IDS_RCT.1.1 The System shall send an alarm to [the Console] and take [the following actions: notify the administrator's designated personnel via email] when an intrusion is detected.

6.1.6.4 IDS_RDR.1 – Restricted Data Review

IDS_RDR.1.1 The System shall provide [administrators with permission to view reports for IDS events] with the capability to read [event 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.

6.1.6.5 [.1 – Guarantee of System Data Availability (EXT)

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 unauthorized modification

IDS_STG.1.3 The System shall ensure that [most recent, up to 1 million records] System data will be maintained when the following conditions occur: *System data storage exhaustion*.

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-Enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 22 – Security Assurance Requirements at EAL2

6.3 Security Requirements Rationale

The ST specifies Evaluation Assurance Level 2. EAL2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface.

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

6.3.1 Security Functional Requirements for the TOE

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

SFR \ OBJECTIVE	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.ENCRYPT	OE.TIME
FAU_GEN.1										✓			
FAU_SAR.1						✓							
FAU_SAR.2						✓	✓	✓					
FAU_SAR.3						✓							
FAU_SEL.1						✓				✓			
FAU_STG.2	✓						✓	✓	✓		✓		
FIA_ATD.1								✓					
FIA_UAU.1						✓	✓	✓					
FIA_UID.1						✓	✓	✓					
FCS_CKM.1												✓	
FCS_CKM.4												✓	
FCS_COP.1												✓	
FMT_MOF.1	✓						✓	✓					
FMT_MTD.1	✓						✓	✓			✓		
FMT_SMF.1	✓						✓	✓					
FMT_SMR.1								✓					
FPT_STM.1										✓			✓
FPT_ITT.1	✓												
IDS_SDC.1 (EXT)		✓	✓										
IDS_ANL.1 (EXT)				✓									
IDS_RCT.1 (EXT)					✓								
IDS_RDR.1 (EXT)						✓	✓	✓					
IDS_STG.1 (EXT)	✓						✓	✓	✓		✓		

Table 23 – Mapping of TOE SFRs to Security Objectives

6.3.2 Sufficiency of Security Requirements

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

OBJECTIVE	RATIONALE

OBJECTIVE	RATIONALE
O.PROTCT	The TOE is required to restrict the administrator console interfaces that can be used to delete audit data. The TOE is required to provide administrator console interfaces that can be used to detect modifications (administrators can compare system activity reports based on audit data generated at different points in time). [FAU_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, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1, FMT_SMF.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]. Data must be protected from disclosure and modification as it travels to and from distributed TOE components [FPT_ITT.1].
O.IDSCAN	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	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.IDANLZ	The Analyser is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].
O.RESPON	The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1 for IDS functionality and IDS_RCT.1 for IPS functionality].
O.EADMIN	The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1].

OBJECTIVE	RATIONALE
O.ACCESS	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the administrator console interfaces that can be used to delete audit data. The TOE is required to provide administrator console interfaces that can be used to detect modifications (administrators can compare system activity reports based on audit data generated at different points in time). [FAU_STG.2] The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1, FMT_SMF.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]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1].
O.IDAUTH	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the administrator console interfaces that can be used to delete audit data. The TOE is required to provide administrator console interfaces that can be used to detect modifications (administrators can compare system activity reports based on audit data generated at different points in time). [FAU_STG.2] The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.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, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1, FMT_SMF.1]. Only authorized administrators of the 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].

OBJECTIVE	RATIONALE
O.OFLOWS	The TOE is required to restrict the administrator console interfaces that can be used to delete audit data. The TOE is required to provide administrator console interfaces that can be used to detect modifications (administrators can compare system activity reports based on audit data generated at different points in time). [FAU_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, failure or attack [IDS_STG.1].
O.ENCRYPT	This objective to protect the confidentiality of its dialogue between distributed TOE components is completely satisfied by • FCS_CKM.1 which ensures that cryptographic keys and parameters are generated with standards-based algorithms. • FCS_CKM.4 which ensures that the cryptographic keys and parameters are safely destroyed. • FCS_COP.1 which ensures robust algorithms are used to support encrypted communications between users and the TOE.
O.AUDITS	[FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].
O.INTEGR	The TOE is required to restrict the administrator console interfaces that can be used to delete audit data. The TOE is required to provide administrator console interfaces that can be used to detect modifications (administrators can compare system activity reports based on audit data generated at different points in time). [FAU_STG.2] System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1].

Table 24 – Rationale for Mapping of TOE SFRs to Objectives

6.3.3 Requirements Dependency Rationale

The dependency requirements rationale is presented in Section 6.7 of the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This Security Target includes five Security Functional Requirements not included in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments; FMT_SMF.1, FPT_ITT.1, FCS_CKM.1, FCS_CKM.4 and FCS_COP.1. The requirement, FMT_SMF.1 was included to satisfy a dependency of FMT_MOF.1 and FMT_MTD.1 introduced in by International Interpretation RI#65 that was adapted in CC Part 2, v2.3 and is included CC v3.1. The SFR introduces no additional dependencies itself. The requirement, FPT_ITT.1 was included to support inter-communications in lieu of FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1. The requirement FPT_ITT.1 does not introduce any dependency requirements.

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

SFR	DEPENDENCY	DEPENDENCY MET	RATIONALE
FAU_GEN.1	FPT_STM.1	YES	Satisfied by the Operational Environment (OE.TIME)
FAU_SAR.1	FAU_GEN.1 FPT_STM.1	YES	FPT_STM.1 satisfied by the Operational Environment (OE.TIME)
FAU_SAR.2	FAU_SAR.1	YES	
FAU_SAR.3	FAU_SAR.1	YES	
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	YES	
FAU_STG.2	FAU_GEN.1	YES	
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	YES	Satisfied by FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_IDC.2 or FCS_CKM.1	YES	Satisfied by FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_IDC.2 or FCS_CKM.1] and FCS_CKM.4	YES	Satisfied by FCS_CKM.1 and FCS_CKM.4
FIA_ATD.1	N/A	N/A	
FIA_UAU.1	FIA_UID.1	YES	
FIA_UID.1	N/A	N/A	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_SMF.1	N/A	N/A	
FMT_SMR.1	FIA_UID.1	YES	
FPT_STM.1	N/A	N/A	
FPT_ITT.1	N/A	N/A	
IDS_SDC.1 (EXT)	N/A	N/A	
IDS_ANL.1 (EXT)	N/A	N/A	
IDS_RCT.1 (EXT)	N/A	N/A	
IDS_RDR.1 (EXT)	N/A	N/A	
IDS_STG.1 (EXT)	N/A	N/A	

Table 25 – Dependency Rationale

6.3.4 Extended Requirements Rationale

There are no extended requirements beyond those in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

The extended requirements rationale is presented in Section 6.5 of the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

6.3.5 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 EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Security Architecture Description: McAfee Nitro Intrusion Prevention System 9.1
ADV_FSP.2: Security-Enforcing Functional Specification	Function Specification: McAfee Nitro Intrusion Prevention System 9.1
ADV_TDS.1: Basic Design	Basic Design: McAfee Nitro Intrusion Prevention System 9.1
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Nitro Intrusion Prevention System 9.1
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Nitro Intrusion Prevention System 9.1
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Nitro Intrusion Prevention System 9.1
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Nitro Intrusion Prevention System 9.1
ALC_DEL.1: Delivery Procedures	Secure Delivery Processes and Procedures: McAfee Nitro Intrusion Prevention System 9.1
ALC_FLR.2: Flaw Reporting	*McAfee Product Flaw Remediation Process*
ATE_COV.1: Evidence of Coverage	Test Plan and Coverage Analysis: McAfee Nitro Intrusion Prevention System 9.1
ATE_FUN.1: Functional Testing	Test Plan and Coverage Analysis: McAfee Nitro Intrusion Prevention System 9.1
ATE_IND.2: Independent Testing – Sample	N/A
AVA_VAN.2: Vulnerability Analysis	N/A

Table 26 – Security Assurance Rationale and Measures

7 TOE Summary Specification

7.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 6.1 – Security Functional Requirements. The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- TSF protection
- Intrusion detection

7.2 Security Audit

The IPS and ESM subsystems each generate three types of logs. These logs are used to store audit records (in the event log) and to store collected data event information (in the traffic alert log and in the traffic flow log). The event log contains records not related to traffic alerts or traffic flow such as TOE management events. The event log is the TOE's log containing the audit trail.

- *event log*
  - Generated by ESM (when using GUI) and IPS (when receiving commands from ESM)
  - Records generated by IPS are sent to ESM periodically in batches for storage and review on ESM. The records are protected during transmission using the proprietary stackless control protocol called SEM (Secure Encrypted Management). The communication between the ESM and the IPS is always initiated by the ESM. The audit trail is protected by the ESM subsystem and is protected from unauthorized logical access by restricting access to the ESM web-based GUI interface that is used to read from the audit trail. There are no interfaces (not ESM web-based GUI interfaces or otherwise) to modify audit records stored in the audit trail.
  - Maximum event log size on IPS and ESM is one million records on all supported IPS and ESM

The audit records received by the ESM are stored in the ESM subsystem's event log. The ESM subsystem's event log is also known as the audit trail. The audit trail is protected by the ESM subsystem. The audit trail is protected from unauthorized logical access by restricting access to the ESM web-based GUI interface that is used to read from the audit trail. There are no interfaces (not ESM web-based GUI interfaces or otherwise) to modify audit records stored in the audit trail.

The ESM provides web-based GUI interfaces to configure auditable events. Events are grouped into categories that correspond to sets of ESM GUI dialogs, menus, and screens. Each category will have a checkbox that allows the user to enable/disable logging of each event category. If a category is disabled, no events that are a part of that category will be logged. The auditable event types include:

- Authentication category - Login, logout, and any user account changes
- Backup category - Database backup process
- Blacklist category - Sending blacklist entries to the device
- Device category - Any device changes or communications such as getting events, flows and logs
- Event Forwarding category - Event forwarding changes or errors
- Health Monitor category - Device status events
- Notifications category - Notification changes or errors
- Policy category - Policy management and applying policies
- Rule Server category - Download and validation of rules downloaded from the rule server
- System category - System setting changes and table rollover logging
- Views category - Changes to views and queries

In addition to the list of events above, it should be noted that audit is always on and hence the start-up and shutdown audit is fulfilled vacuously, however there is a system log that identifies the start and stop of various TOE components.

The ESM provides the only administrative interface to all audit events related to system management that occur on the ESM. The IPS subsystems role in creating audit records is limited to responding to audit storage failure and other exception based audited activity.
The ESM web-based GUI interfaces that can be used to read from the event log allow for selecting events to display within an administrator-configurable time period. When event log records (i.e., audit records) are displayed after a time period has been selected, the following information is displayed for each record:

- time of the event
- user name
- status of the event (IPS events only), which can be any one of:
  - critical
  - warning
  - informational
- location (i.e. IPS or ESM identifier) of the event (is blank if ESM)
- description (details) of the event

When the event log reaches its maximum size, it begins overwriting the oldest stored records. There is an alarm mechanism to alert the administrator when the log runs out of space.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit events for the basic level of audit. Note that the IDS_SDC and IDS_ANL requirements address the recording of results from IDS scanning, sensing, and analyzing tasks (i.e., System data).
- FAU_SAR.1: The TOE provides administrator console interfaces that can be used by authorized administrators and general users that possess permissions that allow access to read the audit trail.

- FAU_SAR.2: The TOE restricts access to the audit trail to authorized administrators and general users that possess permissions that allow access to read the audit trail using administrator console interfaces.
- FAU_SAR.3: The TOE provides administrator console interfaces that can be used to sort audit data. The administrator console interfaces that can be used to sort audit data do not include a separate type of event field. However, there is a "status" field provided by the administrator console that corresponds to IPS component status event types (which include critical, warning, and informational event types).
- FAU_SEL.1: The TOE provides administrator console interfaces that can be include or exclude auditable events based on event type. Note the event type is the audit categories.
- FAU_STG.2: The TOE restricts administrator console interfaces that can be used to delete audit data. The TOE provides administrator console interfaces that can be used to detect modifications (administrators can compare system activity reports based on audit data generated at different points in time).

7.3 Cryptographic Support

The TOE encrypts communications between the ESM and IPS components using AES 256 CBC. ESM and the Console communicate over HTTPS using either AES 125, 192 or 256 CBC. The Console uses a web browser that supports one of these algorithms.

The following table summarizes the cryptographic security functions of FIPS mode.

Security Function	Purpose or Use	Certificate
Approved Security Functions		
AES (FIPS PUB 197) CBC	TLS encryption and decryption.	32-bit Virtual - 2228 64-bit Virtual - 2231

Table 27 – Security Function, Use and Certificate

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1
- FCS_CKM.4
- FCS_COP.1

7.4 Identification and Authentication

There is a single authorized administrator account that can be used to create what are called general user accounts. The authorized administrator may grant general users other privileges (elevating them to

a system administrator role) by creating access groups and assigning users to these groups. However, there are operations such as creating general user accounts that only the authorized administrator account can perform even if a general user were to be assigned all available privileges. Group membership and the permissions assigned to the group by the authorized administrator determines what ESM web-based GUI interfaces a user may access. The ESM stores user account information. User account information is logically protected by the TOE. User account information includes username, password, and group information. Note the terms permissions and privileges are synonymous with authorizations.

Assignable permissions include:

- Add/Delete Devices - Add/remove IPS devices to/from the system.
- Add/Delete Policies - Add/remove/rollback rule policies to/from the system.
- Custom Rules and Variables - Add, modify and delete custom rules, blacklist, and variables.
- Device Management - Configure settings and perform operations on IPS devices.
- ESM Configuration - Configure settings and perform operations on the ESM device.
- Event Management - Management of alert and flow data in addition to all rights of Reporting.
- Notifications - Add, modify and delete notifications and event forwarding destinations.
- Policy Administration - Manage policy settings for IPS devices.
- Reporting - Execute reports and retrieve alert, flow and log data from the IPS devices.
- System Management - Configure system wide settings.
- View Management - Add, modify and delete views in addition to all rights of Reporting.
- Network Port Control – Ability to reconfigure ports on network infrastructure devices (e.g. disable port).
- FIPS Self-Test – Ability to initiate a FIPS self-test on the ESM and IPS devices.

When a user attempts to log into the ESM web-based GUI interface, a username and password are required. If the identification and authentication method specified is defined locally, the TOE will identify and authenticate the user provided the username and password matches the stored attributes. No administrative actions are allowed until the user has been successfully identified and authenticated.

The authorized administrator can set the Allowed Failed Login Attempts value specifies the number of consecutive unsuccessful logins that will be allowed in a single session before the user attempting to login has their account locked. Once a user has their account locked, the system administrator must unlock their account via the Users and Groups section, before that user will be allowed to login again. The default value is three (3).

The ESM web-based GUI interface provides interfaces for users to change their own passwords. The ESM requires passwords to be at least eight characters from the printable character set. Passwords must also include at least one uppercase letter, at least one numeric digit (i.e. 0 thru 9), and at least one non-letter/non-digit (i.e. symbols and/or punctuation marks). The ESM GUI enforces these password composition rules.

The IPS cannot be accessed directly. Their system data collection interfaces are invoked upon receipt of monitored network traffic. The IPS appliances are managed using the ESM appliance, which can only be accessed after a user successfully logs into the ESM appliance using a username and password.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE maintains user identities (user id), authentication data (passwords), authorization (permission/privileges), group information (group/role membership), and alert notification data (e-mail address for alert notification).
- FIA_UAU.1: The TOE offers no TSF-mediated functions until the user is authenticated.
- FIA_UID.1: The TOE offers no TSF-mediated functions until the user is identified.

7.5 Security Management

The ESM provides a GUI to administer the IPS. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction. System data consists of results from IPS scanning, sensing and analyzing tasks. The administrator can use the default policies and rules or using the Policy Manager, the administrator can add new rules and policies, edit the rules and policies, import policies, delete policies, change the rule history, etc. For a complete list of functions and capabilities, see the McAfee Enterprise Security Manager Interface Users Guide.

The administrator console can also be used to manage audit data and user accounts. Management functions correspond to the list of assignable permissions that can be found in section 6.1.2, and include the functions of creating and deleting general user accounts and assigning and removing permissions by the system administrator.

The TOE has three user accounts: authorized administrator, system administrators, and general user. The authorized administrator role is the account that can be used to create general user accounts. The System administrator role corresponds to general user accounts that have been assigned one or more permissions by the authorized administrator. Multiple system administrators may exist, each with differing permissions. The general user role corresponds to general user accounts that have not been assigned any permissions by the authorized administrator.

The TOE restricts access to its interfaces by requiring users to log into the ESM appliance using its GUI, and by encrypting commands sent from the ESM appliance to the IPS appliances. HTTPS is also used to protect the connection between the web browser in the operational environment and the ESM appliance. When the TOE is configured in FIPS mode then all traffic between the ESM and IPS is tunneled through a FIPS certified VPN tunnel and the HTTPS uses a FIPS certified crypto function. The evaluated configuration supports only FIPS mode.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: The TOE restricts the ability to modify the behavior of the functions of System data collection, analysis and reaction by restricting access to administrator console interfaces.
- FMT_MTD.1: The TOE restricts the ability to query and add System data and audit data to authorized administrators. Note that only authorized administrators can query or modify any other types of TOE data, as well.

- FMT_SMF.1: The TOE provides authorized administrators with the ability to manage functions and data related to scanning, sensing, and analyzing tasks, as well as the ability to manage audit data and user accounts.
- FMT_SMR.1: The authorized administrator role corresponds to the single system administrator account that can be used to create general user accounts. The authorized System administrator role corresponds to general user accounts that have been assigned one or more permissions by the authorized administrator. The general user role corresponds to general user accounts that have not been assigned any permissions by the authorized administrator.

7.6 Protection of the TSF

The TOE restricts access to its interfaces by requiring users to log into the ESM using its GUI, and by encrypting commands sent from the ESM to the IPS. HTTPS is also used to protect the connection between the web browser in the operational environment and the ESM. The ESM supports HTTP v1.1 using TLS v1.0. The communication between the ESM and the IPS is always initiated by the ESM. The evaluated configuration supports only the TOE in FIPS mode of operation.

Before the TOE is installed and configured, the IPS and ESM components are preconfigured with different types of cryptographic keys for use with SEM and with HTTPS. During TOE installation and initial configuration, IPS keys on both IPS and ESM appliances are replaced with newly generated keys. The SSL keys and certificate are also replaced with newly generated keys and certificate during TOE installation and initial configuration. The evaluated configuration supports only FIPS mode.

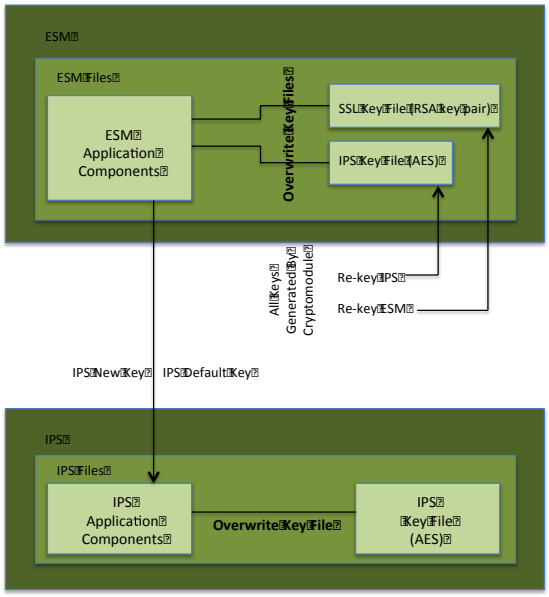


Figure 4: IPS and ESM Keying

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: The TOE encrypts commands sent from the ESM to the IPS. HTTPS is also used to

protect the connection between the web browser in the operational environment and the ESM.

- FPT_STM.1: The hardware for each subsystem includes its own hardware clock that provides reliable time stamps for use in audit and collected data records generated by that subsystem. The clock in the IPS subsystem can only be set by a command from the ESM.

7.7 Intrusion Detection (EXT)

IPS is an Open System Interconnection (OSI) Layer 2 component and can be configured without an IP address, if the TOE is not in FIPS mode. Without an IP address, the device will not respond to pings, traceroutes, or any other high-level mechanics, nor will it respond to ARP requests or any other low-level mechanics.

The TOE can be installed in the following locations in the network architecture of the operational environment:

- *Outside the firewall location* – The TOE is placed between the external interface of the firewall and the border router.
- *DMZ location* – The TOE is placed between the DMZ interface on the firewall and whatever network exists as part of the DMZ.
- *VPN concentrator in DMZ location* – The TOE is placed between the internal interface of the concentrator and the internal switch into which it feeds. This is the only way to examine unencrypted traffic of VPN users on networks set up in this manner.
- *Inside the firewall location* – The TOE is placed between the internal interface of the firewall and the internal switch into which it feeds.
- *IDS Mode location* – The TOE is placed on a mirrored port in any network location.

IPS can detect different types of intrusion attempts by performing analysis of network traffic packets depending on location within a network. The TOE supports installation in different locations in the network architecture of the TOE environment by providing the ability to operate in one of three modes:

- IPS mode (supported when the TOE is located *in-line*)
- Alerts-only mode (supported when the TOE is located *in-line*)
- IDS mode (supported when the TOE is located *in-tap*)

When IPS is located in-line it can operate in what is called an IPS mode. IPS mode consists of the device being located in-line while functioning as an IPS, i.e. the device can drop, pass, reject network traffic according to policy. IPS is placed inline between two devices (i.e., a firewall and a switch) using network cables. All traffic that enters IPS through its physical network interfaces is picked up by iptables for firewall policy rule inspection. The firewall policy rules are checked in order of resulting action in the following order: pass, reject, drop, and alert. If the packet was not passed, rejected, or dropped, it is

passed to Snort for deep packet inspection (i.e. payload). The Snort rules are checked in the same order as the firewall rules: pass, reject, drop, and alert.

When IPS is located in-line it can operate in what is called an alerts-only mode. Alerts-only operating mode consists of IPS being located in-line while functioning as an IDS, i.e. the device can monitor network traffic but not affect it. IPS is placed inline between two devices (i.e., a firewall and a switch) using network cables. All traffic that enters IPS through its physical network interfaces is picked up by iptables for firewall policy rule inspection. The firewall rules are checked in order of resulting action in the following order: pass, reject, drop, and alert. However, in alerts-only mode, pass, reject, and drop actions for each rule are replaced with the alert action. The packet is then always passed to Snort for deep packet inspection. The Snort rules are checked in the same order as the firewall policy rules: pass, reject, drop, alert. However, as with firewall policy rules, in alerts-only mode, the deep packet inspection policy check rule actions are replaced with the alert action and the packet is always passed thru.

When IPS is located in-tap it can operate in what is called an IDS mode. IDS mode (also called passive operating mode) consists of the device being located in-tap while functioning as an IDS, i.e. the TOE can monitor network traffic but not affect it. IPS is placed on a span port of a switch using a network cable. Any traffic that enters the switch is passed through the span port, as well as the actual output port. All traffic that enters IPS through the physical network interface is picked up by iptables for firewall rule inspection. Because the device is not inline, no action other than alert can be taken. After firewall policy rules are checked, the packets are passed on to Snort for checking against the deep packet inspection policy rules.

IPS performs signature analysis, protocol anomaly analysis, behavioral anomaly analysis, and stateful protocol analysis on collected network traffic data and records corresponding network traffic event data when operating in any one of its operating modes. The TOE retrieves authenticated and encrypted signature updates from the IPS central server via an encrypted communication mechanism. Mechanisms, both hardware and software based, are in place to ensure that devices are managed only from properly authorized views

- *Signature analysis* of network traffic packets consists of identifying deviations from normal patterns of behavior using patterns corresponding to known attacks or misuses, e.g. comparing user activity against a database of known attacks
- *Protocol anomaly analysis* of network traffic packets filters each packet to identify deviations from normal patterns of behavior
- *Behavioral anomaly analysis* of network traffic packets consists of identifying deviations from normal patterns of behavior using tracking of all packet statistics including burst rates, bytes and packets per second, threshold limit alerts, source and destination IP addresses and ports, and protocols
- *Stateful protocol analysis* and what is called connection tracking of network traffic packets

consists of identifying deviations from normal patterns of behavior by monitoring and analyzing all packets within a connection or session

The TOE's ESM administrator console provides the ability to examine analytical conclusions drawn by the TOE that describe the conclusion and identifies the information used to reach the conclusion. The IPS and ESM generates three types of logs to store collected data event information:

- *traffic alert log* – these are events that occur when packets match a rule, i.e. this is collected data
    - Records generated by IPS are sent to ESM periodically in batches for storage on ESM.
    - Maximum log size on IPS and ESM depends on the environment:
- *traffic flow log* – these are events that occur when connections are made between targeted IT systems in general (i.e. a flow is not associated with an IDS rule), i.e. this is collected data
    - Records generated by IPS are sent to ESM periodically in batches for storage on ESM
    - Maximum log size on IPS and ESM depends on the environment:
- *device location log* – this data is associated with the location of network infrastructure and end-station devices automatically discovered by, and manually entered into, the ESM
    - There's no practical maximum log size
    - All location data is stored

The IPS devices receive requests for alerts and flows from the ESM containing the date of the last retrieval. All requested data since the date passed are retrieved and passed back to the ESM. IPS can also be configured to automatically send out Syslog messages and SNMP traps when an alert is triggered. IPS devices receive configuration data for Syslog servers and SNMP managers from the ESM, including an alert rate. This data is used for sending Syslog messages and SNMP traps whenever an alert is logged, not to exceed the specified rate. The ESM can generate email SNMP traps, syslog, and text log files. To setup the notifications, the user must be assigned to the System administrator role. The user can configure the conditions/events that will cause a notification to be generated. Conditions or events can include, specified event rate, specified date/time, FIPS compliance failure, device failure, etc. When sending notifications via e-mail, SNMP or syslog, a recipient must be identified. For e-mail, the e-mail address of the person or group that will receive the e-mail must be entered. Recipients can be added or removed as necessary. SNMP uses User Datagram Protocol (UDP) as the transport protocol. It should be noted that due to size limitations of the SNMP trap packets, each line of the notification report is sent in a separate trap. Syslog uses the standard for forwarding log messages in an IP network. Notifications can also be appended to a text file that is stored on the ESM. The information contained in a notification can consist of the results of any query for any combination of devices over any desired time range. The alarm mechanisms used when reacting to collected data may also be used when reacting to audit mechanism events, if the TOE has been configured to do so.

When either of the logs reaches their respective maximum size, they begin overwriting the oldest stored records. There is an alarm mechanism to alert the administrator when the logs run out of space.

The IDS function is designed to satisfy the following security functional requirements:

- IDS_SDC.1: The TOE collects network traffic data for use in scanning, sensing, and analyzing functions, acting as an IDS sensor. Note that different types of network traffic can be collected depending on the TOE‟s location within a network. Also, note that host-based events may be collected for network switches.
- IDS_ANL.1: The TOE performs signature analysis, protocol anomaly analysis, behavioral anomaly analysis, and stateful protocol analysis on collected network traffic data and records corresponding network traffic event data when operating in any one of its operating modes. . Note that the administrator console provides the ability to examine analytical conclusions drawn by the TOE that describe the conclusion and identifies the information used to reach the conclusion.
- IDS_RCT.1: The TOE provides the ability to generate alert and notify an authorized administrator using a configured notification mechanism when an intrusion is detected. The TOE also provides the ability to automatically pass or reject packets (and connections) based on rule configuration when an intrusion is detected.
- IDS_RDR.1: The TOE provides authorized administrators and general users that possess permissions that allow access the ability to review results from IDS scanning, sensing, and analyzing tasks (i.e., System data) using the administrator console.
- IDS_STG.1: The TOE ensures that the most recent system data is always able to be recorded, when the system data storage space is exhausted, the oldest events stored in the system data store will be overwritten.