U.S. Government Protection Profile

Intrusion Detection System System

For

Basic Robustness Environments

Information
Assurance
Directorate

Version 1.7

July 25, 2007

Foreword

This publication, Basic Robustness Intrusion Detection System System Protection Profile, is issued by the National Security Agency as part of its program to promulgate security standards for information systems.

Protection Profile Title:

U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments

Criteria Version:
This Protection Profile *"U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments"* (PP) was updated using Version 3.1 of the Common Criteria (CC).

Editor's note: The purpose of this update was to bring the PP up to the new CC 3.1 standard without changing the authors' original meaning or purpose of the documented requirements. The original PP was developed using version 2.x of the CC. The CC version 2.3 was the final version 2 update that included all international interpretations. CC version 3.1 used the final CC version 2.3 Security Functional Requirements (SFR)s as the new set of SFRs for version 3.1. Some minor changes were made to the SFRs in version 3.1, including moving a few SFRs to Security Assurance Requirements (SAR)s. There may be other minor differences between some SFRs in the version 2.3 PP and the new version 3.1 SFRs. These minor differences were not modified to ensure the author's original intent was preserved.

The version 3.1 SARs were rewritten by the common criteria international community. The NIAP/CCEVS staff developed an assurance equivalence mapping between the version 2.3 and 3.1 SARs. The assurance equivalent version 3.1 SARs replaced the version 2.3 SARs in the PP.

Any issue that may arise when claiming compliance with this PP can be resolved using the observation report (OR) and observation decision (OD) process.

Further information, including the status and updates of this protection profile can be found on the CCEVS website: http://www.niap-ccevs.org/cc-scheme/pp/. Comments on this document should be directed to ppcomments@missi.ncsc.mil. The email should include the title of the document, the page, the section number, the paragraph number, and the detailed comment and recommendation.

TABLE OF CONTENTS

List of Tables

Intrusion Detection System System Protection Profile

1 PROTECTION PROFILE (PP) INTRODUCTION

1.1 INTRODUCTION

This section contains document management and overview information necessary to allow a Protection Profile (PP) to be registered through a Protection Profile Registry. The identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The overview can also be used as a stand-alone abstract for PP catalogues and registers. The Conventions section provides an explanation of how this document is organized. The Terms section gives a basic definition of terms, which are specific to this PP. Finally, the Related Profiles section identifies profiles directly related to this profile and may be of interest to those interested in this profile.

1.2 IDENTIFICATION

Title: U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments

Sponsor: National Security Agency (NSA)

Common Criteria Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2006

PP Version 1.7

Keywords: intrusion detection, intrusion detection system, analyzer, sensor, scanner

Evaluation Assurance Level (EAL) – EAL 2 Augmented with ALC_FLR.2

1.3 OVERVIEW

The Common Criteria (CC) Intrusion Detection System System Protection Profile specifies a set of security functional and assurance requirements for Information Technology (IT) products. An Intrusion Detection System (IDS) monitors an IT System for activity that may inappropriately affect the

IT System's assets. An IT System may range from a computer system to a computer network. An IDS System (System) consists of Sensors, Scanners and Analyzers (i.e., IDS components). Sensors and Scanners collect information regarding IT System activity and vulnerabilities, and they forward the collected information to Analyzers. Analyzers perform intrusion analysis and reporting of the collected information.

Intrusion Detection System System Protection Profile-conformant products support the ability that monitor (both real-time and statically) an IT System for activity that may inappropriately affect the IT System's assets and react appropriately. Intrusion Detection System System Protection Profile-conformant products also provide the ability to protect themselves and their associated data from unauthorized access or modification and ensure accountability for authorized actions.

The IDSSPP provides for a level of protection which is appropriate for IT environments that require detection of malicious and inadvertent attempts to gain inappropriate access to IT resources, where the System can be appropriately protected from hostile attacks. Though products that are Intrusion Detection System System Protection Profile-conformant can be used to monitor and analyze a system or network in a hostile environment, they are not designed to resist direct, hostile attacks. The Intrusion Detection System System Protection Profile does not fully address the threats posed by malicious administrative or system development personnel. This profile is also not intended to result in products that are foolproof and able to detect intrusion attempts by hostile and well-funded attackers. Intrusion Detection System System Protection Profile-conformant products are suitable for use in both commercial and government environments.

The Intrusion Detection System System Protection Profile was constructed to provide a target and metric for the development of Systems. This PP identifies security functions and assurances that represent the lowest common set of requirements that should be addressed by a useful IDS System.

The Intrusion Detection System System Protection Profile is generally applicable to products regardless of whether they are embedded, stand-alone, centralized, or distributed. However, it addresses only security requirements and not any special considerations of any particular product design.

STs that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance as defined in section D3 of part 1

1.4 CONVENTIONS

The requirements in this document are divided into assurance requirements and two sets of functional requirements. The first set of functional requirements, which were drawn from the Common Criteria, is designed to address the core System requirements for self-protection. The second set of requirements, which were invented and categorized by the short name, IDS, is designed to address the requirements for the System's primary function, which is IDS collection of data and responses to conclusions based upon that data.

The CC permits four functional component operations—assignment, refinement, selection, and iteration —to be performed on functional requirements. This PP will highlight the four operations in the following manner:

- assignment: allows the specification of an identified parameter. Indicated with bold text and italics if further operations are necessary by the Security Target author;
- refinement: allows the addition of details. Indicated with bold text and italics if further operations are necessary by the Security Target author;
- selection: allows the specification of one or more elements from a list. Indicated with underlined text; and
- iteration: allows a component to be used more than once with varying operations. Not used in this PP.

In addition, this PP has extended requirements. These new requirements are indicated in bold text and contain the text (EXT) in the title.

1.5 DOCUMENT ORGANIZATION

Section 1 provides the introductory material for the protection profile.

Section 2 describes the Target of Evaluation in terms of its envisaged usage and connectivity.

Section 3 defines the expected TOE security environment in terms of the threats to its security, the security assumptions made about its use, and the security policies that must be followed.

Section 4 identifies the security objectives derived from these threats and policies.

Section 5 identifies and defines the security functional requirements from the CC that must be met by the TOE and the IT environment in order for the functionality-based objectives to be met. This section also identifies the security assurance requirements for EAL2 augmented.

Section 6 provides a rationale to demonstrate that the Information Technology Security Objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirement. Arguments are provided for the coverage of each objective.

Section 7, Appendices, includes the appendices that accompany the PP and provides clarity and/or explanation for the reader.

Appendix A, References, provides background material for further investigation by users of the PP.

Appendix B, Glossary, provides a listing of definitions of terms.

Appendix C, Acronyms, provides a listing of acronyms used throughout the document.

Appendix D, Robustness Environment Characterization, contains a discussion characterizing the level of robustness TOEs compliant with the PP can achieve. The PPRB created a discussion that provides a definition of factors for TOE environments as well as an explanation of how a given level of robustness is categorized.

1.6 RELATED PROTECTION PROFILES

U.S. Government Protection Profile Intrusion Detection System Scanner for Basic Robustness Environments
U.S. Government Protection Profile Intrusion Detection System Sensor for Basic Robustness Environments
U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments

2 TARGET OF EVALUATION (TOE) DESCRIPTION

This Protection Profile specifies the minimum security requirements for a TOE that is a System. A System is one or more Sensors and/or Scanners, and one or more Analyzers. A System monitors an IT System for activity that may inappropriately affect the IT System's assets, performs analysis on the data it collects, and reacts appropriately. The information collected may be obtained from a variety of sources located on an IT System. Similarly, the response functions may affect one or more targets on the IT System.

Sensors must be able to:

- Collect data about all events as they occur on an IT System. Events may include authentication events; data access events; configuration access events; service requests; network traffic; data introduction; and, start-up and shutdown of audit functions.
- Forward all collected data to an authorized Analyzer for data reduction and analysis.

Scanners must be able to:

- Collect static configuration information about an IT System. Configuration information may include detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, and detected known vulnerabilities.
- Forward all collected configuration information to an authorized Analyzer for data reduction and analysis.

Analyzers must be able to:

- Receive data from identified Sensors and Scanners.
- Process specified data to make intrusion/vulnerability determinations.
- Respond to identified intrusions/vulnerabilities. Such responses may include report generation, visual signals/alarms, audible signals/alarms, configuration changes, and/or invocation of remote warnings.

All IDS components must be able to:

- Protect themselves and their data from tampering.
- Be configured by an authorized user.
- Produce an audit trail (e.g., configuration changes, component and data accesses).

Any IT System that needs to be aware of vulnerabilities and cyber attacks should deploy an IDS. The IDS monitors itself as well as its target IT System. The IT System must provide adequate protection for the IDS so that the IDS operates in a non-hostile environment. The following diagrams illustrate examples of how an IDS (represented by a star) may be utilized by IT Systems ranging from a computer system to a computer network. Figure-1 illustrates that an IDS may monitor and exist in a computer system that is not necessarily part of a larger network. Figure-2 illustrates that an IDS may monitor and exist within a computer network. The arrows represent the monitoring functionality of the IDS as opposed to the implementation of the computer network.

Figure-1. Computer System

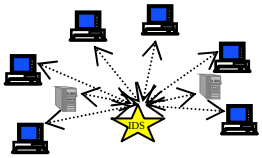


Figure-2. Computer Network

This PP makes a distinction between the System and TOE. The term System is used when the PP is referring to the ID monitoring, analysis, and reaction mechanisms as specified by the IDS security function requirements Class. When the term TOE is used, the PP is referring to the complete IT product that implements all TOE Security Function Requirements necessary to ensure accountability and protection for the ID monitoring, analysis, and reaction capabilities.

3 TOE SECURITY ENVIRONMENT

The TOE described in this PP is intended to operate in environments having a basic level of robustness as defined in the Glossary in Appendix B.

Basic robustness allows processing of data at a single sensitivity level in an environment where users are cooperative and threats are minimal. Authorized users of the TOE are cleared for all information managed by the IDS component, but may not have the need-to-know authorization for all of the data. Hence, the risk that significant damage will be done due to compromise of data is low.

Entities in the IT environment on which the TOE depends for security functions must be of at least the same level of robustness as the TOE. It is necessary for such an environment that the underlying operating system on which the IDS component is installed be evaluated against a basic robustness protection profile for operating systems.

The TOE in and of itself is not of sufficient robustness to store and protect information of such criticality that the integrity or secrecy is critical to the survival of the enterprise.

3.1 ASSUMPTIONS

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

3.1.1 Intended Usage Assumptions

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

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

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

3.1.2 Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will

be protected from unauthorized physical modification.

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

3.1.3 Personnel Assumptions

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

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

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

3.2 THREATS

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

3.2.1 TOE Threats

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

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

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

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

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

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

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

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

3.2.2 IT System Threats

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

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

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

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

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

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

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

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

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

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

3.3 ORGANIZATIONAL SECURITY POLICIES

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

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

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

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

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

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

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

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

4 SECURITY OBJECTIVES

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

4.1 INFORMATION TECHNOLOGY (IT) SECURITY OBJECTIVES

The following are the TOE security objectives:

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

O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

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

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

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

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

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

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

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

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

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The TOEs operating environment must satisfy the following objectives.

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

OE.AUDIT_SORT The IT Environment will provide the capability to sort the audit information

OE.TIME The IT Environment will provide reliable timestamps to the TOE.

OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

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

OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

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

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

5 IT SECURITY REQUIREMENTS

This section defines the functional requirements for the TOE. Functional requirements in this PP were drawn from Part 2 of the CC. These requirements are relevant to supporting the secure operation of the TOE. Functional requirements pertaining to the System collection, analysis, and reaction mechanisms were invented and are identified by the short name IDS.

The functional security requirements for the PP consist of the following components, summarized in Table 1 TOE Functional Components.

Functional Components	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.2	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
FIA_UAU.1	Timing of authentication
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT_ITA.1	Inter-TSF availability within a defined availability metric
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_STM.1	Reliable time stamps
IDS_SDC.1	System Data Collection
IDS_ANL.1	Analyzer analysis
IDS_RCT.1	Analyzer react
IDS_RDR.1	Restricted Data Review
IDS_STG.1	Guarantee of System Data Availability
IDS_STG.2	Prevention of System data loss

Table 1 TOE Functional Components

5.1 PP APPLICATION NOTE USAGE

5.1.1 Usage

This PP defines the requirements for an IDS System composed of Sensors, Scanner, and Analyzers. There are component-level PPs for all three of the System components. This PP provides guidance for users in the form of *family application notes* to assist in applying the functional requirements in a System context. Products may be evaluated against the System PP, one or more component PPs, or a combination. If a product has already satisfied one of the component PPs, the family application notes in this PP describe how the results from the previous component evaluation could be reused in a System evaluation.

This PP does not address the traditional issue of how composing multiple evaluated products affects the evaluation status of each product. The evaluation community considers composing evaluated products a research issue and there is no international agreement on a direction in this arena. For these reasons, this PP does not attempt to levy requirements for the traditional composition of IDS components.

5.1.2 Composition Philosophy

This protection profile includes a number of *family application notes* that are intended to provide some insight for incorporating available component information into the system product. These application notes are directed at Security Target (ST) authors and those that would create and/or evaluate evidence for the System TOE. These application notes are only applicable if detailed information (the ST and evaluator work units) from one or more component evaluations can be obtained by those involved with the System evaluation. Furthermore, the application notes are only valid if accepted by the National Information Assurance Partnership (NIAP) oversight body.

The ST author may benefit from existing component evaluations by adapting refinements in the related component STs into composite System ST requirement refinements. While creation of the System ST can be expedited to some degree, it is not clear that any savings can be achieved when it comes to evaluating the System ST.

Those involved with evidence may benefit by either not having to reproduce existing evidence or to reevaluate existing evidence. It is offered that ideally the component evidence (i.e., that which supported the component evaluation) would not have to be reproduced at all, including obtaining it from an OEM in order to support the evaluation of an

integrated System product. It is also intended that the information would not have to be reevaluated, provided that the previous component evaluation conclusions can be demonstrated to be valid. Note that this will require evidence, up to and including all of the information that went into the original evaluation, to perform the necessary analysis and demonstrate the validity. In some instances, it may be the case that validating a previous conclusion would require more work than the initial evaluation. Hence, it is recommended that careful consideration must be involved when making the decision to reuse results rather than reproducing them. The objective here is to provide an alternate means, that may in some cases be more efficient or practical, to achieve the same evaluation goal.

The application notes provide some general guidance, but here are other general guidelines that must be understood in order to apply them appropriately. If any component has not been evaluated, or its information cannot be obtained or validated, then that component must be evaluated entirely in the context of the System. While results from component evaluations may be generally applicable to a System evaluation, it is possible there may be components that have a very significant impact on other components; thereby invalidating any results from one or more of the components involved. In general, the more disjoint the components, the more applicable and valid their results will be.

Note that this protection profile does not attempt to address the issues of NIAP acceptability of evidence and conclusion reuse, nor does it attempt to address the issue of obtaining detailed evaluation work units that may be produced by different organizations.

5.2 SECURITY AUDIT (FAU)

5.2.1 FAU_GEN.1 Audit data generation

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

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

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

c) **Access to the System and access to the TOE and System data**. FAU_GEN.1.1

Application Note: The auditable events for the basic level of auditing are included in Table 2 Auditable Events.

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

Table 2 Auditable Events

Application Note: The IDS_SDC and IDS_ANL requirements in this PP address the recording of results from IDS scanning, sensing, and analysing tasks (i.e., System data).

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

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

b) **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,** the additional information specified in the **Details** column of Table 2 Auditable Events.
FAU_GEN.1.2

Family Application Note: Available results from any component evaluation may be applicable to this requirement. All auditable events from each component evaluation will also be auditable events in the System context. Additional analysis is necessary to determine if any interactions among the components are required to be auditable as defined by this requirement.

5.2.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide ***[assignment: authorised users]*** with the capability to read ***[assignment: list of audit information]*** from the audit records. FAU_SAR.1.1

Application Note: This requirement applies to authorised users of the TOE. The requirement is left open for the writers of the ST to define which authorised users may access what audit data.

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

Family Application Note: Available results from any component evaluation may be applicable to this requirement. However, for the System PP, all System audit data needs to meet this requirement. Note that it is not required that any given component have access or provide an interface to all audit data. Rather, it would be adequate if each component provided access to only its own audit data. This should not be confused with the events that are the focus of the IDS, which are dealt with in subsequent requirements.

5.2.3 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. FAU_SAR.2.1

Family Application Note: Available results from any component evaluation may be applicable to this requirement. It would be acceptable to define the set of authorised users as the set of authorised users from all components. Unless the TOE introduces additional constraints, it is unlikely that the set could be reduced. However, additional authorised users could be added.

5.2.4 FAU_SAR.3 Selectable audit review

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

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Any additional audit events that may have been added in a System ST in refining the FAU_GEN.1 requirement are applicable.

5.2.5 FAU_SEL.1 Selective audit

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

a) event type;

b) ***[assignment: list of additional attributes that audit selectivity is based upon]***. FAU_SEL.1.1

Family Application Note: Available results from any component evaluation may be applicable to this requirement. The TOE must address selection for any events that may have been added in addition to the set of components.

5.2.6 FAU_STG.2 Guarantees of audit data availability

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

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

FAU_STG.2.3 The TSF shall ensure that ***[assignment: metric for saving audit records]*** audit records will be maintained when the following conditions occur: ***[selection: audit storage exhaustion, failure, attack]***. FAU_STG.2.3

Family Application Note: Available results from any component evaluation may be applicable to this requirement. The TOE must address availability for any events that may have been added in addition to the set of components.

5.2.7 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall ***[selection: 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records']*** and send an alarm if the audit trail is full. FAU_STG.4.1

Application Note: The ST must define what actions the TOE takes if the audit trail becomes full. Anything that causes the System to stop collecting or producing System data may not be the best solution, as this will only affect the System and not the IT System on which it is monitoring (e.g., shutting down).

Family Application Note: Available results from any component evaluation may be applicable to this requirement. The TOE must address audit data loss for any events that may have been added in addition to the set of components.

5.3 IDENTIFICATION AND AUTHENTICATION (FIA)

5.3.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow ***[assignment: list of TSF-mediated actions]*** on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.1

Application Note: The ST must define any mediated actions that are permitted before a user is authenticated. Actions must be limited to aiding a user in accessing the TOE. An acceptable action before authentication is using the help facility.

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. FIA_UAU.1.2

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Additional analysis may be required if any new interfaces or functions have been introduced to any component. Note that the concept of identification and authentication may be localised to individual IDS components. That is, it is not necessary to require a single TOE logon mechanism.

5.3.2 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **a settable, non-zero number** of unsuccessful authentication attempts occur related to **external IT products attempting to authenticate**. FIA_AFL.1.1

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

5.3.3 FIA_ATD.1 User attribute definition

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

a) User identity;

b) Authentication data;

c) Authorisations; and

d) ***[assignment: any other security attributes]***. FIA_ATD.1.1

Application Note: At a minimum, there must be sufficient user information for identification and authentication purposes. That information includes maintaining any authorisations a user may possess.

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Any additional user attributes added for the TOE must satisfy this requirement. Note that it is not necessary that the attributes be uniformly defined across all components.

5.3.4 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow ***[assignment: list of TSF-mediated actions]*** on behalf of the user to be performed before the user is identified. FIA_UID.1.1

Application Note: The ST must define any mediated actions that are permitted before a user is identified. Actions must be limited to aiding a user in accessing the System. An acceptable action before identification is using the help facility.

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. FIA_UID.1.2

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Additional analysis may be required if any new interfaces or functions have been introduced to any component. Note that the concept of identification and authentication may be localised to individual components. That is, it is not necessary to require a single TOE logon mechanism.

5.4 SECURITY MANAGEMENT (FMT)

5.4.1 FMT_MOF.1 Management of security functions behaviour

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

Application Note: The TOE may have administrative roles on the operating System that do not have permissions to change the configuration options of the System.

Family Application Note: Available results from any component evaluation may be applicable to this requirement. The TOE would need to address any administrative roles added beyond those defined in the components. However, the set of administrative roles need be no more than the set already defined in all of the components.

5.4.2 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 all other TOE data** to ***[assignment: the authorised identified roles]***. FMT_MTD.1.1

Application Note: The ST should define which roles are permitted to access the System data and all other TOE data. The ST may define any number of roles to meet this requirement.

Family Application Note: Available results from any component evaluation may be applicable to this requirement. The TOE would need to address any applicable roles added beyond those defined in the components. However, the set of roles need be no more than the set already defined in all of the components.

5.4.3 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the **following *roles:* authorised administrator**, **authorised System administrators, and *[assignment: other authorised identified roles]***. FMT_SMR.1.1

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

Family Application Note: Available results from any component evaluation may be applicable to this requirement. The System ST would need include all of the component-defined roles and add any roles added beyond those defined in the components. However, the set of roles need be no more than the set already defined in all of the components.

5.5 PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

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

FPT_ITA.1.1 The TSF shall ensure the availability of **audit and System data** provided to a remote trusted IT product within ***[assignment: a defined availability metric]***

given the following conditions ***[assignment: conditions to ensure availability]***. FPT_ITA.1.1

Application Note: The ST should state what the System does to promote availability to the audit and System data.

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Additional analysis and testing may be required to support this requirement since multiple components exist to support the transfer of System and audit data. The System ST should require consistent metrics for the entire TOE when refining this requirement. However, if that is not practical, it may be acceptable to adopt metrics that vary from component to component so long as they do conflict.

5.5.2 FPT_ITC.1 Inter-TSF confidentiality during transmission

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

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Additional analysis and testing may be required to support this requirement since multiple IDS components exist to support the transfer of System and audit data.

5.5.3 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: ***[assignment: a defined modification metric]***. FPT_ITI.1.1

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform ***[assignment: action to be taken]*** if modifications are detected. FPT_ITI.1.2

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Additional analysis and testing may be required to support this requirement since multiple components exist to support the transfer of System and audit data. Note that it is acceptable to require different actions for each of the IDS components and the System as a whole.

5.5.4 FPT_STM.1 Reliable time stamps

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

Family Application Note: Available results from any component evaluation may be applicable to this

requirement. The System should address time correlation among components. This could be accomplished either with a technical or procedural mechanism.

5.6 IDS COMPONENT REQUIREMENTS (IDS)

5.6.1 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) [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.1.1

Application Note: The ST will define the components of a System. This requirement indicates that the System must include at least one Sensor or Scanner by requiring a given TOE collect information pertaining to at least one of the selections in bullet **a** above. A Sensor would generally collect information pertaining to the following events in bullet **a**: start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, and data introduction. The Scanner would generally collect static configuration information which include the following events in bullet **a**: detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, and detected known vulnerabilities. Malicious code includes viruses, worms, simple Trojan horses, etc. Access control configuration includes access control lists, search for writeable files and directories, etc. Service configuration includes identification of network services and/or associated network ports, host services, versions of services, protocols acknowledged by services, etc. Authentication configuration includes cracking passwords, configuration settings (e.g., minimum password length, duration between allowed and required password changes), acceptable authentication means (e.g., NTLM, kerberos), defined guest accounts, account authorisations, etc. Accountability policy configuration includes size of audit trails, whether audit is enabled, what to do when the audit trail fills, etc. Known vulnerabilities is fairly open ended, but may include installed patches, checks for common or default configuration errors, etc.

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

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

b) The additional information specified in the *Details* column of Table 3 System Events. (EXT) IDS_SDC.1.2

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	Detected known vulnerabilities	**Identification of the known vulnerability**

Table 3 System Events

Application Note: In the case where a Sensor is collecting host-based events, for the identification and authentication event, the source address could be a subject IDS on a local machine and the destination is defined by default. For the data access and data introduction events, the source address could be filename and the destination address may be target location for the file.

Family Application Note: Available results from any component evaluation may be applicable to this requirement.

5.6.2 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) [selection: *statistical, signature, integrity*]; and

b) [assignment: *other analytical functions*]. (EXT) IDS_ANL.1.1

Application Note: Statistical analysis involves identifying deviations from normal patterns of behavior. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a System. For example, patterns of System settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing System settings or user activity at some point in time with those of another point in time to detect differences.

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) IDS_ANL.1.2

Application Note: The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.

Family Application Note: Available results from any component evaluation may be applicable to this requirement.

5.6.3 IDS_RCT.1 Analyser react (EXT)

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

Application Note: There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The Analyser may optionally perform other actions when intrusions are detected; these actions should be defined in the ST. An intrusion in this requirement applies to any conclusions reached by the analyser related to past, present, and future intrusions or intrusion potential.

Family Application Note: Available results from any component evaluation may be applicable to this requirement.

5.6.4 IDS_RDR.1 Restricted Data Review (EXT)

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.1.1

Application Note: This requirement applies to authorised users of the System. The requirement is left open for the writers of the ST to define which authorised users may access what System data.

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.1.2

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)** IDS_RDR.1.3

Application Note: The System needs to define the authorised users that may view the audit records. These authorised users may or may not be the same as those for a IDS component

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Note that the definition of authorised users and System data may vary from IDS component to IDS component.

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

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

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

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

IDS_ STG.1.3 **The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*]. (EXT)** IDS_STG.1.3

Application Note: The ST needs to define the amount of System data that could be lost under the identified scenarios.

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Each component must protect its data while it controls the data. Additional analysis would be required to address any new data, beyond that previously defined in individual components.

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

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

Application Note: The ST must define what actions the System takes if the storage capacity has been reached. Anything that causes the System to stop collecting static information may not be the best solution, as this will only affect the System and not the System on which it is collecting data (e.g., shutting down the System).

Family Application Note: Available results from any component evaluation may be applicable to this requirement. However, the System must take into account the relationships between components and address how the reaction of any given IDS component may affect any other in the System context.

5.7 ASSURANCE REQUIREMENTS

This chapter defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 4 summarizes the components.

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle 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**
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - conformance
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 4 Assurance Requirements

Class ADV: Development

5.7.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

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

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

5.7.2 ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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

ADV_FSP.2.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

5.7.3 ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

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

ADV_TDS.1.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

Class AGD: Guidance documents

5.7.4 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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

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

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

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

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

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

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

Evaluator action elements:

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

5.7.5 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

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

Class ALC: Life-cycle support

5.7.6 ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

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

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

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

5.7.7 ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

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

5.7.8 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

Evaluator action elements:

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

5.7.9 ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

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

Class ATE: Tests

5.7.10 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

5.7.11 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

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

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

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

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

Evaluator action elements:

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

5.7.12 ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.

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

Class AVA: Vulnerability assessment

5.7.13 AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

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

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

Application Note: The TOE version used as the basis for testing should include a reference to the specific signature set in place when this activity is conducted.

6 RATIONALE

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

6.1 RATIONALE FOR IT SECURITY OBJECTIVES

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Intrusion Detection System System Protection Profile. Table 5 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

	O.PROTCT	O.IDSCAN	O,IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION
A.ACCESS																	X			
A.DYNMIC																X	X			
A.ASCOPE																	X			
A.PROTCT														X						
A.LOCATE														X						
A.MANAGE																X				
A.NOEVIL													X	X	X					
A.NOTRUST														X	X					
T.COMINT	X						X	X			X									
T.COMDIS	X						X	X				X								
T.LOSSOF	X						X	X			X									
T.NOHALT		X	X	X			X	X												
T.PRIVIL	X						X	X												
T.IMPCON						X	X	X					X							
T.INFLUX									X											
T.FACCNT										X										
T.SCNCFG		X																		
T.SCNMLC		X																		
T.SCNVUL		X																		
T.FALACT					X															
T.FALREC				X																
T.FALASC				X																

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION
T.MISUSE			X																	
T.INADVE			X																	
T.MISACT			X																	
P.DETECT		X	X							X								X		
P.ANALYZ				X																
P.MANAGE	X					X	X	X					X		X	X				
P.ACCESS	X						X	X												X
P.ACCACT								X		X								X	X	
P.INTGTY											X									
P.PROTCT									X					X						

Table 5 Security Environment vs. Objectives

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The

O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

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

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

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

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

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

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

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

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

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

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

TOE monitors.

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

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

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

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

The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability. The ST will state whether this threat must be addressed by a Scanner.

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

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

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

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the

O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.

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

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

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

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

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

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

6.2 RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT

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

6.3 RATIONALE FOR SECURITY REQUIREMENTS

This section demonstrates that the functional components selected for the Intrusion Detection System System Protection Profile provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

	O.PROTCT	O.IDSCAN	O,IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION
FAU_GEN.1										X					
FAU_SAR 1						X									
FAU_SAR.2							X	X							
FAU_SAR.3						X								X	
FAU_SEL.1						X				X					
FAU_STG.2	X						X	X	X		X				X
FAU_STG.4									X	X					
FIA_UAU.1							X	X							
FIA_ATD.1								X							
FIA_UID.1							X	X							
FMT_MOF.1	X						X	X							
FMT_MTD.1	X						X	X			X				
FMT_SMR.1								X							
FPT_ITA.1												X			
FPT_ITC.1											X	X			
FPT_ITI.1											X	X			
ADV_ARC.1	X					X		X		X	X				
FPT_STM.1										X			X		
IDS_SDC.1		X	X												
IDS_ANL.1				X											
IDS_RCT.1					X										
IDS_RDR.1						X	X	X							
IDS_STG.1	X						X	X	X		X				
IDS_STG.2									X						

Table 6 Requirements vs. Objectives Mapping

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

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

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. 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]. 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 ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

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

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

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

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

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

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

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

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

The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and

produced [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

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

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

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

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [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]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event the its audit trail is full [FAU_STG.4]. 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 System must prevent the loss of audit data in the event the its audit trail is full [IDS_STG.2].

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

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

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

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The 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]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1].

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

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

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2].

OE.AUDIT_SORT The IT Environment will provide the capability to sort audit information.

The IT environment must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3,].

OE.TIME The IT Environment will provide reliable time stamp to the TOE. Time stamps associated with an audit record must be reliable [FPT_STM.1].

6.4 RATIONALE FOR ASSURANCE REQUIREMENTS

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

6.5 RATIONALE FOR EXTENDED REQUIREMENTS

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

6.6 RATIONALE FOR STRENGTH OF FUNCTION

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

6.7 RATIONALE FOR SATISFYING ALL DEPENDENCIES

The Intrusion Detection System System Protection Profile does satisfy all the requirement dependencies of the Common Criteria. Table 7 Requirement Dependencies lists each requirement from the Intrusion Detection System System Protection Profile with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_SAR.2	FAU_SAR.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	YES
FAU_STG.2	FAU_GEN.1	YES
FAU_STG.4	FAU_STG.2	YES
FIA_UAU.1	FIA_UID.1	YES
FMT_MOF.1	FMT_SMR.1	YES
FMT_MTD.1	FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.1	YES

Table 7 Requirement Dependencies

7 APPENDICES

A: References

[1] *Common Criteria for Information Technology Security Evaluation*, CCIMB-99-031, Version 2.1, August 1999.

[1a] Common Criteria for Information Technology Security Evaluation, CCMB-206-09-001 thru 003, Version 3.1, September 2006

[2] *NSA Glossary of Terms Used in Security and Intrusion Detection*, Greg Stocksdale, NSA Information Systems Security Organization, April 1998.

B: Glossary

This section describes terms that are used throughout the IDSSPP and other Protection Profiles in the Intrusion Detection System family. The same terms section is used among all Protection Profiles to maintain consistency. When possible, terms are defined as they exist in the *Common Criteria for Information Technology Security Evaluation* or the *NSA Glossary of Terms Used in Security and Intrusion Detection*[2] provided by the NSA Information Systems Security Organization. The definitions were modified only to provide consistency with the IDSSPP. For example, occurrences of *computer system* or *network* were replaced with IT System. The authors of the IDSSPP defined all other terms as necessary.

Analyzer data – Data collected by the Analyzer functions
Analyzer functions – The active part of the Analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.
Assets - Information or resources to be protected by the countermeasures of a TOE.
Attack - An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit - The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Audit Trail - In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication - To establish the validity of a claimed user or object.
Authorized Administrator – A subset of authorized users that manage an IDS component
Authorized User - A user that is allowed to perform IDS functions and access data
Availability - Assuring information and communications services will be ready for use when expected.
Compromise - An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
Confidentiality - Assuring information will be kept secret, with access limited to appropriate persons.
Evaluation - Assessment of a PP, a ST or a TOE, against defined criteria.
IDS component - a Sensor, Scanner, or Analyzer.
Information Technology (IT) System - May range from a computer system to a computer network
Integrity - Assuring information will not be accidentally or maliciously altered or destroyed.
Intrusion - Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection - Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins

or attempts either manually or via software expert systems that operate on logs or other information available on the network.
Intrusion Detection System (IDS) - A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
Intrusion Detection System Analyzer (Analyzer) – The component of an IDS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).
Intrusion Detection System Scanner (Scanner) – The component of an IDS that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
Intrusion Detection System Sensor (Sensor) - The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.
IT Product - A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Network - Two or more machines interconnected for communications.
Packet - A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packet Sniffer - A device or program that monitors the data traveling between computers on a network
Protection Profile (PP) - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Scanner data – Data collected by the Scanner functions
Scanner functions – The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data)
Security - A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
Sensor data – Data collected by the Sensor functions
Sensor functions – The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data)
Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security Target (ST) - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Target of Evaluation (TOE) - An IT product of system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Threat - The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security
TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

Trojan Horse - An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.
TSF data - Data created by and for the TOE, that might affect the operation of the TOE.
TSF Scope of Control (TSC) - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Virus - A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.
Vulnerability - Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

C: Acronyms

CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
IT	Information Technology
NIAP	National Information Assurance Partnership
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions

D: Robustness Environment Characterization

General Environmental Characterization

In trying to specify the environments in which TOEs with various levels of robustness are appropriate, it is useful to first discuss the two defining factors that characterize that environment: value of the resources and authorization of the entities to those resources.

In general terms, the environment for a TOE can be characterized by the authorization (or lack of authorization) the least trustworthy entity has with respect to the highest value of TOE resources (i.e. the TOE itself and all of the data processed by the TOE).

Note that there are an infinite number of combinations of entity authorization and value of resources; this conceptually "makes sense" because there are an infinite number of potential environments, depending on how the resources are valued by the organization, and the variety of authorizations the organization defines for the associated entities. In the next section, these two environmental factors will be related to the robustness required for selection of an appropriate TOE.

Value of Resources

Value of the resources associated with the TOE includes the data being processed or used by the TOE, as well as the TOE itself (for example, a real-time control processor). "Value" is assigned by the using organization. For example, in the DoD low-value data might be equivalent to data marked "For Official Use Only", while high-value data may be those classified Top Secret. In a commercial enterprise, low-value data might be the internal organizational structure as captured in the corporate on-line phone book, while high-value data might be corporate research results for the next generation product. Note that when considering the value of the data one must also consider the value of data or resources that are accessible through exploitation of the TOE. For example, a firewall may have "low value" data itself, but it might protect an enclave with high value data. If the firewall was being depended upon to protect the high value data, then it must be treated as a high-value-data TOE.

Authorization of Entities

Authorization that entities (users, administrators, other IT systems) have with respect to the TOE (and thus the resources of that TOE, including the TOE itself) is an abstract concept reflecting a combination of the trustworthiness of an entity and the access and privileges granted to that entity with respect to the resources of the TOE. For instance, entities that have total authorization to all data on the TOE are at one end of this spectrum; these entities may have privileges that allow them to read, write, and modify anything on the TOE, including all TSF data. Entities at the other end of the spectrum are those that are authorized to few or no TOE resources. For example, in the case of a router, non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources. In

the case of an OS, an entity may not be allowed to log on to the TOE at all (that is, they are not valid users listed in the OS's user database).

It is important to note that authorization **does not** refer to the **access** that the entities actually have to the TOE or its data. For example, suppose the owner of the system determines that no one other than employees was authorized to certain data on a TOE, yet they connect the TOE to the Internet. There are millions of entities that are not **authorized** to the data (because they are not employees), but they actually have connectivity to the TOE through the Internet and thus can attempt to access the TOE and its associated resources.

Entities are characterized according to the value of resources to which they are authorized; the extent of their authorization is implicitly a measure of how trustworthy the entity is with respect to compromise of the data (that is, compromise of any of the applicable security policies; e.g., confidentiality, integrity, availability). In other words, in this model the greater the extent of an entity's authorization, the more trustworthy (with respect to applicable policies) that entity is.

Selection of Appropriate Robustness Levels

Robustness is a characteristic of a TOE defining how well it can protect itself and its resources; a more robust TOE is better able to protect itself. This section relates the defining factors of IT environments, authorization, and value of resources to the selection of appropriate robustness levels.

When assessing any environment with respect to Information Assurance the critical point to consider is the likelihood of an attempted security policy compromise, which was characterized in the previous section in terms of entity authorization and resource value. As previously mentioned, robustness is a characteristic of a TOE that reflects the extent to which a TOE can protect itself and its resources. It follows that as the likelihood of an attempted resource compromise increases, the robustness of an appropriate TOE should also increase.

It is critical to note that several combinations of the environmental factors will result in environments in which the likelihood of an attempted security policy compromise is similar. Consider the following two cases:

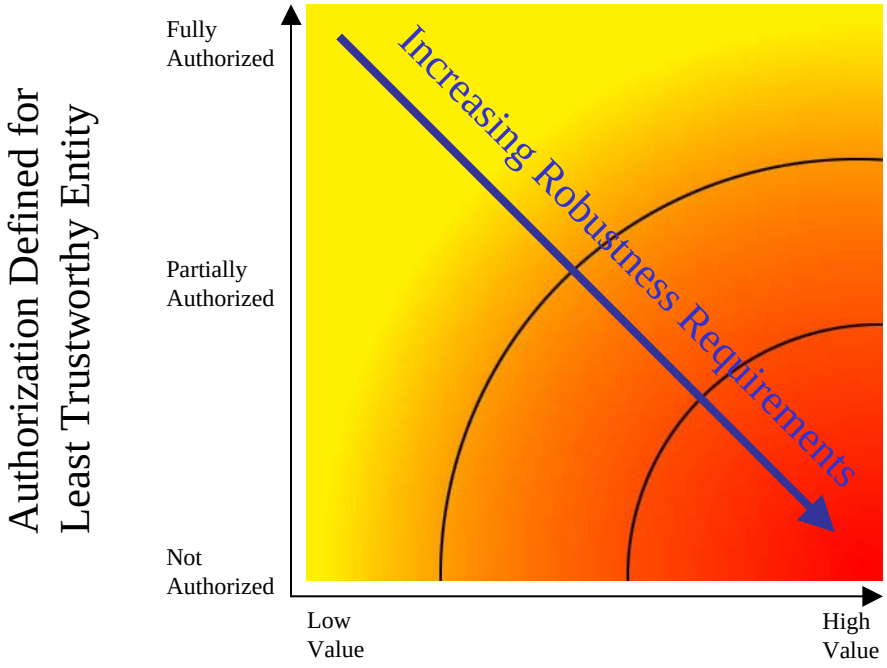
The first case is a TOE that processes only low-value data. Although the organization has stated that only its employees are authorized to log on to the system and access the data, the system is connected to the Internet to allow authorized employees to access the system from home. In this case, the least trusted entities would be unauthorized entities (e.g. non-employees) exposed to the TOE because of the Internet connectivity. However, since only low-value data are being processed, the likelihood that unauthorized entities would find it worth their while to attempt to compromise the data on the system is low and selection of a basic robustness TOE would be appropriate.

The second case is a TOE that processes high-value (e.g., classified) information. The organization requires that the TOE be stand-alone, and that every user with physical and logical access to the TOE undergo an investigation so that they are authorized to the highest value data on the TOE. Because of the extensive checks done during this investigation, the organization is assured that only highly trusted users are authorized to use the TOE. In this case, even though high value information is being processed, it is unlikely that a compromise of that data will be attempted because of the authorization and trustworthiness of the users and once again, selection of a basic robustness TOE would be appropriate.

The preceding examples demonstrated that it is possible for radically different combinations of entity authorization/resource values to result in a similar likelihood of an attempted compromise. As mentioned earlier, the robustness of a system is an indication of the protection being provided to counter compromise attempts. Therefore, a basic robustness system should be sufficient to counter compromise attempts where the likelihood of an attempted compromise is low. The following chart depicts the “universe” of environments characterized by the two factors discussed in the previous section: on one axis is the authorization defined for the least trustworthy entity, and on the other axis is the highest value of resources associated with the TOE.

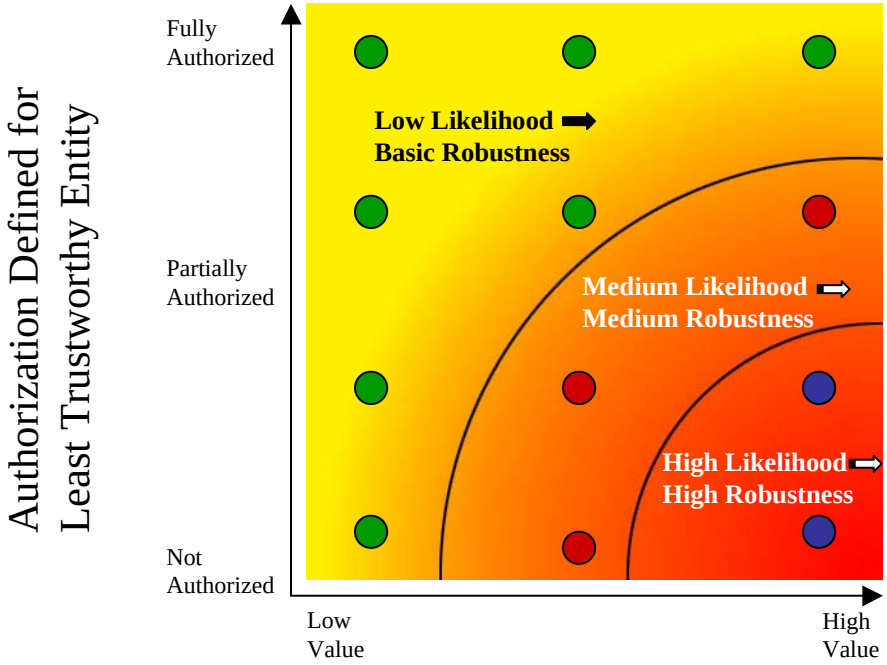
As depicted in the following figure, the robustness of the TOEs required in each environment steadily increases as one goes from the upper left of the chart to the lower right; this corresponds to the need to counter increasingly likely attack attempts by the least trustworthy entities in the environment. Note that the shading of the chart is intended to reflect- the notion that different environments engender similar levels of “likelihood of attempted compromise”, signified by a similar color. Further, the delineations between such environments are not stark, but rather are finely grained and gradual.

While it would be possible to create many different "levels of robustness" at small intervals along the “Increasing Robustness Requirements” line to counter the increasing likelihood of attempted compromise due to those attacks, it would not be practical nor particularly useful. Instead, in order to implement the robustness strategy where there are only three robustness levels: Basic, Medium, and High, the graph is divided into three sections, with each section corresponding to a set of environments where the likelihood of attempted compromise is roughly similar. This is graphically depicted in the following chart.



In this second representation of environments and the robustness plane below, the "dots" represent given instantiations of environments; like-colored dots define environments with a similar likelihood of attempted compromise. Correspondingly, a TOE with a given robustness should provide sufficient protection for environments characterized by like-colored dots. In choosing the appropriateness of a given robustness level TOE PP for an environment, then, the user must first consider the lowest authorization for an entity as well as the highest value of the resources in that environment. This should result in a "point" in the chart above, corresponding to the likelihood that that entity will attempt to compromise the most valuable resource in the environment. The appropriate robustness level for the specified TOE to counter this likelihood can then be chosen.

The difficult part of this activity is differentiating the authorization of various entities, as well as determining the relative values of resources; (e.g., what constitutes "low value" data vs. "medium value" data). Because every organization will be different, a rigorous definition is not possible. In Section 3 of this PP, the targeted threat level for a Basic robustness TOE is characterized. This information is provided to help organizations using this PP -ensure that the functional requirements specified by this Basic robustness PP are appropriate for their intended application of a compliant TOE.


Authorization Defined for Least Trustworthy Entity
Fully Authorized
Partially Authorized
Not Authorized
Low Likelihood
Basic Robustness
Medium Likelihood
Medium Robustness
High Likelihood
High Robustness
Low Value
High Value
Highest Value of Resources Associated with the TOE