IntruShield Product Family
Intrusion Detection System
Security Target

Version 0.97

August 25, 2004

Prepared for:
McAfee, Incorporated
3965 Freedom Circle
Santa Clara, CA 95054

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

The IntruShield Product Family, Intrusion Detection System, meets the applicable security functional requirements, assumptions, objectives, and threats of the US Government Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002 (IDSSPP) with the exception of FPT_STM.1 time stamp.

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. McAfee Incorporated provides the TOE, which includes the IntruShield 1200, 2600, and the IntruShield 4000 Sensors, an IntruShield Security Management System (ISM), and an Update Server.

- The Security Target contains the following additional sections:
- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

1.1 Security Target, TOE and CC Identification

ST Title – IntruShield Product Family, Intrusion Detection System, Security Target

ST Version –Version 0.97

ST Date – August 25, 2004

TOE Identification – The TOE is composed of the following three components:

The TOE is identified as one or more of these sensors:

1. McAfee Incorporated IntruShield Sensors,
    a. IntruShield 1200 appliance, Rev. 2 or earlier
    b. IntruShield 2600 appliance, Rev. 2 or earlier
    c. IntruShield 4000 appliance, Rev. 2 or earlier
2. IntruShield Security Management System (ISM) Version 1.8.3.5
3. Update Server Version 04.06.07.01– hosts The Sensor Builds Version 1.8.3.10, The Signature Set 1.8.29.2, and The ISM Updates 1.8.3.5

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
    - Part 2 Extended (with IDS_SDC.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, and IDS_STG.2)

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
    - Part 3 Conformant
    - Evaluation Assurance Level 3 (EAL3)

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
    - Note that operations already performed in the corresponding Protection Profile are not identified in this Security Target.
- Explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified with "**(EXP)**".
- Requirements that have been modified from the original text in the Common Criteria to be compliant with an International Interpretation are identified with **(RI #n).**
- Requirements that have been modified from the original text in the Common Criteria to be compliant with an Interpretation recommended by the U.S. Common Criteria Evaluation and Validation Scheme are identified with **(NIAP ..).**
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Acronyms

The acronyms used within this Security Target:

ACM	Access Control Management
AGD	Administrator Guidance Document
CC	Common Criteria
CM	Control Management
DAC	Discretionary Access Control
DO	Delivery Operation

EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
IDS	Intrusion Detection System
I/O	Input/Output
NIST	National Institute of Standards and Technology
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control
VLAN	Virtual Local Area Network

1.3.3 Terminology

The following terminology is used in this document:

Alert	An alert is a notification of a system event, attack, or other incident that triggers the intrusion Detection System.
Alert Viewer	A graphical user interface for viewing specific attack information in the IntruShield System. The Alert Viewer interface is part of the ISM, and focuses on alert forensic analysis.
Appropriate Administrator	Any administrator with the authorization to perform the administrator action for discussion
Attack	A set of actions performed by an attacker that poses a threat to the security state of a protected entity in terms of confidentiality, integrity, authenticity, availability, authorization, and access policies.
CIDR	**Classless Inter-Domain Routing**. A scheme which allocates blocks of Internet addresses in a way that allows summarization into a smaller number of routing table entries. A CIDR address contains the standard 32-bit IP address but includes information on how many bits are used for the network prefix. For example, in the CIDR address 123.231.121.04/22, the "/22" indicates the first 25 bits are used to identify the unique network leaving the remaining bits to identify the specific host
Denial of Service	In a Denial of Service (DoS) attack, the attacker attempts to crash a service (or the machine), overload network links, overload the CPU, or fill up the disk. The attacker does not always try to gain information, but to simply act as a vandal to prevent you from making use of your machine. Ping floods and Smurf attacks are examples of DoS attacks.
Distributed Denial Of Service	Distributed Denial of Service (DDoS) attacks usually consist of standard DoS attacks orchestrated by attackers covertly controlling many, sometimes hundreds, of different machines.

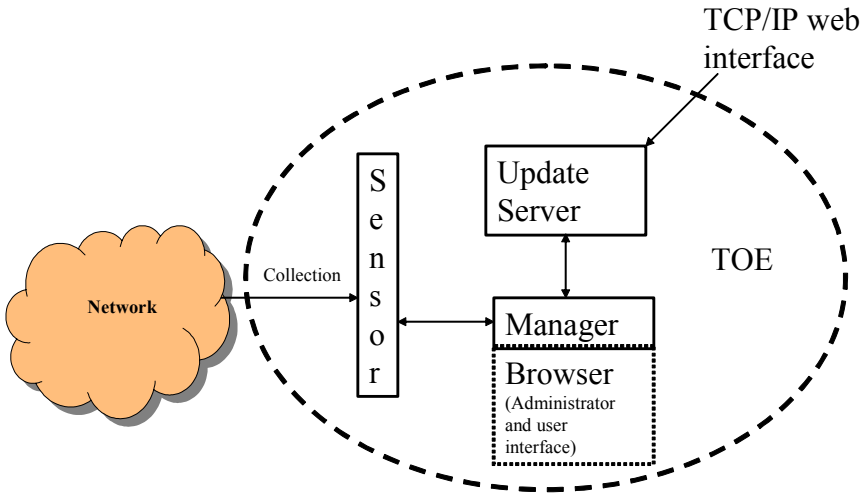
HTTPS	The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is http using a Secure Socket Layer (SSL).
Intrusion	Unauthorized access to, and/or activity in, an information system. Usually for the purpose of tampering with or disrupting normal services. See also **Attack**.
Intrusion Detection	The process of identifying that an intrusion has been attempted, is occurring, or has occurred.
NTP	Network Time Protocol provides a mechanism to synchronize time on computers across an internet. The specification for NTP version 3 is defined in RFC 1305. Such synchronization can be very useful for multi-machine activities that depend upon accurate time stamps.
Policy	A user-configured security rule that determines the permission of traffic across a network. Policies can set rules for protocols (HTTP, UDP), machines (NT, Solaris), operating systems (Unix), and other types of network information. A policy also defines what actions should be taken in the event of non-permissible activity.
Policy Violations	All activities for which the underlying traffic content may not be malicious by itself, but are explicitly forbidden by the usage policies of the network as defined by a security policy. These can include "protocol violations" wherein packets do not conform to network protocol standards. (For example, they are incorrectly structured, have an invalid combination of flags set, or contain incorrect values.) Examples might include TCP packets with their SYN and RST flags enabled, or an IP packet whose specified length doesn't match its actual length. A protocol violation can be an indication of a possible attack, but can also be triggered by malfunctioning software or hardware.
Port Cluster	Port Cluster is a more intuitive term for an Interface Group. **Interface Group** An interface group enables multiple sensor ports to be grouped together for the effective monitoring of asymmetric environments. Interface groups normalize the impact of traffic flows split across multiple interfaces, thus maintaining state to avoid information loss. Once configured, an interface group appears in the Resource Tree as a single interface node (icon) under the sensor where it is located. All of the ports that make up the interface are configured as one logical entity, keeping the configuration consistent.
MySQL DATABASE	A Relational database. Allows the definition of data structures, storage and retrieval operations, and integrity constraints. The data and relations between them are kept in organized tables, which are collections of records and each record in a table contains the same fields.
Roles	A class of user privileges that determines the authorized activities of the various users in the system.
Sensor	The sensor is a network device containing the intrusion detection engine. It analyzes network traffic, searching for signs of unauthorized activity.
Signature	Activities or alterations to an information system indicating an attack or attempted attack, detectable by examination of audit trail logs.
Span Mode	One of the monitoring modes available for an IntruShield sensor. Functions by mirroring the packet information on a switch or hub and sending the information to a sensor for inspection, while continuing the transmission of traffic with negligible latency. SPAN mode is typically half-duplex, and works through a connection of a sensor to a port on a hub or the SPAN port of a switch.

SPAN Port	On a switch, SPAN mirrors the traffic at one switched segment onto a predefined port, known as a SPAN port.
SSL	A secure socket layer (SSL) is an encryption protocol invoked on a Web server that uses HTTPS.
Tap	A tap is hardware device that passes traffic unidirectionally from a network segment to the IDS. Traffic is mirrored as it passes through the tap. This mirror image is sent to the IDS for inspection. This prevents traffic passing from being directed at the IDS.
Tap Mode	One of the monitoring modes available for an IntruShield sensor. Functions by mirroring the packet information and sending the information to a sensor for inspection, while continuing the transmission of traffic with negligible latency. Tap mode works through installation of an external wire tap, a port on a hub, the SPAN port of a switch, or through an internal tap when deploying the I-2600. Also known as passive monitoring mode.
Trojan Horse	A computer program that has a useful function, but which also contains additional hidden, typically malicious functions.
Virtual IDS	An IntruShield feature that enables you to logically segment a sensor into a large number of virtual sensors, each of which can be customized with its own security policy. Virtual IDS (VIDS) are represented in the ISM as *interfaces* and *sub-interfaces*.
VLAN	Virtual Local Area Network. A logical grouping of two or more nodes which are not necessarily on the same physical network segment, but which share the same network number. This is often associated with switched Ethernet networks. In McAfee Incorporated, also an administrative interface that allows an administrator to change the type of monitored traffic to a VLAN.
Vulnerability	Any characteristic of a computer system that will allow someone to keep it from operating correctly, or that will let unauthorized users take control of the system.

2 TOE Description

The TOE is the McAfee, Inc., IntruShield Intrusion Detection System product. The TOE consists of three main components that are: the IntruShield sensor(s), the IntruShield Security Management system, and the Update server.

The following figure provides a high-level visual representation of the TOE.



IntruShield sensors are high-performance, scalable, and flexible content processing appliances. The IntruShield sensor performs stateful inspection for each packet to discover and prevent intrusions, misuse, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks. McAfee Incorporated offers three types of sensor appliances providing different bandwidth and deployment strategies. These are the *IntruShield 1200,* the *IntruShield 2600,* and the *IntruShield 4000 sensors*. All three sensor types provide the same security functions.

The IntruShield Security Management (ISM) consists of software that is used to configure and manage an IntruShield deployment. The ISM is a set of applications, MySQL DATABASE is embedded. MySQL database is installed during ISM installation. The MySQL database must reside on the same platform as does the ISM. ISM is available in two versions: IntruShield Global Manager and IntruShield Manager. Both versions of the ISM are part of the TOE. The IntruShield Global Manager and IntruShield Manager are the same software. The difference between the two versions is one of scalability. Both versions of the ISM operate within an IT environment composed of an Intel-based hardware platform with a Windows 2000 operating system (OS). The IntruShield Manager supports up to 6 IntruShield sensors of any kind while the ISM Global Manager supports unlimited number of IntruShield sensors of any kind.

The McAfee Incorporated Update Server is a McAfee-owned and operated file server that provides updates to the signature files and software of IntruShield sensors in customer installations. The Update Server always resides at McAfee Incorporated.

2.1 Product Type

The IntruShield system from McAfee Incorporated Corporation is a network Intrusion Detection system (IDS) that offers real-time network intrusion detection and prevention against the following types of attacks for enterprise networks:

- network traffic
- detected known vulnerabilities,

2.2 Product Description

The IntruShield IDS product is a combination of network appliances and software built for the detection and prevention of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, and network misuse. The IntruShield IDS combines real-time detection and prevention for the most comprehensive and effective network security system. The IntruShield system enables highly accurate network attack detection and prevention at up to 2 Gbps. The product line includes the IntruShield 4000 sensor appliance, the IntruShield 2600 sensor appliance, the IntruShield 1200 sensor appliance, and the IntruShield Security Management (ISM) system.

The IntruShield IDS system is composed of a family of sensor appliances, an IntruShield ISM system, and an Update Server. The sensor appliances are stand-alone appliances from McAfee Incorporated. The three sensor appliances are the IntruShield 1200, IntruShield 2600, and the IntruShield 4000. All other components of the product are software only components that run on a Windows workstation. The ISM system is an IDS management solution for managing IntruShield sensor appliance deployments for large and distributed enterprise networks. The ISM operates with an MYSQL DATABASE to persist configuration information and alert data. ISM for Windows 2000 includes the MySQL database.

2.3 Product Features

The TOE implements the following features:

The Sensor Subsystem performs the following components:

- *Traffic Capture* is non–intrusive and captures packets into a data store for review.
- *Load balancing and protocol verification* makes security decisions such that it can filter packets of no interest.
- *Denial of Service detection and response* detects DoS attacks and provides an alert capability and the capability to drop packets identified that are part of the DoS attack.
- *Signature detection and anomaly detection* performs anomaly detection, logs attack information, and performs response functions. The response functions include the following: alert, packet log, TCP reset, ICMP host unreachable, forward blocking, and drop packets.
- *Sensor management* is the interface between the sensor and the ISM. It has the responsibilities to push policies that have been defined in the Management Subsystem to the appropriate sensor module.

The IntruShield ISM provides management functions to manage IntruShield sensor appliance deployments for large and distributed enterprise networks. The ISM system is an intuitive, scalable, powerful web-based security management system that provides network intrusion prevention. It offers features to define, distribute, enforce, and audit security policies to protect critical servers, data centers, individual departments, and distributed branch and remote offices of a global business. The ISM provides a Web-based Management interface to the sensor. The ISM is a centralized web-based application that runs on a client platform. The ISM performs Real-time Alert Analysis. This analysis provides intelligent management and analysis of alerts in real time with granular drill-down capabilities and color-coding quickly pinpoints the target, source, and severity of network attacks.

The management features provided by the ISM include the following:

- Automated Real-time Threat Updates: Automated process delivers real-time, enterprise-wide signature updates without requiring sensor reboots, providing protection against newly-discovered attacks while eliminating manual updates and sensor downtime.
- Granular Security Policy Management: Flexible and custom policy management per sensor — from multiple network segments to individual hosts — delivers improved attack detection and prevention.
- Administrative Domains: Scalable security policy administration with role-based access control allows delegation of administrative responsibilities.
- Forensic Analysis: Analysis tools, including report generation, enable detailed historical and real-time forensic analysis to determine network attack patterns.
- Comprehensive Response Management: A set of response actions — including user-defined responses and notification capabilities — provide proactive attack notification and prevention.
- Interoperability with Enterprise Managers: Interoperability with enterprise and security management applications.

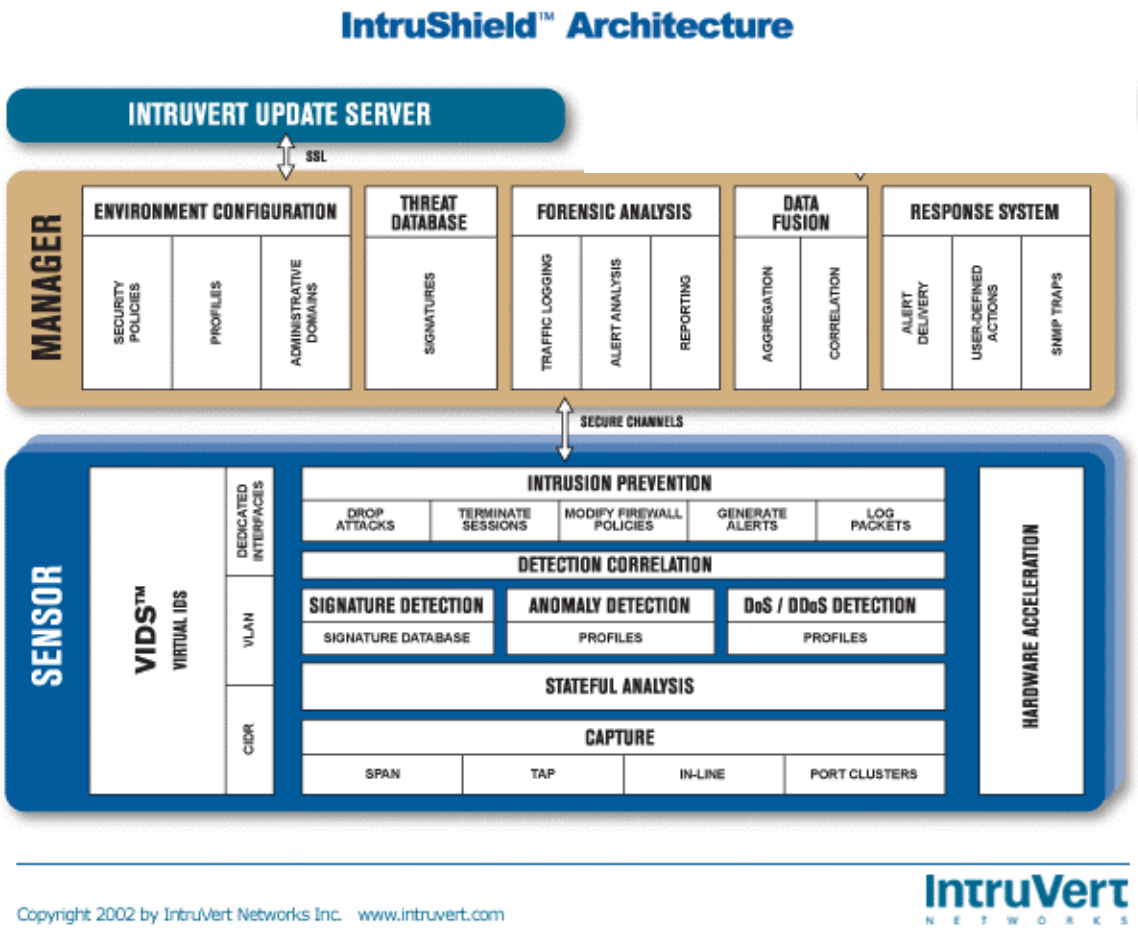
The McAfee Incorporated Update Server is a McAfee Incorporated-owned and -operated file server that updates the signature files of IntruShield sensors in McAfee Incorporated customer installations. McAfee Incorporated uses the Update Server to securely provide fully automated, real-time signature updates without requiring any manual intervention. McAfee Incorporated develops and releases signature updates. Since new vulnerabilities are discovered almost daily, signature updates are released on a regular basis. These new signatures and patches are made available to customers through the Internet via the McAfee Incorporated Update Server.

2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.4.1 Physical Boundaries

The components of the IntruShield IDS TOE are the Collection Subsystem, the ISM Subsystem, and the Update Server subsystem. Each subsystem performs dedicated functions. The following figure provides a high-level depiction of the IntruShield subsystem architecture.



2.4.1.1 Collection Subsystem

The Collection Subsystem is provided by the IntruShield Sensor appliance. The primary function of an IntruShield sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The sensor examines packets according to user-configured *policies*, or rule sets, which determine what attacks to watch for, and how to react with countermeasures if an attack is detected. If an

attack is detected, the sensor raises an *alert* to describe the event, and responds according to its configured policy. Sensors can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even dropping packets entirely before they reach their target.

Unlike single-port sensors, a single multi-port IntruShield sensor can monitor many network segments in any combination of *operating modes*—that is, the *monitoring* or *deployment* mode for the sensor —SPAN mode, tap mode, or in-line mode.[1] Additionally, IntruShield's Virtual IDS (VIDS) feature enables you to further segment a port on a sensor into many "virtual sensors."

2.4.1.2 Manager Subsystem

The ISM is the Manager Subsystem. The ISM server is a dedicated Windows 2000 platform running the ISM software. The ISM is also referred to as The Manager. There are two versions of the ISM system:

1. *IntruShield Global Manager* that is best suited for global IDS deployments of up to many sensors, and the Global Manager that operates running Windows with an embedded MySQL database.
2. *IntruShield Manager* that supports large or distributed deployments of up to three sensors. IntruShield Manager is supported only on Windows 2000 with an embedded MySQL database. Functionally, the products are otherwise identical. The Security Target uses the term "ISM" to describe either version.

The ISM software is a Web-based user interface for configuring and managing the IntruShield Sensors.
The ISM has the following components:

- *Network Console* is the first screen displayed after the user logs on to the system. The Network Console displays system health—i.e., whether all components of the system are functioning properly, the number of unacknowledged alerts in the system and the configuration options available to the current user. Options available within the Network Console are determined by the current user's assigned role(s).
- *System Health Viewer* displays the status of the ISM, database, and any deployed sensors; including all system faults.
- *System Configuration Tool* provides all system configuration options, and facilitates the configuration of sensors, administrative domains, users, roles, attack policies and responses, user-created signatures, and system reports. Access to various activities, such as user management, system configuration, or policy management is based on the current user's role(s) and privileges.
- *Alert Viewer* displays detected security events that violate your configured security policies. The Alert Viewer provides powerful drill-down capabilities to enable you to see all the details on a particular alert, including its type, source and destination addresses,

An administrator or user can directly use the ISM interface from the server itself as it is a Windows ISM server.

The keyboard, mouse and screen interfaces into the ISM interface are customer provided.

The IntruShield ISM server operates with a MYSQL DATABASE (relational database management system) for storing persistent configuration information and event data. The ISM for Windows 2000 includes a MySQL database that is installed during ISM software installation.

2.4.1.3 Update Server

As stated in Section 2.3, the Update Server is a McAfee Incorporated -owned and -operated file server that updates the signature files of IntruShield sensors in customer installations. McAfee Incorporated uses the Update Server to securely provide fully automated, real-time signature updates without requiring any manual intervention. According to a user-configured schedule or via a manual process, the ISM polls the McAfee Incorporated Update Server, and compares the file on the Update Server with what is already available in the ISM server to determine what it needs

[1] SPAN, and Tap Modes, also know as passive monitoring, mirror the packer under investigation and allow the original packet to continue with negligible latency.

to download. Once it has received the update, the ISM then determines what signatures need to be pushed out to sensors based on the policy applied to the sensor.

The TOE uses the Update Server to securely provide fully automated, real-time signature updates without requiring any manual intervention according to a user-configured schedule or via a manual process. The ISM polls the Update Server, and compares the file on the Update Server with what is already available in the ISM server to determine what it needs to download. Once it has received the update, the ISM then determines what signatures need to be pushed out to sensors based on the policy applied to the sensor. For example, a policy defined for a Windows environment will receive only updated signatures that apply to that environment.

2.4.2 Logical Boundaries

The logical boundaries of the TOE are divided into two groups, one related to the administration and security attributes associated with the TOE (Security Audit, Identification and Authentication, Security Management, and Protection of Security Functions), and the other related to the collection and analysis of the network traffic (System Data Collection, Data Analysis and Data Review, Availability and Loss).

2.4.2.1 Security Audit

The ISM generates audit records related to the administration/management of the TOE and traffic logs for IDS information. The ISM records both the audit and traffic log information into a data store, which is part of the TOE. The data store employed is MySQL. The MYSQL DATABASE provides storage and retrieval for audit and traffic log information. This function records attempts to access the system itself, such as successful and failed authentication, as well as the actions taken by the user once authenticated. Auditable actions include changes to the IDS rules and viewing the audit records of both the system access and the IDS traffic log.

2.4.2.2 Identification and Authentication

The ISM is the only TOE subsystem that provides an external user interface protected by identification and authentication mechanism. The sensor provides and external administrative interface protected by identification and authentication mechanism. The ISM of the TOE requires users to provide unique identification (user IDs) and authentication data (passwords) before any access to the TOE is granted

2.4.2.3 Security Management

The ISM provides a web-based (using https) management interface for all administration, including the IDS rule set, user accounts and roles, and audit functions.

2.4.2.4 Protection of Security Functions

The TOE protects the security functions it provides through a variety of mechanisms. One of the primary protections is that users must authenticate before any administrative operations can be performed on the system. The signature files are protected on the Update Server by the fact that it is physically isolated within a physically protected area within McAfee Incorporated and under McAfee Incorporated control. The data that is transferred between the ISM and the sensor is encrypted using a SSL/SNMP proprietary protocol, and the signature information communicated from the Update Server to the ISM is encrypted using SSL version 3.0.

The McAfee Incorporated sensors are protected on the monitored network by “hiding” the fact it is there. This is done primarily by using a non-TCP/IP network stack on the sensors, which prevents it from being accessed as a network device on the network. Also, the signature files are protected doubly as the system is configured to not accept any management requests or input from the monitored network.

The ISM server is a dedicated Windows 2000 server running the ISM software. The TOE contains MySQL database in which ISM stores the traffic logs as well as the audit of human interaction with the User/Admin interface. The MySQL DATABASE resides on the same platform as does the ISM. All MYSQL DATABASE tables used for TSF data are dynamically allocated so that the limit on the recording capacity of the audited information is the limit of the physical disk partition on the platform that is not dedicated to the operating system, the MYSQL DATABASE, and the ISM. This assures there is always adequate disk space to record current and new data that has been found to

match the current rule set. However, as a safety feature, if the audit and/or log data could not be written to a MYSQL DATABASE table, an alarm is presented at the Management Console.

2.4.2.5 System Data Collection

The TOE has the ability to set rules to govern the collection of data regarding potential intrusions. While the Update Server contains default rules to detect currently known vulnerabilities and exploits, new rules can be created to detect new vulnerabilities as well as specific network traffic, allowing the administrator complete control over the types of traffic that will be monitored.

2.4.2.6 System Data Analysis

The TOE provides tools at the ISM console for menu selection to analyze both IDS traffic log data as well as audit information. The TOE provides two methods of reviewing traffic log information, one is a real-time viewer. The real-time viewer is a "tab" selection at the ISM console. Also available at the console to review traffic log data is the ISM Activity Log that enables the user generate reports. Audit information is reviewed from the console through the user Activities Audit Report.

2.4.2.7 System Data Review, Availability and Loss

IDS Audit data can only be viewed by authorized users (specific roles). The ISM console provides a user interface for menu selectable data review. The data stores of the raw collection data are limited only by the storage capacity of the platform and table management of the MYSQL DATABASE. The TOE monitors the data store to determine when storage is exhausted and then the TOE takes appropriate action.

3 Security Environment

This Security Target provides the following policies, threats and assumptions about the TOE.

3.1 Threats to Security

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.

3.1.1 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.

3.1.2 IT System Threats

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

T.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.

3.2 Organization Security Policies

The following policies apply to the TOE and the intended environment of the TOE.

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

3.3 Secure Usage Assumptions

The following usage assumptions are made about the intended environment of the TOE.

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 Operating System Assumption

A.TIME The Windows 2000 operating system, which is a part of the environment, shall provide reliable time stamps for the TOE.

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment. All of the identified organizational policies, objectives, threats, and assumptions are addressed by the security objectives described below.

4.1 IT Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

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

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 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 other IDS components, the TOE will ensure the confidentiality of the System data.

4.2 IT Security Objectives for the Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

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

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

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

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

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

O.TIME The TOE operating environment shall provide an accurate time stamp.

5 IT Security Requirements

This section provides a list of all security functional requirements for the TOE as taken from the IDSSPP and CC Part 2. This ST includes one IT environment. The following table identifies the IT Security Requirement.

Security Functional Components	IT Environment
FPT_STM.1	Reliable time stamps

Table 1 IT Security Requirement

5.1 TOE Security Functional Requirements

The following table lists the SFRs required that are satisfied by the TOE.

Security Functional Class	Security Functional Components
Security audit (FAU)	Audit data generation (FAU_GEN.1)
	Audit review (FAU_SAR.1)
	Restricted audit review (FAU_SAR.2)
	Selectable audit review (FAU_SAR.3)
	Selective audit (FAU_SEL.1)
	Guarantees of audit data availability (FAU_STG.2)
	Prevention of audit data loss (FAU_STG.4)
Identification and authentication (FIA)	User authentication before any action (FIA_UAU.2)

Security Functional Class	Security Functional Components
	User attribute definition (FIA_ATD.1)
	User identification before any action (FIA_UID.2)
Security management (FMT)	Management of security functions behavior (FMT_MOF.1)
	Management of TSF data (FMT_MTD.1)
	Specification of Management Functions (FMT_SMF.1.1)
Protection of the TSF (FPT)	Security roles (FMT_SMR.1)
	Basic internal TSF data transfer protection (FPT_ITT.1)
	Non-bypassability of the TSP (FPT_RVM.1)
	TSF domain separation (FPT_SEP.1)
Intrusion Detection System (IDS)	Reliable time stamps (FPT_STM.1)
	System Data Collection (IDS_SDC.1)
	Analyzer analysis (IDS_ANL.1)
	Analyzer react (IDS_RCT.1)
	Restricted Data Review (IDS_RDR.1)
	Guarantee of System Data Availability (IDS_STG.1)
	Prevention of System data loss (IDS_STG.2)

Table 2 Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

5.1.1.1.1 FAU_GEN.1.1

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

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

b) All auditable events for the **[basic]** level of audit (see Table 2); and

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

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.2	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are	User identity

Component	Event	Details
	part of a role	

Table 3 Auditable Events

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

5.1.1.1.2 FAU_GEN.1.2 NIAP-0410

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 3 Auditable Events**].

5.1.1.2 Audit review (FAU_SAR.1)

5.1.1.2.1 FAU_SAR.1.1

The TSF shall provide **[authorized administrator, Security Expert, and System Administrator]** with the capability to read **[all of the audit information]** from the audit records.

5.1.1.2.2 FAU_SAR.1.2

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

5.1.1.3 Restricted audit review (FAU_SAR.2)

5.1.1.3.1 FAU_SAR.2.1

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

5.1.1.4 Selectable audit review (FAU_SAR.3)

5.1.1.4.1 FAU_SAR.3.1

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

5.1.1.5 Selective audit (FAU_SEL.1)

5.1.1.5.1 FAU_SEL.1.1

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

a) event type;

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

5.1.1.6 Guarantees of audit data availability (FAU_STG.2 – NIAP-0422)

5.1.1.6.1 FAU_STG.2.1 NIAP-0422

The TSF shall protect the stored audit records **in the audit trail** from unauthorized deletion.

5.1.1.6.2 FAU_STG.2.2 NIAP-0422

The TSF shall be able to detect modifications to the audit records **in the audit trail**.

5.1.1.6.3 FAU_STG.2.3(a)

The TSF shall ensure that [**all already recorded**] audit records will be maintained when the following conditions occur: [**failure, attack**].

5.1.1.6.4 FAU_STG.2.3(b)

The TSF shall ensure that [**newly generated]** audit records will be maintained when the following condition occurs [**storage exhaustion**]**.**

5.1.1.7 Prevention of audit data loss (FAU_STG.4)

5.1.1.7.1 FAU_STG.4.1

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

5.1.2 Identification and authentication (FIA)

5.1.2.1 User authentication before any action (FIA_UAU.2)

5.1.2.1.1 FIA_UAU.2.1

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

5.1.2.2 User attribute definition (FIA_ATD.1)

5.1.2.2.1 FIA_ATD.1.1

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

- **a)** User identity;
- **b)** Authentication data;
- **c)** Authorizations; and
- **d)** [**No other security attributes**].

5.1.2.3 User identification before any action (FIA_UID.2)

5.1.2.3.1 FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.3 Security management (FMT)

5.1.3.1 Management of security functions behavior (FMT_MOF.1)

5.1.3.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to modify the behavior of the functions of System data collection, analysis and reaction to **authorized administrator, Security Expert, and System Administrator**.

5.1.3.2 Management of TSF data (FMT_MTD.1)

5.1.3.2.1 FMT_MTD.1.1

The TSF shall restrict the ability to query and add System and audit data, and shall restrict the ability to query and modify all other TOE data to [**authorized administrator, Security Expert, and Systems Administrator**].

5.1.3.3 Specification of Management Functions (FMT_SMF.1) [RI-65][2]

5.1.3.3.1 FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: **[modify the behaviour of the system data collection, analysis and reactions, and the query audit data and system data].**

5.1.3.4 Security roles (FMT_SMR.1)

5.1.3.4.1 FMT_SMR.1.1

The TSF shall maintain the **following *roles:* authorized administrator, authorized System administrator, and [Security Expert, Operator, Restricted, and No Role].**

5.1.3.4.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.1.4 Protection of the TOE security functions (FPT)

5.1.4.1 Basic internal TSF data transfer protection (FPT_ITT.1)

5.1.4.1.1 FPT_ITT.1.1

The TSF shall protect TSF data from ***[modification]*** when it is transmitted between separate parts of the TOE.

5.1.4.2 Non-bypassability of the TSP (FPT_RVM.1)

5.1.4.2.1 FPT_RVM.1.1

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

5.1.4.3 TSF domain separation (FPT_SEP.1)

5.1.4.3.1 FPT_SEP.1.1

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

5.1.4.3.2 FPT_SEP.1.2

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

[2] This requirement has been modified to comply with International Interpretation #65

5.1.4.4 Reliable time stamps (FPT_STM.1)

5.1.4.4.1 FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use **with the assistance of the IT environment. (EXP)**

5.1.5 IDS Component Requirements (IDS)

5.1.5.1 System Data Collection (EXP) (IDS_SDC.1)

5.1.5.1.1 IDS_SDC.1.1

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

a) [***network traffic, detect known vulnerabilities***]

5.1.5.1.2 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 Systems Events. **(EXP)**

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Detect vulnerabilities	Identification of known vulnerability

Table 4 System Events

5.1.5.2 Analyzer analysis (EXP) (IDS_ANL.1)

5.1.5.2.1 IDS_ANL.1.1

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

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

b) [**thresholds, statistical anomaly, protocol anomaly-based detection mechanisms]. (EXP)**

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

5.1.5.3 Analyzer react (EXP) (IDS_RCT.1)

5.1.5.3.1 IDS_RCT.1.1

The System shall send an alarm to [**the administrator**] and take [**log an alert, drop packet, or send TCP reset, or send ICMP host unreachable, or log packet]** when an intrusion is detected. **(EXP)**

5.1.5.4 Restricted Data Review (EXP) (IDS_RDR.1)

5.1.5.4.1 IDS_RDR.1.1

The System shall provide [**authorized administrator, System Administrator, Operator, and Security Expert**] with the capability to read [**all captured IDS data**] from the System data. **(EXP)**

5.1.5.4.2 IDS_RDR.1.2

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

5.1.5.4.3 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. **(EXP)**

5.1.5.5 Guarantee of System Data Availability (EXP) (IDS_STG.1)

5.1.5.5.1 IDS_STG.1.1

The System shall protect the stored System data from unauthorized deletion. **(EXP)**

5.1.5.5.2 IDS_ STG.1.2

The System shall protect the stored System data from modification. **(EXP)**

5.1.5.5.3 IDS_STG.1.3

The TSF shall ensure that [**all already recorded**] system events will be maintained when the following conditions occur: [**failure, attack, storage exhaustion**].

5.1.5.6 Prevention of System data loss (EXP) (IDS_STG.2)

5.1.5.6.1 IDS_STG.2.1

The System shall [***ignore system data***] and send an alarm if the storage capacity has been reached. **(EXP)**

5.2 Security Functional Requirement for the IT Environment

5.2.1.1.1 FPT_STM.1.1

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

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.3 Authorization Controls
	ACM_SCP.1 TOE CM Coverage
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal Function Specification
	ADV_HLD.2 Security-enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration

Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life-cycle Support (ALC)	ALC_DVS.1 Identification of security measures
Tests (ATE)	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: High-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	ATE_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 5 EAL3 Assurance Components

5.3.1 Configuration Management (ACM)

5.3.1.1 Configuration Items (ACM_CAP.3)

5.3.1.1.1 ACM_CAP.3.1D

The developer shall provide a reference for the TOE.

5.3.1.1.2 ACM_CAP.3.2D

The developer shall use the CM system.

5.3.1.1.3 ACM_CAP.3.3D

The developer shall provide CM documentation.

5.3.1.1.4 ACM_CAP.3.1C

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

5.3.1.1.5 ACM_CAP.3.2C

The TOE shall be labeled with its reference.

5.3.1.1.6 ACM_CAP.3.3C

The CM documentation shall include a configuration list and a CM plan.

5.3.1.1.7 International Interpretation RI #3

The configuration list shall uniquely identify all configuration items that comprise the TOE.[3]

5.3.1.1.8 ACM_CAP.3.4C

The configuration list shall describe the configuration items that comprise the TOE.

[3] This new assurance requirement has been added to conform to International Interpretation RI #3

5.3.1.1.9 ACM_CAP.3.5C

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

5.3.1.1.10 ACM_CAP.3.6C

The CM system shall uniquely identify all configuration items.

5.3.1.1.11 ACM_CAP.3.7C

The CM plan shall describe how the CM system is used.

5.3.1.1.12 ACM_CAP.3.8C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

5.3.1.1.13 ACM_CAP.3.9C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

5.3.1.1.14 ACM_CAP.3.10C

The CM system shall provide measures such that only authorized changes are made to the configuration items.

5.3.1.1.15 ACM_CAP.3.1E

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

5.3.1.2 **TOE CM Coverage (ACM_SCP.1)**

5.3.1.2.1 ACM_SCP.1.1D **[RI-4][4]**

The developer shall provide a list of configuration items for the TOE.

5.3.1.2.2 ACM_SCP.1.1C **[RI-4][5]**

The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

5.3.1.2.3 ACM_SCP.1.1E

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

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Delivery Procedures (ADO_DEL.1)

5.3.2.1.1 ADO_DEL.1.1D

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

[4] This requirement has been modified to comply with International Interpretation RI #4
[5] This requirement has been modified to comply with International Interpretation #4

5.3.2.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

5.3.2.1.3 ADO_DEL.1.1C

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

5.3.2.1.4 ADO_DEL.1.1E

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

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

5.3.2.2.1 ADO_IGS.1.1D

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

5.3.2.2.2 ADO_IGS.1.1C **[RI-51]**

The **installation, generation and start-up** documentation shall describe **all** the steps necessary for secure installation, generation, and start-up of the TOE.[6]

5.3.2.2.3 ADO_IGS.1.1E

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

5.3.2.2.4 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal Function Specification (ADV_FSP.1)

5.3.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

5.3.3.1.2 ADV_FSP.1.1C

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

5.3.3.1.3 ADV_FSP.1.2C

The functional specification shall be internally consistent.

[6] This requirement has been modified to comply with International Interpretation #51.

5.3.3.1.4 ADV_FSP.1.3C

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

5.3.3.1.5 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

5.3.3.1.6 ADV_FSP.1.1E

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

5.3.3.1.7 ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

5.3.3.2.1 ADV_HLD.2.1D

The developer shall provide the high level design of the TSF.

5.3.3.2.2 ADV_HLD.2.1C

The presentation of the high level design shall be informal.

5.3.3.2.3 ADV_HLD.2.2C

The high level design shall be internally consistent.

5.3.3.2.4 ADV_HLD.2.3C

The high level design shall describe the structure of the TSF in terms of subsystems.

5.3.3.2.5 ADV_HLD.2.4C

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

5.3.3.2.6 ADV_HLD.2.5C

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

5.3.3.2.7 ADV_HLD.2.6C

The high level design shall identify all interfaces to the subsystems of the TSF.

5.3.3.2.8 ADV_HLD.2.7C

The high level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

5.3.3.2.9 ADV_HLD.2.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.2.10 ADV_HLD.2.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.3.3.2.11 ADV_HLD.2.1E

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

5.3.3.2.12 ADV_HLD.2.2E

The evaluator shall determine that the high level design is an accurate and complete instantiation of the TOE security requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

5.3.3.3.1 ADV_RCR.1.1D

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

5.3.3.3.2 ADV_RCR.1.1C

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

5.3.3.3.3 ADV_RCR.1.1E

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

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator Guidance (AGD_ADM.1)

5.3.4.1.1 AGD_ADM.1.1D

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

5.3.4.1.2 AGD_ADM.1.1C

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

5.3.4.1.3 AGD_ADM.1.2C

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

5.3.4.1.4 AGD_ADM.1.3C

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

5.3.4.1.5 AGD_ADM.1.4C

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

5.3.4.1.6 AGD_ADM.1.5C

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

5.3.4.1.7 AGD_ADM.1.6C

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

5.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documents supplied for evaluation.

5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

5.3.4.1.10 AGD_ADM.1.1E

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

5.3.4.2 User Guidance (AGD_USR.1)

5.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.3.4.2.2 AGD_USR.1.1C

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

5.3.4.2.3 AGD_USR.1.2C

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

5.3.4.2.4 AGD_USR.1.3C

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

5.3.4.2.5 AGD_USR.1.4C

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

5.3.4.2.6 AGD_USR.1.5C

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

5.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

5.3.4.2.8 AGD_USR.1.1E

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

5.3.5 Life Cycle Support (ALC)

5.3.5.1 **Identification of security measures (ALC_DVS.1)**

5.3.5.1.1 ALC_DVS.1.1D

The developer shall produce development security documentation.

5.3.5.1.2 ALC_DVS.1.1C

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

5.3.5.1.3 ALC_DVS.1.2C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.3.5.1.4 ALC_DVS.1.1E

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

5.3.5.1.5 ALC_DVS.1.2E

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

5.3.6 Security Testing (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

5.3.6.1.1 ATE_COV.2.1D

The developer shall provide an analysis of the test coverage.

5.3.6.1.2 ATE_COV.2.1C

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

5.3.6.1.3 ATE_COV.2.2C

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.3.6.2 ATE_COV.2.1E

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

5.3.6.3 Testing: high-level design (ATE_DPT.1)

5.3.6.3.1 ATE_DPT.1.1D

The developer shall provide the analysis of the depth of testing.

5.3.6.3.2 ATE_DPT.1.1C

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

5.3.6.3.3 ATE_DPT.1.2E

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

5.3.6.4 Functional testing (ATE_FUN.1)

5.3.6.4.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.3.6.4.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.3.6.4.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

5.3.6.4.4 ATE_FUN.1.2C

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

5.3.6.4.5 ATE_FUN.1.3C

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

5.3.6.4.6 ATE_FUN.1.4C

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

5.3.6.4.7 ATE_FUN.1.5C

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

5.3.6.4.8 ATE_FUN.1.1E

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

5.3.6.5 Independent testing – sample (ATE_IND.2)

5.3.6.5.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.3.6.5.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.3.6.5.3 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.

5.3.6.5.4 ATE_IND.2.1E

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

5.3.6.5.5 ATE_IND.2.2E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.3.6.5.6 ATE_IND.2.3E

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

5.3.7 Vulnerability Assessment

5.3.7.1 Examination of Guidance (AVA_MSU.1)

5.3.7.1.1 AVA_MSU.1.1D

The developer shall provide guidance documentation.

5.3.7.1.2 AVA_MSU.1.1C

The guidance documentation 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.

5.3.7.1.3 AVA_MSU.1.2C

The guidance documentation shall be complete, clear, consistent and reasonable.

5.3.7.1.4 AVA_MSU.1.3C

The guidance documentation shall list all assumptions about the intended environment.

5.3.7.1.5 AVA_MSU.1.4C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

5.3.7.1.6 AVA_MSU.1.1E

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

5.3.7.1.7 AVA_MSU.1.2E

The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

5.3.7.1.8 AVA_MSU.1.3E

The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

5.3.7.2.1 AVA_SOF.1.1D

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

5.3.7.2.2 AVA_SOF.1.1C

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

5.3.7.2.3 AVA_SOF.1.2C

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

5.3.7.2.4 AVA_SOF.1.1E

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

5.3.7.2.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

5.3.7.3.1 AVA_VLA.1.1D [RI-51]

The developer shall perform a vulnerability analysis.[7]

[7] This requirement has been modified to comply with International Interpretation #51.

5.3.7.3.2 AVA_VLA.1.2D [RI-51]

The developer shall provide vulnerability analysis documentation. [8]

5.3.7.3.3 AVA_VLA.1.1C [RI-51]

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.[9]

5.3.7.3.4 AVA_VLA.1.2C [RI-51]

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.[10]

5.3.7.3.5 AVA_VLA.1.3C [RI-51]

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. [11]

5.3.7.3.6 AVA_VLA.1.1E

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

5.3.7.3.7 AVA_VLA.1.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

[8] This requirement has been modified to comply with International Interpretation #51.
[9] This requirement has been modified to comply with International Interpretation #51.
[10] This requirement has been added to comply with International Interpretation #51.
[11] This requirement has been added to comply with International Interpretation #51.

6 TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

FAU_GEN.1 Audit Data Generation

The ISM generates audit records and stores them into the MySQL database, running on the same dedicated platform as does the IntruShield management software. The MySQL database provides storage and retrieval for audit log information. This function records attempts to access the system itself, such as successful and failed authentication, as well as the actions taken by the user once authenticated. Auditable actions include changes to the IDS rules and viewing the audit records.

Auditing is the recording of events within the system. The ISM records the audit information into a data store.

The following information about an audited event is stored in the audit log whenever that audited event is recorded in the audit information:

a) Startup and shutdown of the audit function,

b) Date and time of the event,

c) Type of event,

d) Subject (user) identity, and

e) the outcome (success or failure) of the event.

Other actions that can be performed at the Management Console are audited. This includes the following:

a) Access to the TOE and System data that includes the object IDS and the requested access

b) All modification to the audit configuration that occur during collection

c) All authentication attempts, including the user and location where authentication was attempted

d) All modification to the behavior of the TSF

e) All modifications to TSF data values

f) Modification of user accounts, creation, deletion, and modifications.

FAU_SAR.1 Audit Review

The ISM provides the ability for user with the authorized role to view security audit data for the system. The TSF provides the roles: authorized administrator known as Super User, Security Expert, and Systems Administrators with the capability to read all of the audit information from the audit records. The audit logs are viewable through the standard web-based management interface.

FAU_SAR.2 Restricted Audit Review

No security related actions can be taken without a successful user authentication, and hence only authorized users who have been authenticated into the Super user, Security Expert, and Systems Administrators role can view the audit records.

FAU_SAR.3 Selectable Audit Review

While viewing the security audit records, it is possible to sort and filter the data based upon the following properties:

- Date and time
- User
- Type of event
- Success or Failure of the event

FAU_SEL.1 Selectable Audit

The ISM allows a user with the Super User role to set the types of auditable events by their type. The ISM allows the Super User to include or exclude auditable events from the set of audited events based on the event type. Similarly, a person assigned to the Security Expert role can include or exclude recorded events in the traffic log that match a specific signature.

FAU_STG.2 Guarantees of Data Availability

The only way to access the audit records is through the management console. The TOE provides protection for the security audit records primarily by preventing access to the system without successful authentication. Secondly is the use of roles, requiring that a user have the proper role before gaining access to the audit records, even after a successful authentication. Further there is no TSF interface to disable audit or delete or modify audit records. The audit function starts automatically when the TOE is installed. Once recorded, audit data cannot be modified except, in the case where the audit log reach its capacity. Under these circumstances new audit data will overwrite the oldest audit data. This occurrence will also cause a system fault message to be posted to the system fault log. Only TSF interfaces to the audit mechanism allow the creation of an audit log, viewing audit information, backing up and restoring audit log information. The TSF shall ensure that all already recorded audit records will be maintained when the following conditions occur: failure, attack. The TSF shall ensure that [newly generated] audit records will be maintained when the following conditions occurs storage exhaustion.

FAU_STG.4 Prevention of Audit Data Loss

The ISM records the audit log information into a data store. The data store employed is a part of the ISM.

Data Store tables used for TSF audit data are capable in storing 50,000 audit records if the audit log should be filled up and alarm is presented at the Management console and the oldest data stored in the audit log is overwritten with the newest data.

6.1.2 Identification and Authentication

FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes: user name (identification data), password (authentication data), and their assigned role (authorizations data). A user can have more than one role but could not log-in with more than one role at any specified time. Role log-in ID depends on the domain.

FIA_UAU.2 User Authentication Before Any Action and FIA_UID.2 User Identification Before Any Action

Identification and authentication provided by the ISM, by requiring the user to enter both a user ID and a password. The user's ID and password supplied by the user are verified by comparing them to user attributes already established and stored. If the user ID and password matches a valid user attributes, the user supply that user ID and password is allowed to proceed with privileges determine by the role assigned to that user account. If the user ID and password do not match a valid user attributes, the user submitting them is simply return to the screen (or prompt) requesting user ID and password.

6.1.3 Security Management

FMT_MOF.1 Management of Security Functions Behavior

The ISM requires user authentication before any actions can be performed (other than identification and authentication) on the TOE, security-related or otherwise. Due to this, only authorized users can access any functions on the system. Signatures are updated by McAfee Incorporated on a protected server with a controlled space and/or by an administrative person with the Security Expert role. Only users with "System Administrator" privileges can implement rules on the IDS. System Administrators can also create, delete, and modify existing rules on the system. System Administrators are also the only role that can manage the security settings on the system, such as user accounts and audit settings.

FMT_MTD.1 Management of TSF Data

See FMT_SMR.1.

FMT_SMF.1 Specification of Management Functions (RI#65)

The ISM implements interfaces that allow users to perform the following instructions:

- Modify policies, including which events are detected, whether alerts are logged for each event detected and how the system will react when events are detected.
- Query the Audit Logs.
- Query the alerts logged for detected events.

FMT_SMR.1 Security Roles

The TSF is capable of maintaining the following roles. Authorized administrator is known as Super User role and authorized System Administrator is known as System Administrator.

Super User	All functions. Super Users must manage themselves within the domain(s) they reside. They can read, modify, delete and push policy. Super User's can also administer other administrators and their roles. Adding, maintaining, and deleting users and role assignments.
Restricted User	A restricted user has read-only access to Alert Viewer data. They can not read configuration information.
System Administrator	Manager, Sensors, Sensor_Name, and Failover Pairs node actions (interfaces and sub-interfaces included). System Admins do not control Super Users, and can change own role to anything but Super User. System Admins can add, maintain, and delete admin domains, read Alert data, read Audit data.
Operator	Reporting only. Run and analyze reports (Generate Reports).
Security Expert	Responsible for Policy configuration and application, software/signature updates, and alert monitoring (Alert Viewer and Report Generator).
No Role	The user cannot perform any actions. This is the state when a user is first created.

6.1.4 Protection of Security Functions

FPT_ITT.1 Basic internal TSF data transfer protection

The McAfee Incorporated Sensors, ISM, Update Server, and Management Console all protect TSF data from disclosure and modification, when it is transmitted between separate parts of the TOE, by communicating using SSL version 3.0 connections.

The Sensor communicates with ISM through its dedicated 10/100 Ethernet, out-of-band management port using TCP/IP. This communications uses secure channels; providing link privacy using encryption and mutual authentication using public key authentication. It is recommended that ISM use a separate, dedicated management subnet to interconnect with the sensor. ISM communicates with the Update Server using the same 10/100, out-of-band management Ethernet port. Communication between ISM and the Update Server is secured via SSL.

There is no communication between the sensor and Update Server.

FPT_RVM.1 Non-bypassability of the TSP

The TSF requires that all users successfully authenticate before any actions can view or modify the TSP. No actions are allowed on the TOE until after successful authentication, and the allowed actions are determined by the assigned user role.

The McAfee Incorporated sensors are protected on the monitored network by "hiding" the fact it is there. This is done by using a non-TCP/IP network stack on the sensors, which prevents it from being accessed as a network device on the network. Also, the signature files are protected doubly as the system is configured to not accept any management requests or input from the monitored network.

FPT_SEP.1 TSF Domain Separation

The TOE consists of three architecturally separate components that are: the IntruShield sensor(s), the IntruShield Security Management system, and the McAfee Incorporated Update server. The IntruShield sensor is an appliance dedicated to its function. The sensor's only interface that is external to the TOE is a passive listener and the sensor views the packet construction as input data only. The IntruShield ISM is a software application that executes on a dedicated platform with an operating system. The ISM has network connections to the IntruShield sensors and the Update server and an encrypted connection through HTTPS to a client web browser running in a user workstation. All of these network connections are encrypted. The IntruShield Update Server is a repository of signatures. It responds to requests from ISMs for a signature update or it sends scheduled signature updates to ISMs. The Update Server provides no other external interface and all ISM connections are encrypted.

FPT_STM.1 Reliable Time Stamps

The TOE uses Windows Time Services provided by the Windows operating system to provide time stamps for the TSF to write time stamps for audit records, both the security records and the System Data records.

Both the Update Server and the ISM receives reliable time stamps from the Windows 2000, which is part of the environment. The Sensor receives a time reference from the ISM.

The ISM periodically passes a timestamp reference to the sensor. The Sensor uses this timestamp to synchronize its own timing mechanism. The sensor has an independent timing mechanism, synchronizing at regular intervals by timestamps sent form the ISM. On the other hand, the ISM has no time mechanism and must retrieve the time from the Windows Time Service, provided by the Windows operating system, each time it requires a time reference. This is the same for the Update Server.

6.1.5 System Data Collection

IDS_SDC.1 System Data Collection

The collection subsystem is used to detect events while monitoring the target network. Upon detection of such events, the collection subsystem shall generate data, which is then sent to the ISM for storage in the system database. The types of events that can be detected are shown in the table below. For each event detected the

collection subsystem records and the ISM stores date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event along with additional details for each event type.

The Update Server maintains default signatures to detect currently known vulnerabilities and exploits of interest in network traffic. The ISM allows the Security Expert to establish new rules to detect new vulnerabilities as well as specific network traffic, allowing the Security Expert complete control over the types of traffic that will be monitored and to set rules to govern the collection of data regarding potential intrusions. The following table identifies the events audited and the information recorded in the audit record.

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Detect vulnerabilities	Identification of known vulnerability

6.1.6 System Data Analysis

IDS_ANL.1 Analyzer Analysis

To analyze the data collected by the McAfee Incorporated Sensor, the ISM uses signatures. A signature is the protection profile term for a rule as defined by the TOE. They are patterns of traffic that can be used to detect attacks or exploits. Since many attacks or exploits require several network connections to work, the ISM also provides the ability to detect these more complex patterns through sensors placed at strategic locations throughout the network.

The TOE comes with default signatures for known exploits, and the administrator can add new signatures at any time. New signatures are provided from the Update Server as they are created and are downloaded. New signatures also can be created by an administrator authenticated in the Security Expert role manually. This gives the administrator control over the detection of traffic, allowing customization for the intended environment.

When a pattern of traffic has been matched to a signature, the specific event is recorded in the traffic log where it can be viewed and analyzed by users authenticated in the Security Expert role. The events are logged with the following information: the event type and signature match, the time of the event, the data source and a copy of the packets used to identify the pattern.

A pattern of traffic that meets a signature is called an “alert.” The graphical interface to view alerts and alert analysis is the “Alert Viewer.” The Alert Viewer is used for the analysis of the alerts detected by IntruShield sensors. Alert details include transmission information such as source and destination IP addresses in the packet, as well as security analysis information (performed by the sensor) such as attack severity and type. Alerts are backed up to the database and archived in order of occurrence.

For detailed analysis of alert information, the Alert Viewer provides a “Drill Down” graphical administrative interface. Drill Down provides the administrator with the capability to review statistical, signature, threshold, and anomaly-based functions by port scan. Alert information is organized by category of alert as follows: _

- Severity: by severity,
- Attack: by attack name,
- Source IP: by source IP addresses,
- Destination IP: by destination (target) IP addresses,
- Interface: by the sensor interface where alerts were captured,
- Domain: by admin domain where alerts were captured,
- Type: by attack type,
- Sensor: by the sensors where alerts were captured, and
- Application Protocol: by the application protocol of the detected attack.

For each category of alert, the administrator may continue drill down to provide more detailed information. Drill Down allows the administrator to review alert category information by time, or details.

The “Time View” provides a view the alert count by blocks of time during a specific time period. Time periods are expressed in date/time range. Alert Viewer provides an interface to view alerts in real time, as they occur, as well as a historical view. The historical view sets the filter to retrieve information for both acknowledged and

unacknowledged alerts archived in the database during a specified time. The historical view does not refresh with new alerts as they occur, thus you can focus on analyzing all alerts within the time frame you requested.

The Alert Viewer provides a view to analyze an individual alert called the "Alert Details." The Alert Details interface lists all of the alerts for the selected time span in order of occurrence, with most recent being listed first. Alert details are presented in multiple named columns, known as *attributes*. The attributes represent packet fields such as source and destination IP, as well as sensor analysis fields such as attack severity and type.

The attributes in the Alert Details are as follows:

- Acknowledged: for Historical View, indicates state of recognition. If unchecked by an administrator, then the alert has not been manually acknowledged, Deleted: for Historical View, indicates if the alert has been selected for deletion during current analysis session,
- Time: time when the alert occurred. Alerts are listed from most (top of the list) to least (bottom) recent,
- Severity: system impact severity posed by the attack,
- Attack: specific name of the attack that triggered the alert,
- Source IP: IP address where the attack originated,
- Source IP Port: port on source machine where attack originated,
- Destination IP: IP address the attack was targeting,
- Destination IP Port: port on target machine where attack was destined,
- Domain: admin domain in which the attack was detected,
- Sensor: ID (*name*) of the sensor from where the alert was generated,
- Interface: sensor interface where the attack was detected, and
- Type: the type of attack. The choices are:
    - Exploit: an attack matching a known exploit attack signature.
    - Host Sweep: a reconnaissance attack attempting to see which IP addresses have live systems attached to them.
    - Port Scan: a reconnaissance attack attempting to see what services a particular system is offering.
    - Simple Threshold: denial of service attack against a set threshold limits.
    - Statistical: denial of service attack based on a learning statistical traffic profile.

Throttle: a number of the same Signature attack occurring that exceeded an established limit suppression threshold in a designated period.

IDS_RCT.1 Analyzer React

When signature matches are found, they can either be logged for later use or set to trigger an alarm. Current log entries can be viewed in real time by setting the "Real-time Log Viewer" values at the ISM Management console. Real-time viewing displays a limited number of entries as logged to the database. The number of entries to view can be selected as well as the refresh rate to refresh the console screen.

The ISM provides an interface to establish IDS security policies. A *security policy*, or IDS policy, is a set of rules that governs what traffic is permitted across your network, and how to respond to misuse of the network.
An IntruShield *policy* is a set of rules/instructions defining the malicious activity that can be detected and the response if the malicious activity is detected. Creating a policy enables an administrator in the Security Expert role to define an environment to protect by the different operating systems (OSs), applications, and protocols in the network. These environment parameters, or *rules*, relate to all of the well-known attacks defended against by IntruShield.

All activities for which the underlying traffic content can violate an IntruShield policy may not be malicious by itself, but may be explicitly forbidden by the usage policies of the network as defined by a security policy. These can include "protocol violations" wherein packets do not conform to network protocol standards. (For example, they are incorrectly structured, have an invalid combination of flags set, or contain incorrect values.) Examples might include TCP packets with their SYN and RST flags enabled, or an IP packet whose specified length doesn't match its actual length. A protocol violation can be an indication of a possible attack, but can also be triggered by malfunctioning software or hardware. Policy violations trigger alerts that are displayed on the Management Console.

Alerts are asynchronous notifications sent when a system event or attack triggers the IDS. When a transmission violating a security policy is detected by a sensor, the sensor compiles information about the offending transmission and sends the information to the ISM in the form of an alert. An alert contains a variety of information on the incident that triggered it—such as the type of attack, its source and destination IP addresses, its source and destination ports, as well as security analysis information (performed by the sensor) such as attack severity and type. In addition to the alert that is generated, the IDS policy may be configured to ensure that the sensor responds by doing one or more of the following:

- Dropping the packet
- Sending a TCP reset
- Generating alert
- Logging packets
- Dynamically changing a firewall rule
- Sending an ICMP Host Unreachable in response to attacks detected

These responses are configurable by the end user.

6.1.7 System Data Review, Availability and Loss

IDS_RDR.1 Restricted Data Review

The ISM provides an interface where only successfully authenticated users can access the TOE, and then only users with the Security Expert can view the traffic log data collected and analyzed by sensor. The data gathered by a sensor is transferred to the ISM and then saved in a MYSQL DATABASE table. The Management Console of the ISM provides a Graphical User Interface (GUI) menu driven tool to interpret and review log data based on specific search criteria.

For a user to be authenticated that must use a password with a minimum password length any eight characters on a keyboard. Account lockout is provided after an installed limit of failed password attempts has exceeded. The default limit is three.

IDS_STG.1 Guarantee of System Data Availability

The ISM protects the gathered system traffic logs from unauthorized modification or deletion by presenting only the web-based interface to all users. No users are allowed to edit the logs; they are marked for read-only access, preventing user modification.

Further there is no TSF interface to disable audit or delete or modify audit records. The ability to back up and restore these audit logs does exist. The audit function starts automatically when the TOE is installed. Once recorded, audit data cannot be modified or deleted except by the MYSQL DATABASE managing the audit data. The only TSF interfaces to the audit mechanism allow the creation of an audit log, viewing audit information, and copy the audit information to another media for back-up and restore purposes. The TSF shall ensure that [**all already recorded**] system events will be maintained when the following conditions occur: [***failure, attack, storage exhaustion***].

Audit data storage exhaustion can occur if the disk space allocated to the MYSQL DATABASE segment exceeds the storage allowed. If this unlikely event occurs, an alarm is set and an administrator must backup the audit and alert tables. This alarm is triggered when the log files reach 50%, 70% and 90% of their storage capacity limit.

To prevent audit data storage exhaustion, an administrator is instructed to set a schedule by which audit and alert information is periodically saved. One choice for backup causes all audit and alert tables to be saved on the installation folder, external device (e.g., zip drive), or network device. This action is taken through the ISM interface. The files will then be available for restore and view.

IDS_STG.2 Prevention of System Data Loss

The ISM records the system data into a data store. The data store employed is running on the same dedicated platform as does the IntruShield management. The MYSQL DATABASE provides storage and retrieval for the system data.

All MYSQL DATABASE tables used for TSF data are dynamically allocated so that the limit on the recording capacity of the information is the limit of the physical disk partition on the platform dedicated to the MYSQL

DATABASE data store. This assures there is always adequate disk space to record current and new data that has been found to match the current rule set.

When the storage capacity reach 50%, 70% and 90% of their storage capacity limit, an alarm is presented at the Management console. The administrator must then take action by using a graphical interface to copy the system data to another storage media.

To prevent system data storage exhaustion, an administrator is instructed to set a schedule by which system data is periodically saved. One choice for backup causes all system data to be saved on the installation folder, external device (e.g., zip drive), or network device. This activity is performed through the ISM user interface.

If the MYSQL DATABASE tables on a dedicated disk partition that stores the system data ever becomes exhausted, new system data will be ignored.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL3 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Life-cycle Support
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by McAfee Incorporated ensures that all configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. McAfee Incorporated ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. McAfee Incorporated performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation. These activities are documented in:

- Configuration Management

The Configuration Management assurance measure satisfies the ACM_CAP.3, and ACM_SCP.1 assurance requirements

6.2.2 Delivery and Guidance

McAfee Incorporated provides delivery documentation that explains how the TOE is delivered and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. McAfee Incorporated delivery procedures describe the steps to be used for the secure installation, generation, and start-up of the TOE. These procedures are documented in:

- NAI, IntruVert Order, Delivery, and Billing, Version 13, 6/23/04
- I-4000/I2600/I-1200 Manufacturing Flow Process and Test Plan Document, Version 6.0, #100-0006-00, 6/23/04
- Update Server Delivery Procedure, (ADO) Document, Version 1.0, 3/18/04

McAfee Incorporated provides administrator guidance in the installation and initialization procedures. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install McAfee Incorporated IDS products in accordance with the evaluated configuration.

The administrator guidance is documented in:

- IntruShield IDS System Sensor Installation and Configuration Guide, Version 1.8, 09-2003
- IntruShield Quick Start Guide, Version 1.8
- IntruShield IDS System Manager Installation Guide, Version 1.8, Rev. 3, 07-2004
- IntruShield IDS System Manager Administrator's Guide, Version 1.8, Revision 3, 6-2004
- IntruShield IDS System Getting Started Guide, Version 1.8, Revision 2, 6-2004
- IntruShield IDS Release Notes, Version 1.8

Since there are no users who are not a member of an administrative role, the Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1,
- ADO_IGS.1,
- AGD_ADM.1, and
- AGD_USR.1.

6.2.3 Development

The Design Documentation provided for IntruShield is provided in three documents:

- IntruShield Functional Specification,
- IntruShield High-level Design, and
- IntruShield Informal Correspondence

These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST). The Design Documentation security assurance measure satisfies the following security assurance requirement:

- ADV_FSP.1,
- ADV_HLD.2, and
- ADV_RCR.1.

6.2.4 Life-Cycle Support

The Life-cycle support documentation provided for IntruShield is provided in the document

- Assurance Lifecycle Support

The life-cycle document describes the physical, procedural, personnel, and other development security measures that are used in the development environment to protect the TOE. It includes the physical security of the development location and any procedures used to select development staff.

The Life-cycle Support documented procedures satisfies the ALC_DVS.1 security assurance requirement.

6.2.5 Tests

The Test Documentations are found in the following documents

- IntruShield IDS System Test (ATE)
- ATE Test Results

These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2,
- ATE_DPT.1,
- ATE_FUN, and
- ATE_IND.2.

6.2.6 Vulnerability Assessment

The claim made in this Security Target document is SOF-Basic. The only probabilistic or permutational function on which the strength of the authentication mechanisms depends is the password entered for login to the Management Console. This "Strength of Function" has a probability smaller than one in one million (.000001) that authentication data can be guessed. The minimum password length is 8 characters that can consist of alpha-numeric or symbol that is upper and lower-case sensitive, therefore, satisfying this requirement.

McAfee Incorporated performs vulnerability analyses of the TOE to identify weaknesses that can be exploited in the TOE. All of the SOF claims are based on password space calculations and based on the SOF rationale in this ST; a separate SOF analysis is not applicable. The vulnerability analysis is documented in:

- IntruShield Vulnerability Assessment

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA-MSU.1,
- AVA_SOF.1, and
- AVA_VLA.1.

7 Protection Profile Claims

The assumptions, policies, threats, security objectives and security functional requirements were derived from the IDSSPP. However, this ST does not claim conformance to the PP since the FPT_STM.1 is meet with a combination of the TOE and IT Environment.

This Security Target includes all applicable assumptions, organizational policies, security objectives, and threats statements described in the PP, verbatim. The following threats and security objectives were excluded due to the TOE not having scanner component:

- T.SCNCFG
- T.SCNMLC
- T.SCNVUL
- O.IDSCAN

Security Functional Requirements

This Security Target includes all of the Security Functional Requirements from the PP, except those exclusively related to authenticating external IT products. Specifically:

- FPT_ITA.1 – this requirement is intended to specify how audit and System data are made available to external (trusted) IT products that would provide audit and data services. Since the TOE provides these functions as internally, no external IT products are necessary, and therefore this requirement is not applicable.
- FPT_ITC.1 – this requirement is intended to specify how TSF data is protected while transmitted to external (trusted) IT products. Since the TOE provides all functionality for the IDS in a self-contained manner, no data is transferred to external products, and therefore this requirement is not applicable.
- FPT_ITI.1 - this requirement is intended to specify how modifications to TSF data can be detected when it is transmitted to external (trusted) IT products. This includes both integrity checks and detection of modification during transmission. Since the TOE does not transmit data to external products, this requirement is not applicable.

These three requirements apply to the transfer of information between trusted products. There is no such transfer with IntruShield as there is no such transfer in nearly all IDS systems. The three requirements were replaced with FPT_ITT.1 of the transfer of information between the TOE components.

Refinement

- FMT_MOF.1.1 – This requirement was refined to include the required administrative roles that have permissions to modify the behavior of the functions of System data collection, analysis and reaction. The permission is limited to authorized administrator known as Super User, Security Expert, and System Administrator.

Iterations

- FAU_STG.2.3 - This requirement is intended to satisfy the need for the TSF to ensure that all already recorded audit records will be maintained when failure, attack occurs and that newly generated audit records will be maintained when the storage exhaustion occurs.

Exclusions:

- FIA_AFL.1.1 and FIA_AFL.1.12 these security requirements were intended to detect attempts by untrusted external IT products to access the TOE. The TOE have account lockout specifications for these external IT product connections to the TOE. A required specification, for example, would require an authorized system administrator to specifically unlock a locked account. The TOE does not allow access to itself from external IT products; only authorized users may access the TOE. Therefore, this requirement is not applicable.

Inclusion of Operating System Assumption and an IT Environment Security Objective

- FMT_STM.1.1 – the ISM does not provide timestamps of its own. It relies on the Windows 2000 operating system, which is part of the environment, to provide it with an accurate time stamp. Having received this accurate time stamp from the environment, the ISM provides a time stamp to the Sensor. The Sensor uses this time stamp to set its own internal real time clock. A.TIME assumption and O.TIME an IT environment security objective addresses time stamp.

8 Rationale

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

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or organizational security policy.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	O.PROTCT	O,IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.TIME
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			
A.TIME																	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										
T.PRIVIL	X					X	X										
T.IMPCON					X	X	X					X					
T.INFLUX								X									
T.FACCNT									X								

	O.PROTCT	O,IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.TIME
T.SCNCFG																	
T.SCNMLC																	
T.SCNVUL																	
T.FALACT				X													
T.FALREC			X														
T.FALASC			X														
T.MISUSE		X															
T.INADVE		X															
T.MISACT		X															
P.DETECT		X							X								
P.ANALYZ			X														
P.MANAGE	X				X	X	X					X		X	X		
P.ACCESS	X					X	X										
P.ACCACT							X		X								
P.INTGTY										X							
P.PROTCT								X					X				

Table 6 Environment to Objective Correspondence

8.1.1.1 A.ACCESS

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

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

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

8.1.1.3 A.ASCOPE

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

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

8.1.1.4 A.PROTCT

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

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

8.1.1.5 A.LOCATE

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

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

8.1.1.6 A.MANAGE

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

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

8.1.1.7 A.NOEVIL

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

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

8.1.1.8 A.NOTRST

The TOE can only be accessed by authorized users.

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

8.1.1.9 A.TIME

The Windows Operating System, which is part of the environment, will provide a reliable time stamp.

The O.TIME IT environment security objective provides a reliable timestamp for the TOE to use for accurately tracking audit records. FPT_STM.1.1 requires the Windows operating system to provide this reliable time stamp. This time stamp will ensure that the TOE has an accurate time stamp to use in the audit trails.

8.1.1.10 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.

8.1.1.11 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.

8.1.1.12 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.

8.1.1.13 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.

8.1.1.14 T.IMPCON

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

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

8.1.1.15 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.

8.1.1.16 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.

8.1.1.17 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.

8.1.1.18 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.

8.1.1.19 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.

8.1.1.20 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.

8.1.1.21 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.

8.1.1.22 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.

8.1.1.23 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, and O.IDSENS objectives address this policy by requiring collection of audit, Sensor, and data.

8.1.1.24 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.

8.1.1.25 P.MANAGE

The TOE shall only be managed by authorized users.

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

8.1.1.26 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.

8.1.1.27 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.

8.1.1.28 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.

8.1.1.29 P. PROTCT

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

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

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 7** indicates the requirements that effectively satisfy the individual objectives.

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.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	ORESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.TIME
FAU_GEN.1										X			
FAU_SAR 1						X							
FAU_SAR.2							X	X					
FAU_SAR.3						X							
FAU_SEL.1						X				X			
FAU_STG.2	X						X	X	X		X		
FAU_STG.4									X	X			
FIA_UAU.2							X	X					
FIA_ATD.1								X					
FIA_UID.2							X	X					
FMT_MOF.1	X						X	X					
FMT_MTD.1	X						X	X			X		
FMT_SMF.1					X	X	X						
FMT_SMR.1								X					
FPT_ITT.1												X	
FPT_RVM.1	X					X		X		X	X		
FPT_SEP.1	X					X		X		X	X		

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	ORESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.TIME
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 7 Objective to Requirement Correspondence

8.2.1.1 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 successful before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

8.2.1.2 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].

8.2.1.3 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].

8.2.1.4 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]. The responses can be configured for each administrative domain [FMT_SMF.1]

8.2.1.5 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_SAR.3, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1]. The TSF is capable of performing security management functions through the administrator interface [FMT_SMF.1].

8.2.1.6 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.2, FIA_UAU.2]. 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]. The TFS is required to perform security management functions such as create log-ins and assign roles to user log-in IDs [FMT_SMF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].

8.2.1.7 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.2, FIA_UAU.2]. 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 TOE 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 [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

8.2.1.8 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 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].

8.2.1.9 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 that its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

8.2.1.10 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 TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1].

8.2.1.11 O.EXPORT

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

The TSF shall protect TSF data from modification when it is transmitted between separate parts of the TOE [FPT_ITT.1.1]. The encryption and authentication applied to system data while it is in transit between any two IDS components.

8.2.1.12 O.TIME

The TOE operating environment (Windows 2000), shall provide an accurate time stamp.

This IT security environment objective assures that an accurate time stamp is used by the TOE. Accurate record information based on time and date can be produced, queried, and tracked. This objective addresses A.TIME and Security Functional Requirement FMT_STM.1.1.

8.2.2 Strength of Function (SOF) Rationale

The rationale for TOE Strength of Function described in this section satisfies the SOF-Basic claim. The reasoning for SOF-Basic claim is that the TOE strength of function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential. The SOF-basic strength level is also sufficient to meet the objectives of the TOE given the security environment described in the ST.

This Security Target includes a probabilistic or permutation analysis of the password mechanism required by AVA_SOF.1. This is provided below along with specific functional security requirements:

> FIA_UAU.2.1 (Identification and Authentication) was satisfied in compliance with Protection Profile functional security requirement for SOF-Basic claim. The only probabilistic or permutational function on which the strength of the authentication mechanisms depends is the password entered for login into the Management Console.
>
> The Management Console valid range or values for password is at least 8 characters, is case sensitive, and can consist of any alpha-numeric character or symbol.
>
> The CEM general evaluation guidance (page 367) for SOF indicated that patterns of human usage must be taken into consideration. Assuming that in a worst case scenario a user chooses a number comprising only eight characters, the number of password permutations demonstrated is below:
>
> 52 alpha (upper 26 and lower 26 = 52)
> 10 digits (0 to 9)

32 symbols (~, `, !, @, #, $, %, ^, &, *, (,), _, +, -, =, [,], {, }, \, |, ;, : ", ', ,, ., <, >, ?, /)

94 possible values

$6.10x10^{15}$ or 94^8 = (94*94*94*94*94**94*94*94) = 6,095,689,385,410,816

Presume that a manual password input or entry is 6 seconds. The best number of attempts for an attacker is (60/6 = 10 possible password entries every minute, or 600 password entries every hour). Typically, an attacker would need to input (6,095,689,385,410,816/ 2 =) 3,047,844,692,705,408 passwords, over (3,047,844,692,705,408 / 600) 5,079,741,154,509 hours, prior to entering the correct password. The average triumphant attack would, as a result, occur in slightly less than:

5,079,741,154,509 / 24 /365) = 579,879,127 years

According to the Common Evaluation Methodology Table B3 (page 365), the elapse time *is not practical.* The result presents a HIGH strength of function, which surpasses SOF-Basic.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a medium level of risk to the assets. The security environment assumes physical protection and the TOE itself offers only a very limited interface and can only be configured during initialization, offering essentially no opportunity for an attacker to subvert the security policies without physical access. As such, it is believed that EAL 3 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, except as noted below. Table 8 Requirement Dependency Rationale lists each requirement from Section 5.1 with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is proved.

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.2	FIA_UID.2	YES
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	YES
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.2	YES

Table 8 Requirement Dependency Rationales

8.5 Explicitly Stated Requirements Rationale

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing

and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

The FPT_STM.1 is explicitly stated to address the provision of a timestamp by the TOE and its IT Environment which is not addressed by the CC Part 2. The dependency raised by this requirement is address with the addition of the FPT_STM.1 requirement on the IT Environment.

The ISM part of the TOE gets its time stamp from the environment. The ISM has no time mechanism and must retrieve the time from the Windows Time Service, provided by the Windows operating system, each time it requires a time reference.

8.6 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. Working together, this set of security functions satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The c security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 9 Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

	SECURITY AUDIT	IDENTITY & AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF SECURITY FUNCTIONS	SYSTEM DATA COLLECTION	SYSTEM DATA ANALYSIS	SYSTEM DATA REVIEW, AVAILABILITY & LOSS
FAU_GEN.1	X						
FAU_SAR 1	X						
FAU_SAR.2	X						
FAU_SAR.3	X						
FAU_SEL.1	X						
FAU_STG.2	X						
FAU_STG.4	X						
FIA_UAU.2		X					
FIA_ATD.1		X					
FIA_UID.2		X					
FMT_MOF.1			X				
FMT_MTD.1			X				
FMT_SMF.1			X				
FMT_SMR.1			X				
FPT_ITT.1				X			

	SECURITY AUDIT	IDENTITY & AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF SECURITY FUNCTIONS	SYSTEM DATA COLLECTION	SYSTEM DATA ANALYSIS	SYSTEM DATA REVIEW, AVAILABILITY & LOSS
FPT_RVM.1				X			
FPT_SEP.1				X			
FPT_STM.1				X			
IDS_SDC.1					X		
IDS_ANL.1						X	
IDS_RCT.1						X	
IDS_RDR.1							X
IDS_STG.1							X
IDS_STG.2							X

Table 9 Security Functions vs. Requirements Mapping

8.7 PP Claims Rationale

See section 7, Protection Profile Claims.