Intrusion, Inc. SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Security Target
December 20, 2002
Document No. F2-1202-004

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite L
Columbia, MD 21046-2587

Phone: 301-498-0150
Fax: 301-498-0855

The information in this document is subject to change. COACT, Inc. assumes no liability for any errors or omissions that may appear in this document.

DOCUMENT INTRODUCTION

Prepared By:

COACT, Inc.
9140 Guilford Road, Suite L
Columbia, Maryland 21046-2587

Prepared For:

Intrusion, Inc.
1101 East Arapaho Road
Richardson, Texas 75081

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
	December 20, 2002, Final release.

TABLE OF CONTENTS

LIST OF FIGURES ..... **xi**
LIST OF TABLES ..... **xiii**
LIST OF ACRONYMS ..... **xv**
1. SECURITY TARGET INTRODUCTION **1**
1.1 Security Target Reference 1
1.1.1 Security Target Name 1
1.1.2 TOE Reference 1
1.1.3 Security Target Evaluation Status 1
1.1.4 Evaluation Assurance Level 1
1.1.5 Keywords 1
1.2 TOE Overview 1
1.2.1 Security Target Organisation 2
1.3 Common Criteria Conformance 2
1.4 Protection Profile Conformance 2
2. TOE DESCRIPTION **3**
2.1 SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE Description 3
2.1.1 Physical Boundary 4
2.1.2 Logical Boundary 4
2.1.2.1 Sensor Executables 5
2.1.2.2 Administrative Console Executables 5
2.1.2.3 Additional Executables 5
2.1.3 System Requirements 6
2.2 SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Evaluated Configuration 7
3. SECURITY ENVIRONMENT **11**
3.1 Introduction 11
3.2 Assumptions 11
3.2.1 Connectivity Assumptions 11
3.2.2 Personnel Assumptions 12
3.2.3 Physical Assumptions 12
3.3 Threats 12
3.3.1 Threats Addressed by the TOE 12

3.3.2 Threats Addressed by the TOE Operational Environment 13
3.4 Organisational Security Policies 13
4. SECURITY OBJECTIVES 15
4.1 Security Objectives for the TOE 15
4.2 Security Objectives for the IT Environment 15
4.3 Security Objectives for the Non-IT Environment 15
4.4 Security Objectives Rationale 16
5. IT SECURITY REQUIREMENTS 31
5.1 Security Functional Requirements 31
5.1.1 Security Audit (FAU) 36
5.1.1.1 FAU_SAA.3 Simple Attack Heuristics 36
5.1.1.2 FAU_SAR.1 Audit Review 37
5.1.1.3 FAU_SAR.3 Selectable Audit Review 37
5.1.1.4 FAU_SEL.1 Selective Audit 38
5.1.2 Security Management (FMT) 39
5.1.2.1 FMT_MOF.1 Management of Security Functions Behaviour 39
5.1.2.2 FMT_MTD.1 Management of TSF Data 39
5.1.3 Protection of the TSF (FPT) 40
5.1.3.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection 40
5.1.4 Explicitly Stated Requirements (IDS) 41
5.1.4.1 FXP_IDS_ALM.1 Sensor Alarm 41
5.1.4.2 FXP_IDS_ANL.1 Sensor Data Analysis 42
5.1.4.3 FXP_IDS_COL.1 Sensor Data Collection 42
5.1.4.4 FXP_IDS_GEN.1 Sensor Data Generation 43
5.2 Security Functional Requirements for the IT Environment 45
5.2.1 Security Audit (FAU) 47
5.2.1.1 FAU_STG.1-NIAP-0423 Protected Audit Trail Storage 47
5.2.2 Identification and Authentication (FIA) 47
5.2.2.1 FIA_UAU.1 Timing of Authentication 47
5.2.2.2 FIA_UID.1 Timing of Identification 48
5.2.3 Security Management (FMT) 48
5.2.3.1 FMT_SMR.1 Security Roles 48

5.2.4 Protection of the TSF (FPT) 48
5.2.4.1 FPT_STM.1 Reliable Time Stamps 48
5.3 TOE Security Assurance Requirements 48
6. TOE SUMMARY SPECIFICATION 51
6.1 TOE Security Functions 51
6.2 Assurance Measures 67
6.2.1 Rationale for TOE Assurance Requirements 68
7. PROTECTION PROFILE CLAIMS 71
7.1 Protection Profile Reference 71
7.2 Protection Profile Refinements 71
7.3 Protection Profile Additions 71
7.4 Protection Profile Rationale 71
8. RATIONALE 73
8.1 Security Objectives Rationale 73
8.2 Security Requirements Rationale 73
8.3 TOE Summary Specification Rationale 73
8.4 PP Claims Rationale 73

LIST OF FIGURES

Figure 1 - TOE Evaluated Configuration..... 9

LIST OF TABLES

Table 1 - Correspondence Between Assumptions, Threats and Policies to Objectives 16
Table 2 - Functional Components..... 31
Table 3 - Functional Components to Objectives Mapping..... 34
Table 4 - Security Functional Requirements for the IT Environment..... 45
Table 5 - SFRs for the IT Environment to Objectives for the IT Environment Mapping..... 46
Table 6 - Assurance Requirements..... 48
Table 7 - Functions to Security Functional Requirements Mapping..... 51
Table 8 - Security Functional Requirements to Functions Mapping..... 54
Table 9 - Assurance Measures..... 67

ACRONYMS LIST

ARP	Address Resolution Protocol
CC	Common Criteria
EAL2	Evaluation Assurance Level 2
IDS	Intrusion Detection System
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
NIAP	National Information Assurance Partnership
NIDS	Network Intrusion Detection System
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
SF	Security Function
SFP	Security Function Policy
SNMP	Simple Network Message Protocol
SNP	SecureNet Pro™
SOF	Strength of Function
SP1	Service Pack 1
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
WAN	Wide Area Network

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) interpretations through December 20, 2002. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Security Target

1.1.2 TOE Reference

SecureNet Pro™ Intrusion Detection System Version 4.1 SP1

1.1.3 Security Target Evaluation Status

The COACT, Inc. CAFE Laboratory has evaluated this ST.

1.1.4 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.1*.

1.1.5 Keywords

Intrusion Detection, Intrusion Detection System (IDS), Sensor, SecureNet™ CC, SecureNet Pro™ (SNP)

1.2 TOE Overview

This Security Target defines the requirements for the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE. The TOE is the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1, which is a network monitoring and intrusion detection software based application. The SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE is deployed as a two-tier architecture (SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Sensor and SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Administrative Console) or as an optional three-tier architecture (Sensor, Administrative Console, and Provider Manager). The

evaluated configuration, which this ST defines, is the two-tier architecture that includes the Sensor and Administrative Console only, the Provider Manager is an optional feature and thus, outside the scope of this ST. For this evaluation, SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE is divided into two primary parts, the Sensor and the Administrative Console. The Sensor performs intrusion detection and analysis functions. The Administrative Console enables the Administrator to monitor, configure and administer Sensors remotely, view Sensor monitoring sessions, replay archived sessions and generate reports.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

The SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE is compliant with the Common Criteria (CC) Version 2.1, functional requirements (Part 2) extended and assurance requirements (Part 3) conformant for EAL2.

1.4 Protection Profile Conformance

The SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE does not claim conformance to any registered Protection Profile.

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE Description

The SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE is a network monitoring and intrusion detection software based application. The SecureNet™ Pro Intrusion Detection System Version 4.1 SP1 TOE is deployed as a two-tier architecture (SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Sensor and SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Administrative Console) or as an optional three-tier architecture (Sensor, Administrative Console, and Provider Manager). The evaluated configuration, which this ST defines, (reference Section 2.2 of this ST) is the two-tier architecture that includes the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Sensor and SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Administrative Console only. The Provider Manager is an optional feature and thus, outside the scope of this ST. For this evaluation, SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE is divided into two primary parts, the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Sensor and the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Administrative Console software applications. Note: The remainder of this ST refers to the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE as the "TOE", the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Sensor as the "Sensor" and the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Administrative Console as the "Administrative Console". The Sensor performs intrusion detection and analysis functions. The Administrative Console enables the Administrator to monitor, configure and administer Sensors remotely, view Sensor monitoring sessions, replay archived sessions and generate reports. The Sensor captures data that is being sent across a network through a network interface running in promiscuous mode. As such, it monitors packets on the network and attempts to discover unauthorised access and improper or malicious use. The network interface running in promiscuous mode allows the Sensor to operate unobtrusively, quietly gathering data from the network on which it is installed. By running the network interface in promiscuous mode, the TOE, running signature pack 1.3, receives all packets travelling through the local network. The Sensor identifies intrusion attempts based on signature recognition of known attack scenarios using signature pack 1.3. The authenticity of the

SecureNet Pro™ Signature Packs is verified using MD-5 checksum or Gnu Privacy Guard. Signatures are required input for proper operation of the TOE but all signatures are outside the scope of this evaluation.

The Sensor is placed on strategic points of the network, where the bulk of network traffic will pass, and the Administrative Console is placed on a more secure part of the network. The Sensor monitors, captures, and analyses network traffic searching for intrusion attempts based on signature recognition of known attack scenarios and improper or malicious use. The Sensor stores the data it has captured to disk and responds to queries from the Administrative Console by forwarding the requested data. The Sensor sends alert messages to the Administrative Console in the event it discovers a potential threat to the network.

The Administrative Console is a group of X Windows applications, requiring an X display system to execute, which gives the Administrator the capability to perform Sensor management through a Graphical User Interface (GUI). Additionally, the Administrative Console is used for report generation, real-time Sensor activity decoding (monitoring session), and replaying logged (stored on disk) Sensor activity decoding.

2.1.1 Physical Boundary

The physical Boundary of the TOE includes both the Sensor software application and the Administrative Console software application. The hardware that both applications run on is outside the scope of this evaluation. All system requirements, including the required hardware for both the Sensor and the Administrative Console are outlined in Section 2.1.3 of this ST. It should be noted that the hardware platform and the required system components used to support the Sensor software application are delivered to the client when the SecureNet™ CC7345 delivery package is purchased from Intrusion, Inc. The SecureNet™ CC7345 delivery package also includes the Administrative Console software application however, the hardware platform used to support the Administrative Console is not part of the SecureNet™ CC7345 delivery package.

2.1.2 Logical Boundary

The logical boundary of the TOE is the SNP executables that are responsible for enforcing the TOE security functions. These executables are SNPd (the Sensor executable), SNPc (the Console executable), SNPv (the Session Manager executable), SNPreport (the report generation executable), SNPconfigEngine (Sensor initialisation) and

SNPconfigConsole (Console initialisation). These executables are further discussed in the following subsections.

2.1.2.1 Sensor Executables

The Sensor consists of one primary executable called SNPd. SNPd performs the following tasks:

A) Network monitoring: captures data through a network interface running in promiscuous mode.

B) Activity decoding: decodes, reads, and analyses packet content.

C) Intrusion detection: recognise intrusion attempts.

D) Intrusion response: records information about the intruder and sends alerts(s) to the Administrative Console Event Log. Generates Transport Control Protocol (TCP) resets to prevent Address Resolution Protocol (ARP) attacks and to prevent attacks from determining the Media Access Control (MAC) address of the SecureNet™ CC7345 hardware platform. Optional email notification and Simple Network Message Protocol (SNMP) traps to a network management system is also offered but beyond the scope of the evaluated configuration.

2.1.2.2 Administrative Console Executables

The Administrative Console is a group of X Windows applications that consists of three primary executables; SNPc (Console), SNPv (Session Manager), and SNPreport. SNPc is the primary Administrative Console executable. SNPc manages event data from the monitored Sensor and spawns SNPv and SNPreport when the Administrator selects this option. SNPc spawns SNPv, the Session Viewer, when requested by the Administrator. SNPv is the executable that establishes connections to the monitored Sensor and handles displaying them on the Administrative Console. SNPc spawns SNPreport, the report generator, when requested by the Administrator. SNPreport accepts parameters from the Administrator and displays a report using a local Web browser.

2.1.2.3 Additional Executables

There are two executables that are necessary for the initial configuration of the Sensor and the Administrative Console; the SNPconfigEngine and SNPconfigConsole system configuration files. Initial configuration of the Sensor and Administrative Console is done through the Pilot HTTPS Web GUI interface using these configuration files. The

Web GUI interface is outside the scope of this evaluation. SNPconfigEngine is executed during initialisation of the Sensor and is used to build the trusted Administrative Console configuration file. SNPconfigConsole is executed during the initialisation of the Administrative Console and is used to build to the trusted Sensor configuration file. The Sensor will not report to the Administrative Console unless the Administrator has built a configuration file on the Sensor containing parameters and a password linking that Sensor to the Administrative Console. Likewise the Administrative Console will not accept reports from the Sensor unless the Administrator has built a configuration file on the Administrative Console containing parameters and a password linking it to the Sensor. Note: It is possible and permissible to link the Sensor to more than one Administrative Console and to link the Administrative Console to several Sensors however, doing so is outside the scope of this ST and the evaluated configuration that this ST defines.

2.1.3 System Requirements

When SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE is delivered to the customer, it is included as part of the SecureNet™ CC7345 delivery package. The SecureNet™ CC7345 delivery package includes:

A) SecureNet™ CC7345 hardware platform.

B) Red Hat 6.2 Operating System based on installing Pilot 2.3 SP2 (an integrated software application package running Linux kernel 2.2.19-17 PDS).

C) SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 software application (TOE) provided on CD-ROM.

NOTE: When the SecureNet™ CC7345 delivery package is purchased both the Sensor software application and the Administrative Console software applications are provided on this CD-ROM. However, the Sensor software application is pre-installed on the SecureNet™ CC7345 hardware platform (discussed above) when delivered to the client.

NOTE: The Administrative Console software application must be installed and configured on an X86 hardware platform by an authorised Administrator. The X86 hardware platform used to run the Administrative Console is not part of the SecureNet™ CC7345 delivery package. System requirements for the Administrative Console software application are discussed in the following paragraph.

D) CD with documentation and training manuals.

E) Signature Pack 1.3 (default version 1.3 installed for evaluated configuration; updated Signature Pack versions may be installed; Signature Packs, including version 1.3, are outside the scope of this evaluation).

The Administrative Console software application provided on CD-ROM is included as part of the SecureNet™ CC7345 delivery package. The Administrative Console software application requires an X86 based hardware platform. This X86 based hardware platform required for the Administrative Console software application is not part of the SecureNet™ CC7345 delivery package. The Administrator is responsible for obtaining the minimum platform requirements that are necessary to install, configure and execute the Administrative Console software application. The minimum platform requirements for the Administrative Console software application are as follows: X86 based hardware platform, Red Hat 6.2 Operating System running Linux kernel 2.2.19-17, Pentium III 500 MHz CPU, 256 MB RAM, 8 GB disk space, 100-Mbps NIC, and an X Windows System and application software. The Administrative Console software application can be installed on any system meeting these requirements.

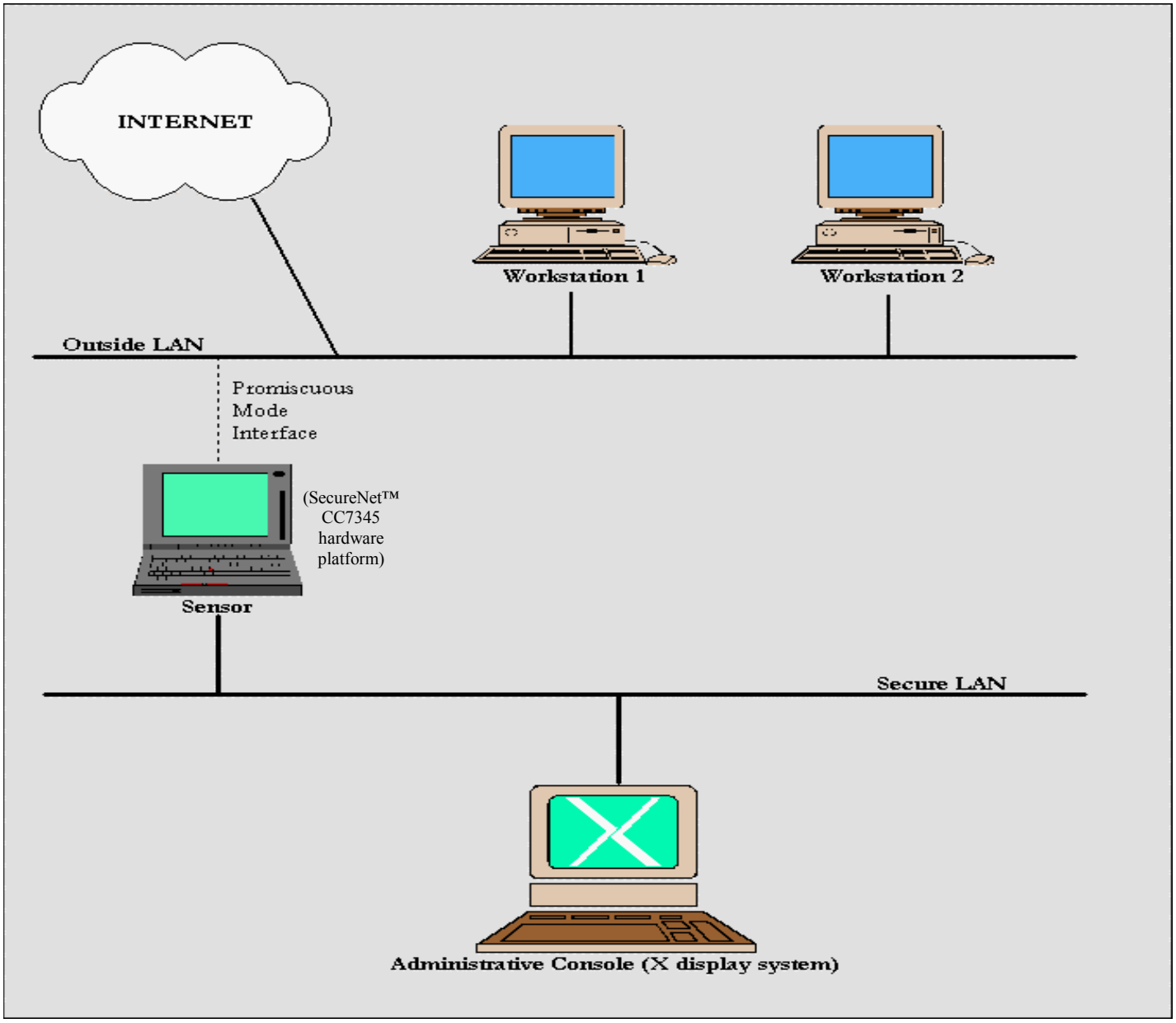
2.2 SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Evaluated Configuration

There are three possible deployments for the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE however; the evaluated configuration discussed in the following paragraph is the only deployment compliant with this Security Target. All other deployments are outside the scope of this ST and thus, do not comply with the evaluated configuration discussed below.

The Administrative Console is deployed on a secure LAN and requires a dedicated host for execution. This secure network does not have direct links to untrusted LANs. The Sensor, running on the SecureNet™ CC7345 hardware platform is connected to the same Secure LAN from one connection and a promiscuous mode interface connects the Sensor to an outside LAN to monitor all traffic on the public network. The secure LAN is used only for the purpose of handling communications between the Sensor and the Administrative Console, thus communication with the Administrative Console is limited only to the Sensor. The evaluated configuration of the TOE is valid only when the operational environment of the TOE utilises all components delivered with the SecureNet™ CC7345 delivery package as specified in Section 2.1.3 and when the TOE's operational environment is compliant with all system requirements

outlined in Section 2.1.3. The following image is a graphical depiction of the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE Evaluated Configuration.

Figure 1 - TOE Evaluated Configuration



CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) IT related threats to the organisation countered by the TOE.

C) Environmental threats requiring controls to provide sufficient protection.

D) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies assumptions (A), threats (T) and organisational security policies (P). For assumptions, threats or policies that apply to the environment, the initial character is followed by a period and then an 'E'. For example, T.E.DOS is a security threat to the environment via a Denial of Service attack.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

3.2.1 Connectivity Assumptions

A.CONSOL The Administrative Console software application will be installed, configured and operated on a dedicated host that meets the system requirements specified to support the Administrative Console software application supplied as part of the SecureNet™ CC7345 delivery package.

A.INTER The Operating System that runs the Administrative Console environment provides the Administrator with an interface to the TOE through an X Windows GUI application.

A.OPSYS The Sensor is run on the Pilot 2.3 SP2 Operating System.

A.SENSOR The SecureNet™ CC7345 delivery package is provisioned and includes all hardware and software necessary to run the Sensor software application. The Sensor software application is delivered to the customer in a pre-installed and operational state.

A.SUPPORT The Pilot 2.3 SP2 Operating System will provide necessary support for the Sensor. The Red Hat Linux 6.2 Operating System will provide necessary support for the Administrative Console.

A.UNAUTH Unauthorised access to the TOE is prevented by the security features of the Operating System, external to the TOE.

3.2.2 Personnel Assumptions

A.ATCKSIG The Administrator is responsible for obtaining the latest signature pack from the Intrusion, Inc. web site for use by the TOE.

A.CONFIG The Administrator will run the configuration executables at system initialisation to build the trusted Sensor and trusted Administrative Console configuration files. The Administrator will follow all administrative guidance procedures supplied in the SecureNet™ CC7345 delivery package to ensure proper configuration of these files.

A.INSTALL The Administrator will follow all administrative guidance procedures supplied in the SecureNet™ CC7345 delivery package to ensure proper installation of the Administrative Console software application.

A.IPADD The Administrator will configure all IP addresses to be monitored by the Sensor.

A.NOEVIL The Administrator is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.2.3 Physical Assumptions

A.CC7345 The SecureNet™ CC7345 delivery package will be purchased from Intrusion, Inc. and delivered to the customer with all specified hardware and software necessary to ensure the TOE's compliance with the requirements outlined in this ST.

A.DEPLOY The Administrative Console requires a dedicated host for execution and is deployed on a secure LAN that has no direct links to untrusted LANs.

A.LOCATE The Administrative Console and the Sensor are located in a physically secure area.

3.3 Threats

3.3.1 Threats Addressed by the TOE

T.ATTACK An authorized or unauthorized user may attempt to unobtrusively attack the systems monitored by the TOE.

3.3.2 Threats Addressed by the TOE Operational Environment

T.E.ATKSIG The Sensor may fail to detect new intrusion scenarios or inappropriate activity on the network.

T.E.CONFIG The Sensor or the Administrative Console may be improperly configured by the Administrator causing intrusion attempts to go undetected.

T.E.CONSL An unauthorised user may gain access to the Administrative Console and attempt to compromise the integrity of the Administrative Console through malicious activity.

T.E.SENSR An unauthorised user may gain access to the Sensor and attempt to compromise the integrity of the Sensor through malicious activity.

3.4 Organisational Security Policies

There are no organisational security policies enforced by the TOE.

CHAPTER 4

4. Security Objectives

4.1 Security Objectives for the TOE

The objectives listed in this section ensure that all of the security threats listed in Chapter 3 have been countered. The security objectives (O) for SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 are:

O.ADMIN The Administrative Console will manage the Sensor and its functions.

O.DETECT The Sensor will monitor the environment and detect intrusion attempts to the network or systems on the network by monitoring all data sent across the network.

O.RESPON The Sensor will respond to detected events by sending alerts of intrusion attempts or inappropriate activity occurring on the network or systems on the network to the Administrative Console.

O.SENSOR The Sensor will collect and store information about all events that are indicative of intrusion attempts or inappropriate activity occurring on the network or systems on the network that the Sensor is monitoring.

4.2 Security Objectives for the IT Environment

O.E.AUDPRO The IT Environment will provide protection from unauthorised deletion for the audit records generated by the TOE.

O.E.I&A The IT Environment will provide Identification and Authentication for authorized users of the TOE.

O.E.ROLES The IT Environment will provide Roles for authorised users of the TOE.

O.E.TIME The IT Environment will provide reliable time stamps for use by the TOE.

4.3 Security Objectives for the Non-IT Environment

O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE.

O.E.LOCATE The Administrative Console and the Sensor will be located in a physically secure area.

O.E.PSWRD The Administrator of the TOE will not reveal the root password that grants access to the Sensor host or the Administrative Console host.

O.E.INSTAL Proper installation of the TOE in compliance with the specified system requirements provides a sound operational environment for the TOE.

O.E.CONFIG Proper configuration of the TOE in compliance with the specified system and connectivity requirements provides a sound operational environment for the TOE.

O.E.OPER Proper operation and maintenance of the TOE in a secure area provides a secure operational environment for the TOE.

O.E.ATKSIG The Administrator will ensure that the latest signature packs are downloaded from the Intrusion, Inc. web site for use by the TOE.

4.4 Security Objectives Rationale

Table 1 demonstrates the correspondence between the security objectives listed in Sections 4.1, 4.2 and 4.3 to the assumptions, threats and policies identified in Sections 3.2, 3.3 and 3.4.

Table 1 - Correspondence Between Assumptions, Threats and Policies to Objectives

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
A.CONSOL The Administrative Console software application will be installed, configured and operated on a dedicated host that meets the system requirements specified to support the Administrative Console software application supplied as part of the SecureNet™ CC7345 delivery package.	O.E.INSTAL Proper installation of the TOE in compliance with the specified system requirements provides a sound operational environment for the TOE. O.E.CONFIG Proper configuration of the TOE in compliance with the specified system and connectivity requirements provides a sound operational environment for the TOE. O.E.OPER Proper operation and maintenance of the TOE in a	The Administrative Console software application is delivered to the customer as part of the SecureNet™ CC7345 delivery package. This delivery package includes guidance documentation to support the correct installation, configuration, and operation of the Administrative Console. The Administrative Console will perform all of its objectives correctly when the Administrative Console software application has been installed, configured and operated in a manner that is consistent with the supplied

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
	secure area provide a secure operational environment for the TOE.	guidance documentation.
A.INTER The Operating System that runs the Administrative Console environment provides the Administrator with an interface to the TOE through an X Windows GUI application.	O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE. O.E.I&A The IT Environment will provide Identification and Authentication for authorized users of the TOE.	The Administrative Console is an X-Windows application through which the Administrator performs all aspects of Sensor management graphically. In order to install, configure, or run the Administrative Console, the Administrator must be logged in to the Operating System (OS) of the host as the root user. The SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE is protected from unauthorised access not by its own security features but by the security features of the host's Operating System. When an Administrator performs any administrative task, a connection circuit is established from the Administrative Console's host to the Sensor.
A.OPSYS The Sensor is run on the Pilot 2.3 SP2 Operating System.	O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE.	The Sensor is deployed on a modified version of the Red Hat Linux 6.2 Operating System, Kernel 2.2.19-17 PDS. Intrusion, Inc. refers to this modification of the OS as Pilot, Version 2.3 SP2. This is a securely configured OS, as it is provided by Intrusion, Inc. as part of the SecureNet™ CC7345

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
		delivery package. The Administrator is responsible for ensuring that the Sensor operates on this securely configured Pilot 2.3 SP2 Operating System; the use of any other Operating System negates the results of this evaluation.
A.SENSOR The SecureNet™ CC7345 delivery package is provisioned and includes all hardware and software necessary to run the Sensor software application. The Sensor software application is delivered to the customer in a pre-installed state.	O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE.	The Sensor is delivered to the customer in a pre-installed state. The Sensor is run on the SecureNet™ CC7345 hardware platform that is supplied to the customer as part of the SecureNet™ CC7345 delivery package. The Administrator is responsible for ensuring that all hardware and software components included in this delivery package are utilised in accordance with the guidance specified in the supplied documentation to enforce the and maintain the integrity of the TOE.
A.SUPPORT The Pilot 2.3 SP2 Operating System will provide necessary support for the Sensor. The Red Hat Linux 6.2 Operating System will provide necessary support for the Administrative Console.	O.E.AUDPRO The IT Environment will provide protection from unauthorized deletion for the audit records generated by the TOE. O.E.I&A The IT Environment will provide Identification and Authentication for authorized users of the TOE.	These IT environment objectives are enforced through functions of the Pilot 2.3 SP2 Operating System, which provides the necessary support for the Sensor to perform its functions. These IT environment objectives are enforced through functions of the Red Hat Linux 6.2 Operating

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
	O.E.ROLES The IT Environment will provide Roles for authorized users of the TOE. O.E.TIME The IT Environment will provide reliable time stamps for use by the TOE.	System, which provides the necessary support for the Administrative Console to perform its functions.
A.UNAUTH Unauthorised access to the TOE is prevented by the security features of the Operating System, external to the TOE.	O.E.I&A The IT Environment will provide Identification and Authentication for authorized users of the TOE. O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE.	The Sensor software application is protected from unauthorised access not by it's own security features but by the security features of the Pilot 2.3 SP2 Operating System, external to the TOE. Pilot 2.3 SP2 provides adequate protection for the TOE from unauthorised access. The Administrative Console software application is protected from unauthorised access not by it's own security features but by the security features of the Red Hat Linux OS that the Administrative Console runs on. The Administrator is responsible for ensuring that all hardware and software components utilised to support both the Sensor and Administrative Console software applications are operated and maintained in a secure environment and in a manner that is consistent with the guidelines specified in the documentation

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
		supplied to support the operation of the TOE.
A.ATCKSIG The Administrator is responsible for obtaining the latest signature pack from the Intrusion, Inc. web site for use by the TOE.	O.E.ATKSIG The Administrator will ensure that the latest signature packs are downloaded from the Intrusion, Inc. web site for use by the TOE.	The recommended method for downloading updated signature packs (signed with GnuPG) from the Intrusion, Inc. website is to use a third party system, from any computer with access to the Internet. The updated signature packs are then transferred to the Sensor to be incorporated into SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 TOE. The Administrator is responsible for obtaining these signature packs which are necessary to enforce the continued integrity of the TOE. The procedures for updating the signature packs are detailed in the guidance documentation delivered with the TOE as part of the SecureNet™ CC7345 delivery package. The Administrator must follow these procedures as instructed.
A.CONFIG The Administrator will run the configuration executables at system initialisation to build the trusted Sensor and trusted Administrative Console configuration files. The Administrator will follow all administrative	O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE.	The Administrator is responsible for configuring all software, as specified in the guidance documentation supplied in the SecureNet™ CC7345 delivery package to ensure that the TOE is operated and maintained in a manner that is necessary to

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
guidance procedures supplied in the SecureNet™ CC7345 delivery package to ensure proper configuration of these files.	O.E.CONFIG Proper configuration of the TOE in compliance with the specified system and connectivity requirements provides a sound operational environment for the TOE.	enforce the continued integrity of the TOE. For the Administrative Console to manage the Sensor, the Administrator must first configure the Sensor as a trusted SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 component. Trusted Sensor configuration is a required process; if it is not performed, the Administrative Console will not communicate with any Sensors. This process must be performed according to the procedures outlined in the guidance documentation delivered with the TOE as part of the SecureNet™ CC7345 delivery package. For the Sensor to be managed from the Administrative Console, the Administrator must configure the specific Administrative Consoles that are to be trusted. The Sensor does not simply allow any Administrative Console to manage it. Instead, only specific “trusted” Administrative Consoles are allowed access to the Sensor. All trusted Administrative Console configuration must be performed according to

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
		the procedures outlined in the guidance documentation delivered with the TOE as part of the SecureNet™ CC7345 delivery package.
A.INSTALL The Administrator will follow all administrative guidance procedures supplied in the SecureNet™ CC7345 delivery package to ensure proper installation of the Administrative Console software application.	O.E.INSTAL Proper installation of the TOE in compliance with the specified system requirements provides a sound operational environment for the TOE.	The Administrator is responsible for installing all software, as specified in the guidance documentation supplied in the SecureNet™ CC7345 delivery package to ensure that the TOE is properly installed and capable of operating in a manner that is necessary to enforce the continued integrity of the TOE.
A.IPADD The Administrator will configure all IP addresses to be monitored by the Sensor.	O.E.CONFIG Proper configuration of the TOE in compliance with the specified system and connectivity requirements provides a sound operational environment for the TOE.	The Administrator is responsible for configuring all software, as specified in the guidance documentation supplied in the SecureNet™ CC7345 delivery package to ensure that the TOE is operated and maintained in a manner that is necessary to enforce the continued integrity of the TOE. For the Sensor to engage in its network monitoring activity-decoding tasks, the Administrator must first correctly configure the IP addresses to be watched. A Sensor only performs state-based intrusion detection on monitored IPs. Non-specified IPs are still monitored using non state-based intrusion

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
		detection techniques. A Sensor only decodes network activity either originating from or destined to a monitored IP address. This allows the Administrator to configure only specific hosts, such as network servers or the workstations of "problem users" to be monitored. For the Sensor to automatically discover IP addresses that are to be monitored, the Administrator must configure the IP address ranges that are considered to be "internal networks." If activity originating from or destined to an address within these ranges is seen, the Sensor detects IP addresses.
A.NOEVIL The Administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE. O.E.OPER Proper operation and maintenance of the TOE in a secure area provide a secure operational environment for the TOE.	The site where SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 is installed will have its own maintenance procedures, physical security, personnel security, and procedural security. The Administrator will configure, operate and maintain the TOE as specified according to the requirements detailed in this ST.

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
A.CC7345 The SecureNet™ CC7345 delivery package will be purchased from Intrusion, Inc. and delivered to the customer with all specified hardware and software necessary to ensure the TOE's compliance with the requirements outlined in this ST.	O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE.	The Administrator will ensure that all hardware and software components necessary to ensure the TOE's full compliance are received in the SecureNet™ CC7345 delivery package with no evidence of tampering. The Administrator will support the TOE's purpose by operating and maintaining the TOE in a manner that is consistent to enforce its continued integrity.
A.DEPLOY The Administrative Console requires a dedicated host for execution and is deployed on a secure LAN that has no direct links to untrusted LANs.	O.E.CONFIG Proper configuration of the TOE in compliance with the specified system and connectivity requirements provides a sound operational environment for the TOE. O.E.INSTAL Proper installation of the TOE in compliance with the specified system requirements provides a sound operational environment for the TOE. O.E.ADMIN The Administrator will ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE.	The Administrative Console is deployed on a secure LAN and requires a dedicated host for execution. This secure network does not have direct links to untrusted LANs. The Sensor, running on the SecureNet™ CC7345 hardware platform is connected to the same Secure LAN from one connection and a promiscuous mode interface connects the Sensor to an outside LAN to monitor all traffic on the public network. The secure LAN is used only for the purpose of handling communications between the Sensor and the Administrative Console, thus communication with the Administrative Console is limited only to the Sensor. The Administrator is responsible for deploying

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
		both the Sensor and the Administrative Console as specified above; any other deployments will negate the results of this evaluation.
A.LOCATE The Administrative Console and the Sensor are located in a physically secure area.	O.E.LOCATE The Administrative Console and the Sensor will be located in a physically secure area.	The Administrative Console and the Sensor must be located in a physically secure area. The site where SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 is installed will have its own procedures to enforce physical security, personnel security, and procedural security. The Administrator is responsible for enforcing these procedures there by enforcing the integrity of the TOE.
T.ATTACK An authorized or unauthorized user may attempt to unobtrusively attack the systems monitored by the TOE.	O.DETECT The Sensor will monitor the environment and detect intrusion attempts to the network or systems on the network by monitoring all data sent across the network. O.SENSOR The Sensor will collect and store information about all events that are indicative of intrusion attempts or inappropriate activity occurring on the network or systems on the network that the Sensor is monitoring. O.RESPON The Sensor will respond to	The Sensor will monitor all data sent across the network through a promiscuous mode interface. The Sensor then collects and stores information that is indicative of intrusions by an authorised or unauthorised user attempting to unobtrusively attack the systems on the network. The Sensor detects these intrusion attempts by decoding and analysing all packets through the use of signature recognition and anomaly detection. Once the packets are analysed and the Sensor has stored the information, the Sensor responds to the event by

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
	detected events by sending alerts of intrusion attempts or inappropriate activity occurring on the network or systems on the network to the Administrative Console. O.ADMIN The Administrative Console will manage the Sensor and its functions.	sending an alert to the Administrative Console either through an optional e-mail notification or through a network management tool. The Administrative Console enables the Administrator to monitor and manage the Sensor remotely, view Sensor monitoring sessions, replay archived sessions and generate reports.
T.E.ATKSIG The Sensor may fail to detect new intrusion scenarios or inappropriate activity on the network.	O.E.ATKSIG The Administrator will ensure that the latest signature packs are downloaded from the Intrusion, Inc. web site for use by the TOE.	The recommended method for downloading updated signature packs (signed with GnuPG) from the Intrusion, Inc. website is to use a third party system, from any computer with access to the Internet. The updated signature packs are then transferred to the Sensor to be incorporated into the TOE. The Administrator is responsible for obtaining these signature packs which are necessary to enforce the continued integrity of the TOE. The procedures for updating the signature packs are detailed in the guidance documentation delivered with the TOE as part of the SecureNet™ CC7345 delivery package. The Administrator must follow these procedures as instructed.
T.E.CONFIG The Sensor or the	O.E.ADMIN The Administrator will	The Administrator is responsible for configuring

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
Administrative Console may be improperly configured by the Administrator causing intrusion attempts to go undetected.	ensure that all hardware and software components that are utilised to support the TOE's purpose will be operated and maintained to enforce the continued integrity of the TOE. O.E.CONFIG Proper configuration of the TOE in compliance with the specified system and connectivity requirements provides a sound operational environment for the TOE.	all software, as specified in the guidance documentation supplied in the SecureNet™ CC7345 delivery package to ensure that the TOE is operated and maintained in a manner that is necessary to enforce the continued integrity of the TOE. Following the guidance documentation supplied in the delivery package will ensure that the TOE will not be improperly configured and that intrusions will not go undetected.
T.E.CONSL An unauthorised user may gain access to the Administrative Console and attempt to compromise the integrity of the Administrative Console through malicious activity.	O.E.PSWRD The Administrator of the TOE will not reveal the root password that grants access to the Sensor host or the Administrative Console host. O.E.LOCATE The Administrative Console and the Sensor will be located in a physically secure area.	The Administrative Console is protected by unauthorised access through physical and logical security parameters. The site where SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 is installed will have its own procedures to enforce physical security, personnel security, and procedural security. The Administrator is responsible for enforcing these procedures there by enforcing the integrity of the TOE. The Administrative Console is protected from unauthorised access by the security features of the Red Hat Linux Operating System host, external to the TOE. Access to the Administrative Console host is protected

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
		through the use of Linux user-level password authentication. Someone wishing to access the Administrative Console must provide valid username/password login credentials in order for the Red Hat Linux Operating System to provide access to the Administrative Console software.
T.E.SENSR An unauthorised user may gain access to the Sensor and attempt to compromise the integrity of the Sensor through malicious activity.	O.E.PSWRD The Administrator of the TOE will not reveal the root password that grants access to the Sensor host or the Administrative Console host. O.E.LOCATE The Administrative Console and the Sensor will be located in a physically secure area.	The Sensor is protected by unauthorised access through physical and logical security parameters. The site where the TOE is installed will have its own procedures to enforce physical security, personnel security, and procedural security. The Administrator is responsible for enforcing these procedures there by enforcing the integrity of the TOE. The Sensor software application is protected from unauthorised access by the security features of the Pilot 2.3 SP2 Operating System, external to the TOE. Pilot 2.3 SP2 provides adequate protection for the Sensor from unauthorised access. Access to the Sensor host is protected through the use of Linux user-level password authentication. Someone

Table Legend		
A = ASSUMPTION, P = POLICY, T = THREAT, O = OBJECTIVE, .E = ENVIRONMENT		
ASSUMPTION, THREAT OR POLICY	**Security Objectives**	**RATIONALE**
		wishing to access the Sensor must provide valid username/password login credentials in order for the Pilot 2.3 SP2 Operating System to provide access to the Sensor software.

CHAPTER 5

5. IT Security Requirements

This section contains the security requirements that are provided by the TOE and the IT environment. These requirements consist of security functional and assurance components for the TOE derived from Part 2 and 3 of the CC with the exception of four explicitly stated requirements and one NIAP interpretation.

5.1 Security Functional Requirements

Table 2 lists the functional requirements and the security objectives each requirement enforces. All functional and assurance dependencies associated with the components in Table 2 have been satisfied.

Table 2 - Functional Components

CC Component Name	Hierarchical To	Dependencies	Objectives Enforced / Rationale
FAU_SAA.3 Simple Attack Heuristics	FAU_SAA.1	None	O.DETECT is partially enforced by FAU_SAA.3, Simple Attack Heuristics, through the intrusion detection security function of the TOE. The Sensor maintains an internal representation of known signature events and compares those signatures to all data that the Sensor has collected from the network. The Sensor collects the data through activity decoding, IP address monitoring, network session monitoring and protocol analysis. Through signature recognition of known attack scenarios, the Sensor is able to indicate an imminent violation of the TSP when an event is found that matches a signature that indicates a potential violation of the TSP.
FAU_SAR.1 Audit Review	No Other Components	FAU_GEN.1 [Satisfied by FXP_IDS_COL .1 and FXP_IDS_GEN .1]	O.SENSOR is partially enforced by FAU_SAR.1, Audit Review, through the intrusion response functionality of the TOE. The Sensor stores information it collects about all events that are indicative of intrusion attempts or inappropriate activity occurring on the network. When the Sensor decodes network activity, it writes the resulting

CC Component Name	Hierarchical To	Dependencies	Objectives Enforced / Rationale
			events to a flat file on disk for storage. O.RESPON is partially enforced by FAU_SAR.1, Audit Review, through the intrusion response functionality of the TOE. The Sensor responds to the intrusion attempts or inappropriate activity by sending an alert to the Administrative Console indicating that an intrusion attempt has occurred and that the event is available for review. Through the Administrative Console, the Administrator is able to view the data collected from the Sensor which includes event priority, source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC.
FAU_SAR.3 Selectable Audit Review	No Other Components	FAU_SAR.1	O.ADMIN is partially enforced by FAU_SAR.3, Selectable Audit Review, through the intrusion response functionality of the TOE. The Administrative Console has the ability to perform searches and sorting of the intrusion attempts collected by the Sensor based on the date and time of the attempted intrusion, subject identity, type of event, success or failure of related events, event priority, source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC.
FAU_SEL.1 Selective Audit	No Other Components	FAU_GEN.1 [Satisfied by FXP_IDS_COL .1 and FXP_IDS_GEN .1] FMT_MTD.1	O.ADMIN is partially enforced by FAU_SEL.1, Selective Audit, through the intrusion response functionality of the TOE. The Administrative Console has the ability include or exclude auditable intrusion attempts from the set of audited intrusion attempts based the object's identity or source IP address, source and destination port, Ethernet MAC, destination IP address, or source and destination MAC.

CC Component Name	Hierarchical To	Dependencies	Objectives Enforced / Rationale
FMT_MOF.1 Management of Security Functions Behaviour	No Other Components	FMT_SMR.1	O.ADMIN is partially enforced by FMT_MOF.1, Management of Security Functions Behaviour, through the intrusion response functionality of the TOE. Sensor functionality is controlled and managed through the Administrative Console.The Administrative Console enforces appropriate management and control over event collection, analysis, and reporting functions of the Sensor.
FMT_MTD.1 Management of TSF Data	No Other Components	FMT_SMR.1	O.ADMIN is partially enforced by FMT_MTD.1, Management of TSF Data, through the intrusion response functionality of the TOE. Sensor functionality is controlled and managed through the Administrative Console. The Administrative Console enforces effective management functions over events collected from the Sensor.
FPT_ITT.1 Basic Internal TSF Data Transfer Protection	No Other Components	None	O.RESPON is partially enforced by FPT_ITT.1, Basic Internal TSF Data Transfer Protection, through the intrusion response functionality of the TOE. The TOE responds to detected events by message integrity and authentication to ensure secure communications between Sensor and Administrative Console.
FXP_IDS_ALM.1 Sensor Alarm	No Other Components	None	O.RESPON is partially enforced by FXP_IDS_ALM.1, Sensor Alarm, through the intrusion response functionality of the TOE. Intrusion response is supported by alerts sent to the Administrative Console when the Sensor detects an intrusion.
FXP_IDS_ANL.1 Sensor Data Analysis	No Other Components	None	O.DETECT and O.SENSOR are partially enforced by FXP_IDS_ANL.1, Sensor Data Analysis, through the intrusion detection security function of the TOE. The Sensor unobtrusively monitors and then collects data that is sent across the network that is indicative of an

CC Component Name	Hierarchical To	Dependencies	Objectives Enforced / Rationale
			intrusion attempt or inappropriate activity. Then, the data is analysed through network monitoring, protocol analysis, and signature recognition.
FXP_IDS_COL.1 Sensor Data Collection	No Other Components	None	O.DETECT and O.SENSOR are partially enforced by FXP_IDS_COL.1, Sensor Data Collection, through the intrusion detection security function of the TOE. The Sensor unobtrusively monitors and then collects data that is sent across the network that is indicative of an intrusion attempt or inappropriate activity. This is achieved through activity decoding, IP address monitoring, network session monitoring, protocol analysis, and signature recognition.
FXP_IDS_GEN.1 Sensor Data Generation	No Other Components	FPT_STM.1	O.RESPON is partially enforced by FXP_IDS_GEN.1, Sensor Data Generation, through the intrusion response functionality of the TOE. This is enforced by the Administrative Console through automated log rotation, archiving capabilities, and report generation of data collected by the Sensor.

Table 3 lists the functional requirements and discusses how the functional requirements work together to enforce the security objectives of the TOE.

Table 3 - Functional Components to Objectives Mapping

Security Functional Requirement	Objective	Rationale
FAU_SAR.3 FAU_SEL.1 FMT_MOF.1 FMT_MTD.1	O.ADMIN	These functions of the TOE work together to enforce O.ADMIN. The Administrative Console manages the Sensor and its functions. This includes the management of Sensor configuration parameters and the selection and review of event data.

Security Functional Requirement	Objective	Rationale
FAU_SAA.3 FXP_IDS_ANL.1 FXP_IDS_COL.1	O.DETECT	These functions of the TOE work together to enforce O.DETECT. The Sensor monitors the environment and detects intrusion attempts to the network or systems on the network by monitoring all data sent across the network. This objective is enforced through the collection and analysis functions performed by the Sensor. The event data collected and analysed by the Sensor is compared against known attack signatures that are indicative of intrusion attempts and inappropriate activity.
FAU_SAR.1 FPT_ITT.1 FXP_IDS_ALM.1	O.RESPON	These functions of the TOE work together to enforce O.RESPON. The Sensor responds to detected events by sending alerts of intrusion attempts or inappropriate activity occurring on the network or systems on the network to the Administrative Console. This objective is enforced through the Sensor functions that alert the Administrator when an intrusion attempt or inappropriate activity has occurred on the network. The Sensor sends an alert to the Administrative Console. Through the Administrative Console, the Administrator is able to view the data collected from the Sensor, which includes event priority, source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC. This information is protected from modification when it is transferred from the Sensor to the Administrative Console.
FAU_SAR.1 FXP_IDS_ANL.1 FXP_IDS_COL.1	O.SENSOR	These functions of the TOE work together to enforce O.SENSOR. The Sensor collects and stores information about all events that are indicative of intrusion attempts or inappropriate activity occurring on the network or systems on the network that the Sensor monitors. This objective is enforced through the collection and analysis functions performed by the Sensor and the review function of the Administrative Console. The Sensor collects and analyses event data indicative of an intrusion attempt or inappropriate activity occurring on the network. The Sensor writes the event to a flat file on disk for storage. The Administrator can review this information through the Administrative Console.

The functional requirements that appear in Table 2 and 3 are described in more detail in the following subsections. These requirements are derived verbatim from either Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.1* or from the requirements modified by National Interpretations with the exception four explicitly stated requirements. Items that are italicised and listed in brackets are either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_SAA.3 Simple Attack Heuristics

Hierarchical to: FAU_SAA.1 Potential Violation Analysis.

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events [assignment: *invalid or illegal parameters, overload of network traffic, MSTREAM DoS Communication Flooding Signature, portscan attacks, Server Message Block based attacks, Secure Shell attacks, Domain Naming System spoofing, Finger intrusions, FTP server based attacks, HTTP attacks, Internet Relay Chat based attacks, attacks on Usenet newsgroups through a Network News Transfer Protocol server, POP3 and SMTP mail server attacks, RPC PortMapper Resetting, Telnet attacks, and Trivial File Transfer Protocol attacks*] that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: *data collected by the Sensor*].

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Dependencies: No dependencies.

Rationale: SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 uses both signature recognition and protocol analysis intrusion detection methods. Signature recognition is a method where incoming/outgoing traffic is compared against well-known "signatures." SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 uses the SNP-L Scripting System, which is an attack detection language that allows decoding and analysis of various types of network transmissions without regard for host packet capture mechanisms, IP fragment reconstruction, and TCP session reassembly. SNP-L uses

language syntax similar to the C programming language. A list of known signatures is frequently updated by Intrusion, Inc. and is publicly available. Signatures may also be added using the network grep system, a text pattern matching system for finding key words or phrases. Protocol analysis allows differentiation of incoming packets so that only those of interest are subjected to further inspection.

5.1.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [assignment: *the Administrator*] with the capability to read [assignment: *data collected from the Sensor which includes event priority, source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC*] from the audit records.

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

Dependencies: FAU_GEN.1 Audit Data Generation.

Rationale: When the Sensor decodes network activity, it writes the resulting events to a flat file on disk for storage. Event data is organised into a tree hierarchy based on event priority and date, and the Administrative Console receives summary data from the Sensor. This event tree is managed through the Administrative Console, where detail information about events is also available. Only the Administrator can monitor and manage the information as the event tree, and may also access detail information when necessary.

5.1.1.3 FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: *searches and sorting*] of audit data based on [assignment: *date and time, subject identity, type of event, success or failure of related events, event priority, source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC*].

Dependencies: FAU_SAR.1 Audit Review.

Rationale: Within the Administrative Console, event data is stored on disk in a hierarchical event database, where it is available for reports. The Administrative Console includes a full featured report generation engine (SNPreport) that allows the creation of

detailed reports of events that the Sensors have recorded, including information about which Sensor generated each displayed alert. The filtering feature of the report generator is accessed through the X Windows application (which is executed by the SNPc executable, which then spawns the SNPreport executable that is responsible for the generation of reports). Reports include information such as time, date, source IP address and source and destination port. Reports can be sorted, grouped, filtered, and formatted according to a variety of criteria.

Events can be filtered by a variety of values, including Ethernet MAC, destination IP address, and source and destination MAC. Events with duplicate event messages can be grouped together in generated reports, allowing reducing the overall size of the reports. Events can be sorted in ascending or descending order by a variety of criteria, including Ethernet MAC, destination IP address, source and destination MAC, event message, and event date.

5.1.1.4 FAU_SEL.1 Selective Audit

Hierarchical to: No other components.

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) [selection: *object identity*].

b) [assignment: *source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC*].

Dependencies: FAU_GEN.1 Audit Data Generation,

FMT_MTD.1 Management of TSF Data.

Rationale: The Administrative Console supports real time retrieval and archiving of event messages from remote Sensors, automated grouping and correlation of received events, and the generation of activity reports. When the Sensor decodes network activity, it writes the resulting events to a flat file on disk for storage. Event data is organised into a tree hierarchy based on event priority and date, and the Administrative Console receives summary data from the Sensor. This event tree is managed through the Administrative Console, where detail information about events is also available. Through the global filtering tool, the Administrator can filter network activity stored in the event tree based on specified parameters, i.e., source IP address, source and destination port, Ethernet

MAC, destination IP address, and source and destination MAC. Only the Administrator can monitor and manage the information found in the event tree.

5.1.2 Security Management (FMT)

5.1.2.1 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour o*f] the functions [assignment: *event collection, analysis, and reporting functions of the Sensor*] to [assignment: *the authorised Administrator*].

Dependencies: FMT_SMR.1 Security Roles, levied on the environment

Rationale: The administrative role is the only role specified that has access to security functions of the Sensor. Sensor functionality is controlled by the Administrator through the Administrative Console. The Administrative Console is an X-Windows application that enables the Administrator to perform all aspects of Sensor management graphically. From the Administrative Console, the functionality of the Engine List provides the Administrator with ways to administer new Sensors and control existing Sensors: configuration parameters can be edited on existing Sensors, new Sensors can be configured or existing Sensors can be deleted.

When an Administrator performs any administrative task, a connection circuit is established from the Administrative Console's host to the specified Sensor. The Administrative Console then performs the following functions:

A) Collects data from one or more Sensors

B) Manage Sensors

C) Monitors network sessions

D) Generates reports of network activity

5.1.2.2 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear* [assignment: *no other operations*]] the [assignment: *network events collected from the Sensor including: invalid or illegal parameters, overload of network traffic, MSTREAM DoS Communication Flooding Signature, portscan attacks, Server Message Block based attacks, Secure Shell attacks, Domain Naming System spoofing,*

Finger intrusions, FTP server based attacks, HTTP attacks, Internet Relay Chat based attacks, attacks on Usenet newsgroups through a Network News Transfer Protocol server, POP3 and SMTP mail server attacks, RPC PortMapper Resetting, Telnet attacks, and Trivial File Transfer Protocol attacks] to [assignment: *the authorised Administrator*].

Dependencies: FMT_SMR.1 Security Roles, levied on the environment.

Rationale: Through the Administrative Console, the Administrator is able to perform functions of Sensor management. The Administrative Console is an X-Windows application that acts as a graphical user interface (GUI) for collecting data from one or more Sensors, monitoring network sessions, generating reports of network activity, and other tasks necessary for the management of SecureNet Pro™ Intrusion Detection System Version 4.1 SP1.

5.1.3 Protection of the TSF (FPT)

5.1.3.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

Hierarchical to: No other components.

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: *modification*] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies.

Rationale: The Sensor and Administrative Console communicate using TCP/IP. SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 uses message integrity verification to reduce the possibility that communications between the Sensor and Administrative Console are compromised. For the Sensor to be managed from the Administrative Console, the specific Administrative Console that is to be trusted must be configured. A Sensor only allows specific, trusted Administrative Consoles to have access to it. If the Administrative Console is unable to connect to the Sensor, for any reason, the Administrative Console will continue to make requests for connection until communication is established. The Administrative Console will send an alert when a connection with the Sensor is severed. Since sensitive information travels between these components, measures are taken to prevent any compromises from occurring. These measures are outlined below:

A) Secure Deployment:

The Sensor and Administrative Console are designed to communicate over a private, secured IP network. This network is not directly accessible by an attacker; it is immune from direct network attacks.

B) Shared-secret Encryption:

All transmissions between the Sensor and Administrative Console are encrypted with shared secret keys using the DES, Triple DES, and Blowfish algorithms. This prevents information from being leaked to an individual using "sniffer" attacks to monitor communications.

C) Message Authentication:

All transmissions between the Sensor and the Administrative Console are authenticated using the MD5 algorithm to prevent an attacker from modifying messages while they are in-route.

D) Address Authentication:

When the Administrative Console connects to the Sensor host, IP address authentication is used to ensure that the Administrative Console is a trusted host. This prevents untrusted network hosts from attempting to access the Sensor.

5.1.4 Explicitly Stated Requirements (IDS)

5.1.4.1 FXP_IDS_ALM.1 Sensor Alarm

Hierarchical to: No other components.

FXP_IDS_ALM.1.1 The Sensor shall send an alarm to [assignment: the *Administrative Console*] and [assignment: *alert the Administrator*] when an intrusion is detected.

Dependencies: No dependencies.

Justification: This explicitly stated requirement has been included in the ST to address alerts when an intrusion is detected. Currently, Part 2 of the CC does not address specific functionality that would sufficiently express IDS functionality.

Rationale: Once the Sensor decodes and analyzes the network traffic and an intrusion attempt has been identified, an alert is sent to the Administrative Console either through an optional e-mail notification or through a network management tool.

5.1.4.2 FXP_IDS_ANL.1 Sensor Data Analysis

Hierarchical to: No other components.

FXP_IDS_ANL.1.1 The Sensor shall perform [selection: *signature and/or protocol*] analysis functions on all IDS data received.

Dependencies: No dependencies.

Justification: This explicitly stated requirement has been included in the ST to address data analysis on all events the Sensor collects. Currently, Part 2 of the CC does not address specific functionality that would sufficiently express IDS functionality.

Rationale: SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 uses both signature recognition and protocol analysis intrusion detection methods. Signature recognition compares incoming/outgoing traffic against well-known signatures. Intrusion, Inc. frequently updates a list of known signatures. These signature updates are downloaded from the Intrusion, Inc. website and signed with GnuPG. The file is downloaded through an Internet connection to any computer on the network. Then the file is loaded directly on the Sensor, and the updates are applied to the outdated file. Custom signatures are added to the list by using the SNP-L scripting language. SNP-L is a custom attack detection scripting language designed for traffic decoding and analysis of various types of network transmissions. Signatures may also be added using the network grep system, a text pattern matching system for finding key words or phrases. Protocol analysis allows differentiation of incoming packets so that only those of interest are subjected to further inspection.

5.1.4.3 FXP_IDS_COL.1 Sensor Data Collection

Hierarchical to: No other components.

FXP_IDS_COL.1.1 The Sensor shall collect [selection: *type of events, date and time of events, identification of events, network traffic*] from the targeted IT system resource(s).

Dependencies: No dependencies.

Justification: This explicitly stated requirement has been included in the ST to address the methods taken by the Sensor to collect data relative to all network traffic. Currently, Part 2 of the CC does not address specific functionality that would sufficiently express IDS functionality.

Rationale: Through a network interface running in promiscuous mode , SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 captures all packets that travel through the network and decodes real-time session activity (active TCP connections).

For the Sensor to engage in its network monitoring and activity-decoding tasks, the Administrator must configure the IP addresses to be watched. A Sensor only performs state-based intrusion detection on monitored IPs. Non-specified IPs are still monitored using non state-based intrusion detection techniques. For the Sensor automatically to discover IP addresses that are to be monitored, the Administrator must configure the IP address ranges that are considered to be internal networks. If activity originating from or destined to an address within these ranges is seen, the Sensor detects IP addresses. The Sensor stores these IP ranges to be monitored in a file that contains the IP parameter range.

When the Sensor decodes network activity, it writes the resulting events to a disk database flat file for storage. Event data is organised into a tree hierarchy based on event priority and date, and the Administrative Console receives summary data from the Sensor. The Administrator can monitor and manage this information as the Event Tree, and may also access detail information when necessary.

Any active TCP connection being decoded by the Sensor can be viewed in real time as well as managed through the Administrative Console's GUI interface. Additionally, any TCP connection that is logged in binary format by the Sensor can be replayed using the logged connection-viewing interface.

5.1.4.4 FXP_IDS_GEN.1 Sensor Data Generation

Hierarchical to: No other components.

FXP_IDS_GEN.1.1 The Sensor shall be able to generate an audit record of [assignment: *network events collected and analysed by the Sensor*]

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

a) Date and time of the event, type of event, subject identity

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC*].

Dependencies: FPT_STM.1 Reliable Time Stamps.

Justification: This explicitly stated requirement has been included in the ST to address audit records of data collected by the Sensor. Currently, Part 2 of the CC only addresses audit functions on *user* data, not data that is collected by the TOE.

Rationale: The Administrative Console is an X Windows executable that operates in a multi-threaded fashion, which gathers data from remote Sensors, archives that data to disk, and allows GUI interactions. The Administrative Console supports automated log rotation and archiving capabilities as well. When events are received from the Sensor, they are written to the local event database on the disk of the Administrative Console host. Event data is organized into a tree hierarchy based on date of occurrence and event priority level. The event tree displays event data received from remote Sensors in a graphical tree format. The output from the event tree displays which Sensor generated each displayed alert, event priority, source and destination port, source IP address, destination IP address, date, time, and event message.

Both the Sensor and the Administrative Console keep track of all event data stored in their respective disk databases, archiving and deleting old data when necessary, based on either age or file size.

Additionally, any active TCP connection being decoded by the Sensor is viewed in real time using the Active Connection Viewing Interface. This interface acts as a graphical terminal for displaying monitored connection data. It enables the Administrator to view the contents of TCP connections and/or log the sessions for future viewing. When logging is used, all data for a particular TCP connection circuit is recorded on the Sensor host, either in binary or text formats.

The Administrative Console includes a full-featured report generation engine (SNPreport) that allows creation of detailed reports of events the Sensors have recorded, including information about which Sensor generated each displayed alert. Because of the filtering feature of the report generator, reports can include information such as time, date, source IP address, source and destination port, and so on.

The Administrator configures the reports using the Administrative Console, then spawns an instance of the Report Generation Engine (SNPreport). Any report that has been created by the Report Generation Engine can be viewed. The Administrative Console spawns an external web browser process (the Administrator must have specified

the full path to the browser executable in the Administrative Console General Configuration dialog box). According to choice, the browser may display the report(s) for viewing on the CRT monitor screen ("standard I/O") of the Administrative Console host. The browser may also output the report(s) to a printer, either one attached directly to the Administrative Console host through the printer port or over the network to a shared network printer.

5.2 Security Functional Requirements for the IT Environment

Table 4 lists the functional requirements levied on the IT environment and the security objectives that each requirement helps to address. All functional and assurance dependencies associated with the components in Table 4 have been satisfied.

Table 4 - Security Functional Requirements for the IT Environment

CC Component Name	Hierarchical To	Dependencies	Objectives Enforced / Rationale
FAU_STG.1-NIAP-0423 Protected Audit Trail Storage	No Other Components	FAU_GEN.1 [Satisfied by FXP_IDS_COL.1 and FXP_IDS_GEN.1]	O.E. AUDPRO is enforced by FAU_STG.1-NIAP-0423, Protected Audit Trail Storage. Audit records of network activity generated by the TOE are protected by the Operating System, external to the TOE thus, a function of the IT environment.
FIA_UAU.1 Timing of Authentication	No Other Components	FIA_UID.1	O.E.I&A is partially enforced by FIA_UAU.1, Timing of Authentication. Before the Administrative Console can perform any functions on the Sensor, the Administrator must first be logged into the Operating System of the host as root user.
FIA_UID.1 Timing of Identification	No Other Components	None	O.E.I&A is partially enforced by FIA_UID.1, Timing of Identification. Before the Administrative Console can perform any functions on the Sensor, the Administrator must first be logged into the Operating System of the host as the root user.

FMT_SMR.1 Security Roles	No Other Components	FIA_UID.1	O.E. ROLES is enforced by FMT_SMR.1, Security Roles. In order to perform any functions on the TOE, the Administrator must first log onto the Operating System of the host using the root password, external to the TOE.
FPT_STM.1 Reliable Time Stamps	No Other Components	None	O.E. TIME is enforced by FPT_STM.1. Time is read from the underlying Operating System, which makes this a function enforced by the environment.

Table 5 lists the functional requirements levied on the IT environment and how they work to meet the security objectives levied on the IT environment thus providing support for the TOE and its functions.

Table 5 - SFRs for the IT Environment to Objectives for the IT Environment Mapping

Security Functional Requirement	Objective	Rationale
FAU_STG.1-NIAP-0423	O.E. AUDPRO	This function of the IT environment fully enforces O.E. AUDPRO. The Operating System is responsible for protecting the audit trail of network activities generated by the TOE.
FIA_UAU.1 FIA_UID.1	O.E.I&A	These functions of the IT environment work together to enforce O.E.I&A. The Operating System is responsible enforcing identification and authentication.
FMT_SMR.1	O.E. ROLES	This function of the IT environment fully enforces O.E. ROLES. The administrative role is the only role specified that has access to security functions of the Sensor and the Administrative Console. Sensor functionality is controlled by the Administrator through the Administrative Console. Access to the Administrative Console is granted by logging into the Operating System as the root user using the root password. This password is protected through the use of Linux user-level password authentication. Only the Administrator has knowledge of this password.
FPT_STM.1	O.E. TIME	This function of the IT environment fully enforces O.E. TIME. A time stamp of all event activity occurring on the network is read from the Operating System.

The functional requirements that appear in Table 4 and 5 are described in more detail in the following subsections. These requirements are derived verbatim from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 2.1 and from NIAP interpretations through December 9, 2002. Items that are italicised and listed in brackets are either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces.

All references to the TSF in Section 5.5 refer to the TOE security functions enforced by the environment.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_STG.1-NIAP-0423 Protected Audit Trail Storage

Hierarchical to: No other components.

FAU_STG.1.1-NIAP-0423 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2-NIAP-0423 The TSF shall be able to [selection: *detect*] unauthorised modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit Data Generation. This dependency is satisfied by FXP_IDS_COL.1 and FXP_IDS_GEN.1. These two explicitly stated requirements are provide the audit data used by the TOE.

Rationale: SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 does not have the capability to protect the audit trail of *user activities*. This protection must be provided by the underlying Operating System.

5.2.2 Identification and Authentication (FIA)

5.2.2.1 FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [assignment: *the environment to control what actions may be taken*] on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of Identification.

Rationale: The underlying Operating System must provide authentication for users of the TOE.

5.2.2.2 FIA_UID.1 Timing of Identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [assignment: *the environment to control what actions may be taken*] on behalf of the user to be performed before the user is identified.

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

Dependencies: No dependencies

Rationale: The underlying Operating System must provide identification for users of the TOE.

5.2.3 Security Management (FMT)

5.2.3.1 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *Administrator*].

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

Dependencies: FIA_UID.1 Timing of Identification.

Rationale: The underlying Operating System must provide for the Administrator role for the TOE.

5.2.4 Protection of the TSF (FPT)

5.2.4.1 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

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

Dependencies: No dependencies.

Rationale: Time used in the TOE audit records is obtained from the underlying Operating System.

5.3 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarised in Table 4.

Table 6 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures

Assurance Class	Component ID	Component Title
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.1	Descriptive High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Tests	ATE_COV.1	Evidence of Coverage
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing – Sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

The major functions implemented by the TOE are:

A) INTRUSION DETECTION: The Intrusion Detection function enforced by the TOE enables the TOE to unobtrusively monitor, collect, decode and analyse data that is sent across the network, thus satisfying the O.DETECT and O.SENSOR objectives. The following processes support the Intrusion Detection function of the TOE: activity decoding, IP address monitoring, network session monitoring, protocol analysis, and signature recognition.

B) INTRUSION RESPONSE: The Intrusion Response function enforced by the TOE enables the TOE to respond to detected events, thus satisfying the O.ADMIN and O.RESPON objectives. The following processes support the Intrusion Response function of the TOE: event logging, report generation, TCP reset, trusted communication between Sensor and Administrative Console.

The Intrusion Detection and Intrusion Response functions are further discussed in detail in Tables 7 and 8 below, which will explain how they work to meet the Security Functional Requirements enforced by the TOE.

Table 7 - Functions to Security Functional Requirements Mapping

Functions	Security Functional Requirements	Rationale
INTRUSION DETECTION	FAU_SAA.3 FXP_IDS_ANL.1 FXP_IDS_COL.1	The primary purpose of the TOE is to identify generic and system-specific threats to the system it is intended to protect, and the mitigation of these risks. The TOE collects data sent across a network through a network interface running in promiscuous mode . The use of this network interface is a fundamental requirement of the TOE, it allows all hosts on a physical network segment to be centrally monitored and protected. Through a network interface running in promiscuous mode , the Sensor can monitor packets that travel through the network, regardless of whether they are addressed to the Sensor host. The Sensor then decodes and analyses network traffic in real time, logs event data to disk, and optionally sends alerts by e-

Functions	Security Functional Requirements	Rationale
		mail or through a network management tool. The Sensor interacts with the Administrative Console, with internal communication being encrypted to protect the data. The scripting language SNP-L is an attack detection language that allows decoding of various types of network transmissions without regard for host packet capture mechanisms, IP fragment reconstruction, or TCP session reassembly. Activity decoding modules are stored in the Module Database, organised in a tree hierarchy. The Module Database Tree displays all activity decoding modules that are currently loaded into a particular Sensor. In addition to known signatures that are updated regularly, custom modules may be written, updated, and stored in this database. Viewing, managing, and updating of the Module Database Tree is carried out through the Administrative Console. SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 uses both signature recognition and protocol analysis intrusion detection methods. Signature recognition compares incoming/outgoing traffic against well-known signatures. There is a list of known signatures that is frequently updated. By using the SNP-L scripting language, custom signatures may also be added to the list. Signatures may also be added using the network grep system, a text pattern matching system for finding key words or phrases. Protocol analysis allows differentiation of incoming packets so that only those of interest are subjected to further inspection. For the Sensor to engage in its network monitoring and activity-decoding tasks, the Administrator must configure the IP addresses to be watched. A Sensor only performs state-based intrusion detection on monitored IPs. Monitored IP address configuration, specifies the parameters. Non-specified IPs are still monitored using non state-based intrusion

Functions	Security Functional Requirements	Rationale
		detection techniques. For the Sensor automatically to discover IP addresses that are to be monitored, the Administrator must configure the IP address ranges that are considered to be internal networks. If activity originating from or destined to an address within these ranges is seen, the Sensor detects IP addresses. The Sensor then stores these IP ranges to be monitored.
INTRUSION RESPONSE	FAU_SAR.1 FAU_SAR.3 FAU_SEL.1 FMT_MOF.1 FMT_MTD.1 FPT_ITT.1 FXP_IDS_ALM.1 FXP_IDS_GEN.1	When the Sensor decodes network activity, it writes the resulting events into a tree hierarchy of flat files on disk for storage. Event data is organised based on priority and date. The Administrative Console receives summary data from the Sensor when requested. The Event Tree is managed through the Administrative Console, where detail information about events is available. Any TCP connection being decoded by the Sensor can be viewed in real time using the Active Connection Viewing Interface. The Administrator may watch the contents of active TCP connections, log sessions, and terminate sessions. In addition, any TCP connection that has been logged in binary format by the Sensor can be replayed using the Logged Connection Viewing Interface. The Sensor includes automated log rotation and archiving capabilities for Sensor management. When the Sensor decodes network activity, it writes the resulting events to a disk database for storage. Event data is organised into a tree hierarchy based on event priority and date. Within the Administrative Console, event data is stored on disk in a hierarchical event database, where it is available for reports. The Administrative Console includes a full-featured report generation engine that allows creation of detailed reports of events the Sensors have recorded, including information

Functions	Security Functional Requirements	Rationale
		about which Sensor generated each displayed alert. Reports include information such as time, date, IP address, and source and destination port. The Administrator configures the reports using the Administrative Console, then it spawns an instance of the Report Generation Engine. Any report that has been created by the Report Generation Engine can be viewed. The Administrative Console spawns an external web browser process (the Administrator must have specified the full path to the browser executable in the Administrative Console General Configuration dialog box). According to choice, the browser may display the report(s) for viewing on the CRT monitor screen ("standard I/O") of the Administrative Console host. The browser may also output the report(s) to a printer, either one attached directly to the Administrative Console host through the printer port or over the network to a shared network printer.

Table 8 shows the mapping between the security functional requirements and the functions listed above.

Table 8 - Security Functional Requirements to Functions Mapping

Security Functional Requirement	Functions	Rationale
FAU_SAA.3	INTRUSION DETECTION	FAU_SAA.3, Simple Attack Heuristics, is satisfied by the intrusion detection security function. Intrusion detection is accomplished through activity decoding, IP address monitoring, network session monitoring, protocol analysis, and signature recognition. These processes are discussed in detail below, which work together to meet the FAU_SAA.3 Security Functional Requirement.

Security Functional Requirement	Functions	Rationale
		Activity Decoding This process is enforced through the SNP-L Scripting System, which is a custom scripting language, designed for high-speed traffic decoding and analysis. This scripting language is an attack detection language that allows decoding of various types of network transmissions without regard for host packet capture mechanisms, IP fragment reconstruction, or TCP session reassembly. **IP Address Monitoring** For the Sensor to engage in its network monitoring and activity-decoding tasks, the Administrator must configure the IP addresses to be watched. A Sensor only performs state-based intrusion detection on monitored IPs. Non-specified IPs are still monitored using non state-based intrusion detection techniques. For the Sensor automatically to discover IP addresses that are to be monitored, the Administrator must configure the IP address ranges that are considered to be internal networks. If activity originating from or destined to an address within these ranges is seen, the Sensor detects IP addresses. The Sensor stores these IP ranges to be monitored in a file for reference. **Network Monitoring** Is enforced through a network interface running in promiscuous mode that enables SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 to capture all packets travelling through the network. SecureNet Pro™

Security Functional Requirement	Functions	Rationale
		Intrusion Detection System Version 4.1 SP1 then decodes and analyses the network traffic, and logs the event data to disk. Additionally, any TCP connection being decoded by the Sensor can be viewed in real time using the Active Connection Viewing Interface. The SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Administrator may watch the contents of active TCP connections, log sessions, terminate sessions, etc. In addition, any TCP connection that has been logged in binary format by the Sensor can be replayed using the Logged Connection Viewing Interface. **Protocol Analysis** Protocol analysis allows differentiation of incoming packets so that only those of interest are subjected to further inspection. **Signature Recognition** Signature recognition compares incoming/outgoing traffic against well-known signatures. A list of known signatures is frequently updated by Intrusion, Inc. and available for download from the Intrusion, Inc. web site. Customer signatures can be added to the list using the SNP-L scripting language.
FXP_IDS_ANL.1	INTRUSION DETECTION	FXP_IDS_ANL.1, Sensor Data Analysis, is satisfied by the intrusion detection security function. Sensor data is analysed through network monitoring, protocol analysis, and signature recognition, which are discussed in detail below. These processes work together to meet the

Security Functional Requirement	Functions	Rationale
		FXP_IDS_ANL.1 Security Functional Requirement. **Network Monitoring** Is enforced through a network interface running in promiscuous mode that enables SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 to capture all packets travelling through the network. SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 then decodes and analyses the network traffic, and logs the event data to disk. Additionally, any TCP connection being decoded by the Sensor can be viewed in real time using the Active Connection Viewing Interface. The SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Administrator may watch the contents of active TCP connections, log sessions, terminate sessions, etc. In addition, any TCP connection that has been logged in binary format by the Sensor can be replayed using the Logged Connection Viewing Interface. **Protocol Analysis** Protocol analysis allows differentiation of incoming packets so that only those of interest are subjected to further inspection. **Signature Recognition** Signature recognition compares incoming/outgoing traffic against well-known signatures. A list of known signatures is frequently updated by Intrusion, Inc. and available for download from the Intrusion, Inc. web site. Customer signatures can be added to the list

Security Functional Requirement	Functions	Rationale
		using the SNP-L scripting language.
FXP_IDS_COL.1	INTRUSION DETECTION	FXP_IDS_COL.1, Sensor Data Collection, is satisfied by the intrusion detection security function. Sensor data collection is accomplished through activity decoding, IP address monitoring, network session monitoring, protocol analysis, and signature recognition. These processes, which work together to meet the FXP_IDS_COL.1 Security Functional Requirement are discussed in detail below. **Activity Decoding** This process is enforced through the SNP-L Scripting System, which is a custom scripting language, designed for high-speed traffic decoding and analysis. This scripting language is an attack detection language that allows decoding of various types of network transmissions on a high level without regard for host packet capture mechanisms, IP fragment reconstruction, or TCP session reassembly. **IP Address Monitoring** For the Sensor to engage in its network monitoring and activity-decoding tasks, the Administrator must configure the IP addresses to be watched. A Sensor only performs state-based intrusion detection on monitored IPs. Non-specified IPs are still monitored using non state-based intrusion detection techniques. For the Sensor automatically to discover IP addresses that are to be monitored, the Administrator must configure the IP address ranges

Security Functional Requirement	Functions	Rationale
		that are considered to be internal networks. If activity originating from or destined to an address within these ranges is seen, the Sensor detects IP addresses. The Sensor stores these IP ranges to be monitored in a file for reference. **Network Monitoring** Is enforced through a network interface running in promiscuous mode that enables SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 to capture all packets travelling through the network. SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 then decodes and analyses the network traffic, and logs the event data to disk. Additionally, any TCP connection being decoded by the Sensor can be viewed in real time using the Active Connection Viewing Interface. The SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Administrator may watch the contents of active TCP connections, log sessions, terminate sessions, etc. In addition, any TCP connection that has been logged in binary format by the Sensor can be replayed using the Logged Connection Viewing Interface. **Protocol Analysis** Protocol analysis allows differentiation of incoming packets so that only those of interest are subjected to further inspection. **Signature Recognition** Signature recognition compares incoming/outgoing traffic against well-known signatures. A list of known signatures is frequently

Security Functional Requirement	Functions	Rationale
		updated by Intrusion, Inc. and available for download from the Intrusion, Inc. web site. Customer signatures can be added to the list using the SNP-L scripting language.
FAU_SAR.1	INTRUSION RESPONSE	FAU_SAR.1, Audit Review, is satisfied through the intrusion response functionality of the TOE, which is supported by report generation of data collected from the Sensor and sent to the Administrative Console. The report generation process satisfies the requirements of the FAU_SAR.1 Security Functional Requirement. A discussion of report generation is detailed below. **Reports** Within the Administrative Console, event data is stored on disk in a hierarchical event database, where it is available for reports. The Administrative Console includes a full-featured report generation engine (SNPreport) that allows creation of detailed reports of events the Sensors have recorded, including information about which Sensor generated each displayed alert. The Administrator configures the reports using the Administrative Console, and then it spawns an instance of the Report Generation Engine (SNPreport). Any report that has been created by the Report Generation Engine can be viewed. The Administrative Console spawns an external web browser process (the Administrator must have specified the full path to the browser executable in the Administrative Console General

Security Functional Requirement	Functions	Rationale
		Configuration dialog box). According to choice, the browser may display the report for viewing on the CRT monitor screen (standard I/O) of the Administrative Console host. The browser may also output the report to a printer, either one attached directly to the Administrative Console host through the printer port or over the network to a shared network printer.
FAU_SAR.3	INTRUSION RESPONSE	FAU_SAR.3, Selectable Audit Review, is satisfied by the intrusion response functionality of the TOE, which is supported by report generation of data collected from the Sensor that is sent to the Administrative Console. The report generation process satisfies the requirements of the FAU_SAR.3 Security Functional Requirement. A discussion of report generation is detailed below. **Reports** The Administrative Console includes a report generation engine that allows the creation of detailed reports of events the Sensor has recorded. These reports include information such as date, time, event priority, source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC. The information collected from the Sensor can be sorted, grouped, filtered, and formatted according to criteria specified by the Administrator. Events can be sorted in ascending or descending order according to Ethernet MAC, IP address, source and destination MAC, event message, or event

Security Functional Requirement	Functions	Rationale
		date. Events with duplicate event messages can be grouped together in generated reports. Events can be filtered by values such as Ethernet MAC, IP address, or source and destination MAC.
FAU_SEL.1	INTRUSION RESPONSE	FAU_SEL.1, Selective Audit, is satisfied by the intrusion response functionality of the TOE, which is enforced through event logging, data archiving, and report generation of data collected from the Sensor and then sent to the Administrative Console. These processes work together to meet the FAU_SEL.1 Security Functional Requirement and are discussed in detail below. **Event Logging** Intrusion response is supported by the event logging functionality, by writing the resulting network activity events to a flat file on disk for storage. Event data is organised into a tree hierarchy based on event priority and date. Through the global filtering tool, the Administrator can filter network activity stored in the event tree based on specified parameters, i.e., source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC. **Data Archiving** SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 includes automated log rotation and archiving capabilities. When the Sensor decodes network activity, it writes the resulting events to a disk database for storage. The Sensor and the Administrative Console keep track

Security Functional Requirement	Functions	Rationale
		of all event data stored in its database, archiving and deleting old data when necessary. **Reports** The Administrative Console includes a report generation engine that allows the creation of detailed reports of events the Sensor(s) have recorded. These reports include information such as date, time, event priority, source IP address, source and destination port, Ethernet MAC, destination IP address, and source and destination MAC.
FMT_MOF.1	INTRUSION RESPONSE	FMT_MOF.1, Management of Security Functions Behaviour, is satisfied by the intrusion response function of the TOE. The intrusion response function enforces appropriate management over event collection, analysis, and reporting functions of the Sensor. These processes work together to meet the FMT_MOF.1 Security Functional Requirement. All Sensor functionality is controlled by the Administrator through the Administrative Console. The Administrative Console is an X-Windows application that enables the Administrator to perform all aspects of Sensor management graphically. From the Administrative Console, the functionality of the Engine List provides the Administrator with ways to administer new Sensors and control the functions of existing Sensors: configuration parameters are edited on existing Sensors, new Sensors are configured or existing Sensors are

Security Functional Requirement	Functions	Rationale
		deleted.
FMT_MTD.1	INTRUSION RESPONSE	FMT_MTD.1, Management of TSF Data, is satisfied by the intrusion response function of the TOE. The intrusion response function enforces effective management functions over data collected from the Sensor and sent to the Administrative Console. The discussion below details how this process works to meet the FMT_MTD.1 Security Functional Requirement. Through the Administrative Console, the Administrator is able to perform all functions of Sensor management graphically. The Administrative Console is an X-Windows application that acts as a graphical user interface for collecting data from one or more Sensors, monitoring network sessions, generating reports of network activity, and other tasks necessary for the management of SecureNet Pro™ Intrusion Detection System Version 4.1 SP1. When an Administrator performs any administrative task, a connection circuit is established from the Administrative Console's host to the specified Sensor. Once this connection circuit is established, the Administrator can manage all data collected from the Sensor through the Administrative Console.
FPT_ITT.1	INTRUSION RESPONSE	FPT_ITT.1, Basic Internal TSF Data Transfer Protection is satisfied by the intrusion response function of the TOE. This SFR is supported by message integrity and authentication to ensure secure communications between Sensor

Security Functional Requirement	Functions	Rationale
		and Administrative Console. Message integrity and authentication used by the TOE are discussed in detail below to show how these processes work to meet the FPT_ITT.1 Security Functional Requirement. **Message Integrity** SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 uses message integrity verification to reduce the possibility that communications between the Sensor and Administrative Console are compromised. For the Sensor to be managed from the Administrative Console, the specific Administrative Consoles that are to be trusted must be configured. A Sensor only allows specific, trusted Administrative Consoles to have access to it. This configuration cannot be specified at the graphical interface; the file *consoles.cfg* on the Sensor must be edited directly. **Authentication** Internal communications between Sensor and Administrative Console are subject to both message integrity and authentication with name, address, and password. The Sensor is assured of a trusted Administrative Console, and the Administrative Console is certain with which Sensor it is communicating. The names, IP addresses, and passwords are contained in the *consoles.cfg* and *engines.cfg* files, which are configured at initialisation.
FXP_IDS_ALM.1	INTRUSION RESPONSE	FXP_IDS_ALM.1, Sensor Alarm, is satisfied through the intrusion

Security Functional Requirement	Functions	Rationale
		response functionality supported by alerts sent to the Administrative Console when an intrusion is detected. The Sensor records information regarding intrusion attempts then sends alerts to the Administrative Console with a time stamp on each entry.
FXP_IDS_GEN.1	INTRUSION RESPONSE	FXP_IDS_GEN.1, Sensor Data Generation, is satisfied through the intrusion response functionality supported by automated log rotation, archiving capabilities, and report generation of data collected by the Sensor. These processes are discussed below showing how they work together to meet the FXP_IDS_GEN.1 explicitly stated Security Functional Requirement. **Data Archiving** SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 includes automated log rotation and archiving capabilities. When the Sensor decodes network activity, it writes the resulting events to a disk database for storage. The Sensor and the Administrative Console keep track of all event data stored in its database, archiving and deleting old data when necessary. **Reports** The Administrative Console includes a report generation engine that allows the creation of detailed reports of events the Sensor has recorded. These reports include information such as date, time, event priority, source IP address, source and destination port,

Security Functional Requirement	Functions	Rationale
		Ethernet MAC, destination IP address, and source and destination MAC.

6.2 Assurance Measures

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in Chapter 5, Table 6. Table 9 provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 9 - Assurance Measures

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.2	Change Controls, February 2002 SecureNet CC™ Security Functions Reference v3, September 2001	Change Controls is an excel spreadsheet that details the revisions made to SNP configuration items through out its life cycle. SFR v3, Section 3, discusses configuration management of SNP.
ADO_DEL.1	SecureNet CC™ Security Functions Reference v3, September 2001 SecureNet CC™ 5.0 User Guide, February 2002	SFR v3, Section 4.1, discusses delivery procedures for SNP. Further information regarding delivery procedures are detailed in Chapter 2 of the User Guide
ADO_IGS.1	SecureNet CC™ Security Functions Reference v3, September 2001 SecureNet CC™ 5.0 User Guide, February 2002	SFR v3, Section 4.2, discusses IGS procedures for SNP. Further information for IGS procedures are detailed in Chapters 3 through 9 of the User Guide.
ADV_FSP.1	SecureNet CC™ Security Functions Reference v3, September 2001	SFR v3, Section 5.1 details the functional specification of SNP.
ADV_HLD.1	SecureNet CC™ Security Functions Reference v3, September 2001	SFR v3, Section 5.2, details the high level design of SNP.
ADV_RCR.1	SecureNet CC™ Security Functions Reference v3, September 2001	SFR v3, Section 5.3, demonstrates the

Assurance Component	Documentation Satisfying Component	Rationale
		correspondence mappings between the FSP and the HLD *and* between the TSS and the FSP.
AGD_ADM.1	SecureNet CC™ 5.0 User Guide, February 2002	As the Administrator is the only role specified for the TOE, the User Guide details all necessary information relative to the Administrator and Administrative functions.
AGD_USR.1	SecureNet CC™ 5.0 User Guide, February 2002	As SNP is transparent to the *end* user, the Administrator is the only user of the TOE thus, the User Guide is intended for the Administrator of SNP.
ATE_COV.1	SecureNet CC™ Testing and Vulnerability Analysis Reference v3.2, September 2001	Evidence of coverage is detailed in TVR v3.2, Section 3.1.
ATE_FUN.1	SecureNet CC™ Testing and Vulnerability Analysis Reference v3.2, September 2001	The results of functional testing performed by Intrusion, Inc. are detailed in TVR v3.2, Section 3.2.
ATE_IND.2	SecureNet CC™ Testing and Vulnerability Analysis Reference v3.2, September 2001	Evaluator to conduct sampling.
AVA_SOF.1	N/A	Strength of TOE Security Function *not* claimed
AVA_VLA.1	SecureNet CC™ Testing and Vulnerability Analysis Reference v3.2, September 2001	Vulnerability analysis results, conducted by Intrusion, Inc., are detailed in Section 4 of TVR v3.2.

6.2.1 Rationale for TOE Assurance Requirements

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

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 8

8. Rationale

8.1 Security Objectives Rationale

The rationale for the security objectives of the TOE is defined in Chapter 4, Section 4.4 Security Objectives Rationale.

8.2 Security Requirements Rationale

The rationale for the security requirements of the TOE is defined in two sections. Rationale for the security functional requirements is given after each functional component description in Chapter 5, Section 5.1 Security Functional Requirements and 5.2 Security Functional Requirements for the IT environment. Rationale for the security assurance requirements is given in Chapter 6, Section 6.2.1 Rationale for the TOE Assurance Requirements.

8.3 TOE Summary Specification Rationale

The rationale for the TOE Summary Specification is defined in Chapter 6, Section 6.1 TOE Security Functions.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.