Juniper Networks IDP 4.0 & NSM 2006.1

Security Target

VERSION 1.0 FINAL

October 31, 2006

Developed for:

1194 North Mathilda Avenue
Sunnyvale, California 94089-1206
Phone: 888-JUNIPER (888-586-4737)
408-745-2000
Fax: 408-745-2100

Prepared by:

8310 N. Capital of Texas Highway, Ste 275
Austin, TX 78731
Office: (512) 310-2228
(877) 321-RISK
Fax: (512) 439-7446

[This page is intentionally left blank.]

Table of Contents

List of Figures

List of Tables

1.0 ST Introduction

1.1 ST Identification

Title:	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target
Version:	1.0
Status:	FINAL
Release Date:	November 1, 2006
Prepared By:	EnPointe Technologies, Inc. (Richard Thomas & Matt Harlan)
TOE Software Identification:	Netscreen Security Manager (NSM) 2006.1 which consists of NSM Server and NSM User Interface
TOE Hardware Identification:	The following IDP appliances constitute the TOE: • IDP 50, • IDP 200, • IDP 600C, • IDP 600F • IDP 1100C, and • IDP 1100F
Assurance Level:	EAL2
Common Criteria:	Common Criteria for Information Technology Security Evaluation (CC), Version 2.2, January 2004 (aligned with ISO/IEC 15408). Common Methodology for Information Technology Security Evaluation (CEM), Version 2.2, January 2004 (aligned with ISO/IEC 18045).
Interpretations:	Final National and International interpretations included within this ST that that have been released on or before the kick-off date (November 22, 2005) are identified within section 9.3 of this ST.
Keywords:	Intrusion Detection System (IDS), Intrusion Detection & Prevention system (IDP), IDP Sensor™, the IDP Management Server™, IDP User Interface™

1.2 CC Conformance

This TOE's conformance to CC is stated in accordance with section 5.4 of CC part 1. The TOE is:

CC Version 2.2, Part 1 - CONFORMANT

CC Version 2.2, Part 2 - EXTENDED

CC Version 2.2, Part 3 – CONFORMANT

EAL2 – CONFORMANT

Intrusion Detection System System Protection Profile, version 1.5 – CONFORMANT

1.3 Document Conventions

Application Notes:	An application note is additional informative and non-normative text that assists the intended audience to better understand the intent of the TOE and its security features. Application notes are identified as a footnote to the corresponding item requiring further clarification with a number in the upper-right position (e.g. FAU_GEN.1[1]). The accompanying text of the application note is then displayed at the bottom of the page containing the corresponding item.
Assignment:	An assignment allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
Interpretation:	An interpretation is a clarification or further definition to a security functional or assurance requirement that has been reviewed and approved by CCIMB or the associated Common Criteria scheme representative as being acceptable to incorporate into a complying ST. CCIMB and NIAP interpretations are identified by labeling the affected security requirement as they are mentioned in the guidance found at the following internet address: http://cio.nist.gov/esd/emaildir/lists/cc-cmt/msg00019.html
Iteration:	An iteration allows for the use of a component more than once with varying operations. Iterations are indicated with a lowercase alphabetic character (e.g. FAU_GEN.1a).
Refinement:	A refinement allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Refinements resulting from an interpretation are additionally indicated with a red font.
Selection:	A selection allows the specification of one or more elements from a list. Selections are indicated by underlining the text and are surrounded by brackets (e.g., [selection]).

1.4 ST Overview

This Security Target (ST) defines the security environment, security requirements, security functions, and assurance measures of IDP 4.0 & NSM 2006.1.

IDP 4.0 provides intrusion detection and prevention capabilities for a network, given the deployment mode chosen. In the Passive Sniffer Mode, the IDP 4.0 appliance provides detection capabilities by passively monitoring traffic on the network. In the Active Gateway Mode, the IDP 4.0 appliance is deployed inline as a gateway on a network requiring all traffic to pass through the IDP 4.0 appliance before reaching the external network and therefore providing the capabilities to detect and prevent intrusions on a network. The determination for network traffic to be considered an intrusion and the preventive actions to be taken on an identified intrusion is dependant upon the configuration of the security policy installed on the IDP 4.0 appliance.

NSM 2006.1 provides a management interface for administrating IDP 4.0 appliances. From within NSM 2006.1, policies and attack objects can be managed and uploaded to the IDP 4.0 appliances. In addition, NSM 2006.1 provides the required functionality for reviewing system data collected by the IDP 4.0 appliances, as well as, the audit data collected by NSM 2006.1 with regards to administrator actions performed.

The following sections provided within this ST are stated in accordance with and exceed the content requirements for a Security Target as specified in Annex C.2 of CC Part 1:

ST Introduction:	The ST introduction provides a unique identification and overview of this ST.
TOE Description:	The TOE description provides an overview of the TOE and describes the physical and logical boundaries of the TOE.
TOE Security Environment:	The security environment describes the assumptions, threats, and organizational security policies that pertain to both the TOE and TOE environment.
Security Objectives:	The security objectives describe the objectives necessary to counter the defined threats and satisfy the assumptions and organizational security policies.
IT Security Requirements:	The IT security requirements provide a set of security functional requirements to be met by the TOE and the TOE environment. The IT security requirements also provide a set of security assurance requirements that are to be satisfied by the TOE.
TOE Summary Specification:	The TOE Summary Specification describes the security functions of the TOE.
PP Claims:	The PP claims identify any PPs that the TOE claims compliance to.
Rationale:	The rationale provides mappings along with rationale for the security environment, security objectives, security requirements, and security functions to assess their completeness, consistency, and suitability.
Annex A:	Annex A lists the acronyms, terms, interpretations, and references used within this ST.

2.0 TOE Description

2.1 Overview of the TOE

The Juniper Networks Intrusion Detection and Prevention system (IDP) version 4.0 is an intrusion detection and prevention device capable of using up to five (5) different detection methods to accurately detect suspicious network traffic (e.g., traffic designed to probe your system) and/or malicious network traffic (e.g., traffic designed to harm your system). IDP is also capable of dropping attacks to prevent damage to a network.

The IDP has the ability to operate in-line as an active gateway or as a passive sniffer. When deployed as an active gateway, IDP uses a policy to control what action to take when an attack is detected (e.g., dropping any identified malicious packets). When deployed as a passive sniffer, IDP can only detect and log attacks.

IDP detection and prevention capabilities are rule-based, so rules can be specified within a Security Policy to define when and how packets or connections are dropped.

When you install the Security Policy on your Sensors, the rules tell each Sensor how to behave. Set your Sensors to log, send alarms, and even drop suspicious traffic—IDP drops only what you tell it to drop.

IDP 4.0 consists of a Sensor or group of Sensors which detect, and optionally prevent, attacks on networks connected to the IDP appliance. NSM 2006.1 consists of an NSM Server™ and NSM User Interface™ (NSM UI) which allow an administrator access to the system data collected by the Sensor(s).

This architecture is used to scale the system into three tiers, as well as to separate management functions from system operation. These three tiers are further described below:

- **Sensors**

  Sensors are appliances that see all network traffic and act as enforcement points that implement Security Policies. They can operate in sniffer mode or as an active inline gateway, and are used to detect and (when in active inline mode) prevent malicious traffic and intrusions. A sensor appliance communicates with a server component through the sensor's external IDP Network Management Interface.

- **NSM Server**

  The NSM Server stores and manages all Attack Objects (including attack signature and protocol anomalies), log information, rulebases, and Security Policies. It collects all logged information from the Sensors and aggregates them for inspection using the NSM UI. The server component receives data from the sensor on its external NSM Device Management Interface.

- **NSM UI**

  The NSM UI is a graphical interface for interacting with the IDP appliance. You can use the NSM UI to remotely access and manipulate the information stored on the NSM Server. It provides distributed access to centralized policies to monitor and control the network.

The Sensor monitors the network on which the IDP appliance is installed. The Sensor is a hardware appliance (called the IDP appliance) that runs the Sensor software on a Linux-based kernel. The Sensor's primary task is to detect suspicious and anomalous network traffic based on specific rules defined in IDP rulebases. If the Sensor is running in-line, it can also take a predefined action against malicious traffic.

The NSM Server runs on a Linux or Solaris kernel, and centralizes the logging, reporting, data, and Security Policy management for the IDP appliance. All objects, Security Policies, and log records are stored in the underlying filesystem on the NSM Server and are administered using the NSM UI. The NSM Server communication with the other two tiers of the IDP appliance (the Sensor and NSM UI) is encrypted and authenticated. It provides different types of alerts and messages to enable multiple administrators to be alerted to network anomalies.

The NSM UI is software that provides a powerful, graphical environment for centrally managing IDP. The UI is a Java-based software application that can be installed on multiple computers on your network. Multiple users can connect to a single NSM Server.

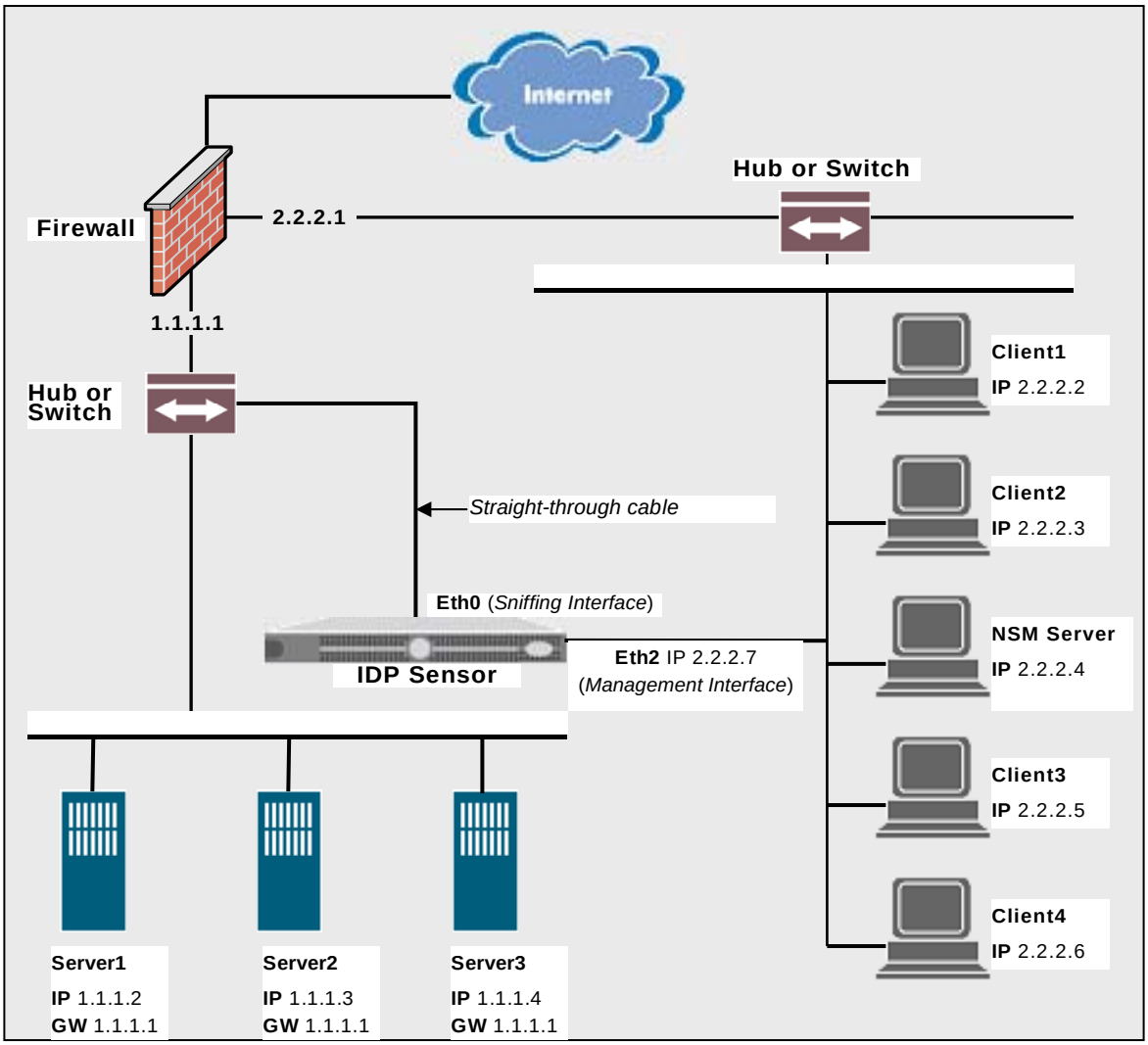
2.1.1 TOE Configurations

The TOE may be configured in either a passive sniffer mode or an active gateway mode. The major difference between these two modes is that the active gateway mode additionally prevents attacks, whereas the passive sniffer mode may only detect attacks. The active gateway mode can be operated in one of four sub-modes which include bridge mode, transparent mode, proxy-ARP mode, and router mode. These various configurations are further described in the following subsections.

2.1.1.1 Passive Sniffer Mode

In the passive sniffer mode configuration, the Sensor connects to the HUB or SPAN port of a switch and sniffs the network traffic as it passes by (you can also use a network TAP). The Sensor monitors network traffic, records security events, and can create alarms for attacks. The passive sniffer mode configuration satisfies all of the security functional requirements as they are identified and described within the Intrusion Detection System System Protection Profile, version 1.5. In particular, note that this mode does not create a single point-of-failure for the system. Figure 1 below provides a diagram that depicts how the IDP is typically deployed in a passive sniffer mode configuration.

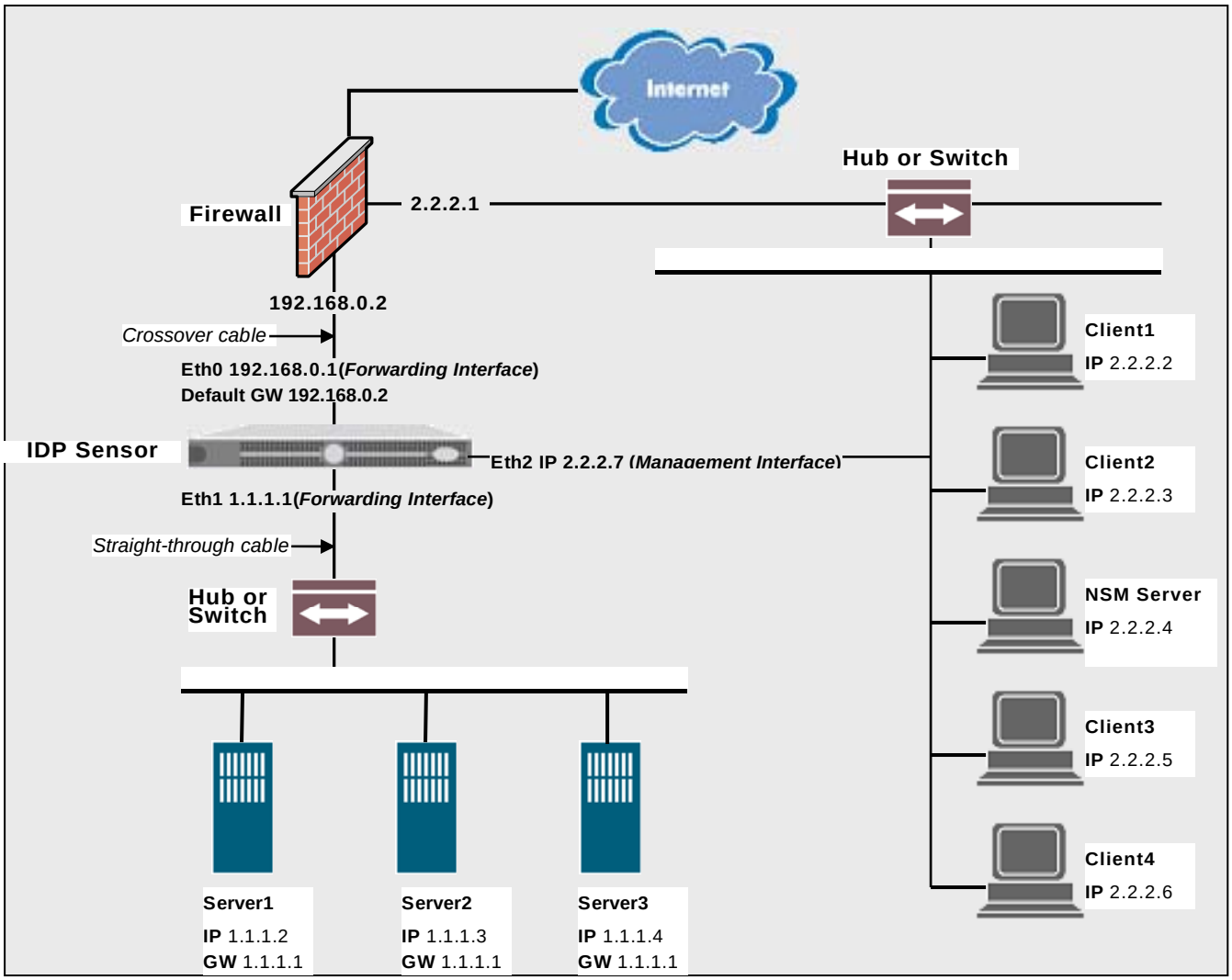
Figure 1: Passive Sniffer Mode Configuration



2.1.1.2 Active Gateway Mode

In the active gateway mode configuration, the Sensor resides inline between the network and the firewall and takes an active role in protecting the network. When the Sensor detects intrusions or attacks defined by Security Policies, the Sensor can drop, block, or ignore the suspicious connection—or drop only the suspicious packets. The active gateway mode configuration satisfies all of the security functional requirements as they are identified and described within the Intrusion Detection System System Protection Profile, version 1.5 and also exceeds these requirements by providing the capability to prevent an attack in addition to detecting the attack. Figure 2 below provides a diagram that depicts how the IDP is typically deployed in an active gateway mode configuration.

Figure 2: Active Gateway Mode Configuration



2.1.1.2.1 Bridge Mode

This mode provides transparent protection without requiring any changes to routing tables or network design. It is called a "transparent" mode because network devices don't know that the sensor exists. Advantages include requiring no changes in IP addressing or routing tables, accommodating Layer 2 broadcasts, support for external load balancing solutions, support for fail-open protection, and being the easiest mode to deploy.

2.1.1.2.2 Transparent Mode

Transparent mode is the same as above, except that it also supports forwarding of all non-IP traffic.

2.1.1.2.3 Proxy-ARP Mode

This mode enables the IDP to respond to and prevent attacks. It automatically learns the network topology and forwards packets to their correct destination. However, the sensor will proxy all ARP requests inbound to the network and therefore is seen by all host machines on the network. Thus, the ARP caches of all host machines must be reconfigured to send all packets needing to be forwarded to the sensor. Its advantages include the ability to prevent attacks without requiring any changes to the network IP addressing scheme.

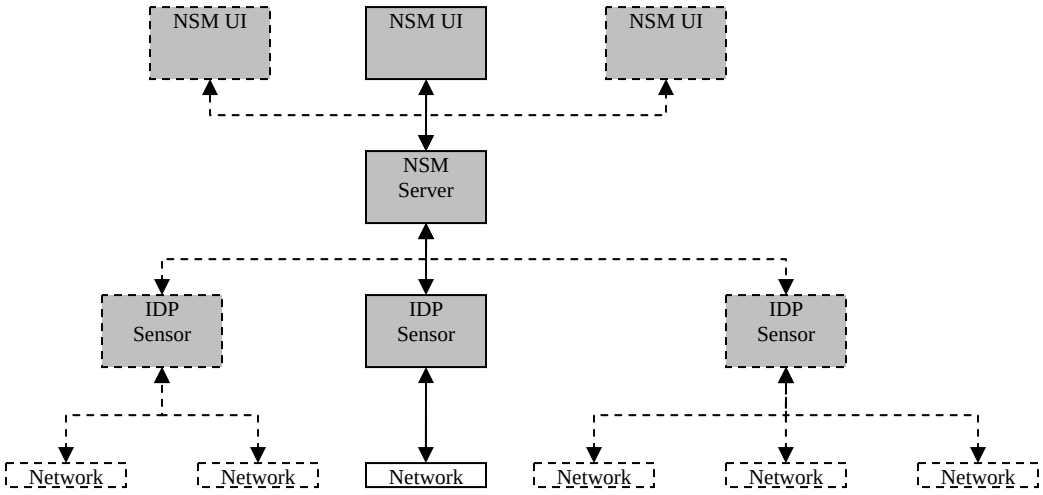
2.1.1.2.4 Router Mode

This mode enables the IDP sensor to act as a router. It contains a routing table to determine where incoming packets need to be sent. This means that all hosts attached to the same subnet as the IDP Sensor should use it as their gateway. This mode is primarily used for compatibility. This mode responds to and prevents attacks, and has the ability to connect to multiple IP networks. Its advantages include the ability to prevent attacks, and connect multiple IP network address spaces.

2.2 Scope and Boundaries of the TOE

2.2.1 Physical Boundaries

The physical boundaries of the TOE include the Sensor, NSM Server, and NSM UI software components that together comprise IDP 4.0 & NSM 2006.1. The underlying operating system for the Sensor is included as part of the TOE. The underlying operating system for the NSM Server is outside the TOE boundaries but provides reliable time stamping capabilities as part of the environment. Additionally, all other hardware and software components that are required to support the correct operation of the TOE are outside of the TOE boundaries.



2.2.2 Logical Boundaries

The logical boundaries of the TOE include the following IT Security features for the Sensor, NSM Server, and NSM UI. These IT security features of IDP 4.0 & NSM 2006.1 enable a user to effectively implement and maintain the IDP appliance.

2.2.2.1 Sensor

The Sensor monitors the network on which the IDP appliance is installed. The Sensor is a hardware appliance (called the IDP appliance) that runs the IDP Sensor software. The Sensor's primary task is to detect suspicious and anomalous network traffic based on specific rules defined in IDP rulebases. If the Sensor is running in-line as an active gateway, it can also take a predefined action against malicious traffic. The Sensor provides both the sensor and analyzer functionalities as defined within the IDSSPP v1.5.

2.2.2.2 NSM Server

The NSM Server is software that manages the system resources of the Sensor and the data it collects. The NSM Server centralizes the logging, reporting, data, and Security Policy management for a set of Sensors. All objects, Security Policies, and log records are stored in the underlying filesystem on the NSM Server and are administered using the NSM UI. NSM Server communication with the other two tiers of the IDP appliance (the Sensor and NSM UI) is encrypted and authenticated. The NSM Server also includes a utility called Profiler that performs scanning capabilities as defined within the IDSSPP v1.5. The Profiler is a network analysis tool that helps you to learn about your internal network, enabling you to create effective Security Policies and minimize unnecessary log records. After you configure the Profiler, it automatically learns about your internal network and the elements that comprise it, including hosts, peers (which host is talking to which other host), ports (non-IP protocols, TCP/UDP ports, RPC programs), and data from layer-7 that uniquely identifies hosts, applications, commands, users, and filenames.

2.2.2.3 NSM User Interface

The NSM User Interface (UI) is software that provides a powerful, graphical environment for centrally managing IDP. The UI is a java-based software application that can be installed on virtually any platform that supports the Java Runtime Environment (JRE) version 1.4.2. Although the UI supports multiple users, only one user at a time can take control of the NSM Server; this eliminates concerns about synchronization or data loss. You can configure the UI with your own preferences—IDP stores user preferences and custom Log Viewer views in the central database so that they remain consistent when you access them from different client machines.

2.3 TOE System Requirements

This section lists the hardware and software required by the TOE to support the correct operation of the TOE.

2.3.1 Hardware Requirements

2.3.1.1 Sensor

IDP requires the use of one or more of the following appliances

- IDP 50, or
- IDP 200, or
- IDP 600C, or
- IDP 600F, or
- IDP 1100C, or
- IDP 1100F

2.3.1.2 NSM Server

NSM Server requires a hardware configuration that meets or exceeds the following:

- CPU: Sun Microsystems UltraSPARC IIi 500MHz (or higher), OR Linux 1GHz (x86) processor (or higher)
- Memeory: 1GB or RAM (or higher); 2GB+ (depending on the number of managed devices and configuration size)
- Swap Space: 4 GB for both GUI Server and Device Server
- Hard Disk: IDE Hard Disk Drive with 10K rpm (minimum); 15K rpm (recommended); 18 GB disk space (minimum); 40 GB disk space (recommended)
- Network Interface: 100MBps NIC Ethernet adapter
- Other: Server must be dedicated to running NetScreen-Security Manager.

2.3.1.3 NSM UI

The NSM UI requires a hardware configuration that meets or exceeds the following:

- IBM® compatible PC
- 400MHz Pentium® II or equivalent (minimum); 700 MHz Pentium II or equivalent (recommended)
- RAM: 256 MB (minimum); 512 MB or above (recommended)
- 384kbps (DSL) or LAN connection - minimum bandwidth required to connect to the NetScreen-Security Manager management system.

2.3.2 Software Requirements

2.3.2.1 Sensor

- Linux Kernel 2.4.31

2.3.2.2 NSM Server

NSM Server requires one of the following operating systems:

- Solaris 8, Solaris 9 operating system
- Red Hat Enterprise Linux ES 3.0 with Update 5 or 4.0 with Update 1
- Red Hat Enterprise Linux AS 3.0 with Update 5 or 4.0 with Update 1

2.3.2.3 NSM UI

The NSM UI requires any operation system platform that supports java and the following java software components:

- Java Runtime Environment (JRE) version 1.4.2
- Microsoft Windows XP, OR Microsoft Windows NT® Workstation/Server 4.0, Service Pack 6a or higher, OR
- Microsoft Windows 2000 Server, Advanced Server, or Professional editions OR
- Red Hat Enterprise Linux ES 3.0 or 4.0, Red Hat Enterprise Linux AS
- US English versions only

3.0 TOE Security Environment

Table 1: TOE Security Environment

Assumptions
A.ACCESS
A.ASCOPE
A.DYNMIC
A.LOCATE
A.MANAGE
A.NOEVIL
A.NOTRST
A.PROTCT
Threats
T.COMDIS
T.COMINT
T.FACCNT
T.FALACT
T.FALASC
T.FALREC
T.IMPCON
T.INADVE
T.INFLUX
T.LOSSOF
T.MISACT
T.MISUSE
T.NOHALT
T.PRIVIL
T.SCNCFG
T.SCNMLC
T.SCNVUL
Organizational Security Policies
P.ACCACT
P.ACCESS
P.ANALYZ
P.DETECT
P.INTGTY
P.MANAGE
P.PROTCT

3.1 Assumptions

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

3.1.1 Intended Usage Assumptions

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

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

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

3.1.2 Personnel Assumptions

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

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

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

3.1.3 Physical Assumptions

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

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

3.2 Threats

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

3.2.1 TOE Threats

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

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

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

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

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

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

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

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

3.2.2 IT System Threats

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

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

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

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

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

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

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

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

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

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

3.3 Organizational Security Policies (OSPs)

The following OSPs are required by the TOE:

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

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

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

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

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

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

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

4.0 Security Objectives

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

Table 2: Security Objectives

Security Objectives for the TOE
O.ACCESS
O.AUDITS
O.EADMIN
O.IDANLZ
O.IDAUTH
O.IDSCAN
O.IDSENS
O.INTEGR
O.OFLOWS
O.PROTCT
O.RESPON
Security Objectives for the IT Environment
OE.AUDIT_PROTECTION
OE.PROTECT
OE.TIME
Security Objectives for the Non-IT Environment
O.CREDEN
O.INSTAL
O.INTROP
O.PERSON
O.PHYCAL

4.1 Security Objectives for the TOE

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

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

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

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

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

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

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

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

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

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

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

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

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

OE.PROTECT The IT environment will protect itself and the TOE from external interference or tampering.

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

4.2.2 Security Objectives for the Non-IT Environment

The TOEs operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

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

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

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

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

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

5.0 IT Security Requirements

This part of the ST defines the detailed IT security requirements that shall be satisfied by the TOE or its environment.

Table 3: IT Security Requirements

TOE Security Functional Requirements	CC Conformance:
FAU_GEN.1 Audit data generation	Drawn from CC Part 2
FAU_SAR.1 Audit review	Drawn from CC Part 2
FAU_SAR.2 Restricted audit review	Drawn from CC Part 2
FAU_SAR.3 Selectable audit review	Drawn from CC Part 2
FAU_SEL.1 Selective audit	Drawn from CC Part 2
FAU_STG.4 Prevention of audit data loss	Drawn from CC Part 2
FIA_ATD.1 User attribute definition	Drawn from CC Part 2
FIA_UAU.1 Timing of authentication	Drawn from CC Part 2
FIA_UID.1 Timing of identification	Drawn from CC Part 2
FMT_MOF.1 Management of security functions behaviour	Drawn from CC Part 2
FMT_MTD.1a Management of TSF data	Drawn from CC Part 2
FMT_MTD.1b Management of TSF data	Drawn from CC Part 2
FMT_SMF.1 Specification of Management Functions	Drawn from CC Part 2
FMT_SMR.1 Security roles	Drawn from CC Part 2
FPT_ITT.1 Basic internal TSF data transfer protection	Drawn from CC Part 2
IDS_SDC.1 System Data Collection (EXP)	Explicitly Stated
IDS_ANL.1 Analyser analysis (EXP)	Explicitly Stated
IDS_RCT.1a Analyser react (EXP)	Explicitly Stated
IDS_RCT.1b Analyser react (EXP)	Explicitly Stated
IDS_RDR.1 Restricted Data Review (EXP)	Explicitly Stated
IDS_STG.1 Guarantee of System Data Availability (EXP)	Explicitly Stated
IDS_STG.2 Prevention of System data loss (EXP)	Explicitly Stated
IT Environment Security Functional Requirements	**CC Conformance:**
FAU_STG.2 Guarantees of audit data availability	Drawn from CC Part 2
FPT_RVM.1 Non-bypassability of the TSP	Drawn from CC Part 2
FPT_SEP.1 TSF domain separation	Drawn from CC Part 2
FPT_STM.1 Reliable time stamps	Drawn from CC Part 2
Security Assurance Requirements for the TOE	**CC Conformance:**
ACM_CAP.2: Configuration items	Drawn from CC Part 3
ADO_DEL.1: Delivery procedures	Drawn from CC Part 3
ADO_IGS.1: Installation generation and start-up procedures	Drawn from CC Part 3
ADV_FSP.1: Informal functional specification	Drawn from CC Part 3
ADV_HLD.1: Descriptive high-level design	Drawn from CC Part 3
ADV_RCR.1: Informal correspondence demonstration	Drawn from CC Part 3
AGD_ADM.1: administrator guidance	Drawn from CC Part 3
AGD_USR.1: User guidance	Drawn from CC Part 3
ATE_COV.1: Evidence of coverage	Drawn from CC Part 3
ATE_FUN.1: Functional testing	Drawn from CC Part 3
ATE_IND.2: Independent testing – sample	Drawn from CC Part 3
AVA_SOF.1: Strength of TOE security function evaluation	Drawn from CC Part 3
AVA_VLA.1: Developer vulnerability analysis	Drawn from CC Part 3

5.1 Security Functional Requirements

5.1.1 TOE Security Functional Requirements for the TOE

5.1.1.1 FAU: Security Audit

5.1.1.1.1 FAU_GEN: Security audit data generation

5.1.1.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1

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

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

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

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

FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**the additional information specified in the Details column of Table 4: Auditable Events**].

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

Table 4: Auditable Events

5.1.1.1.2 FAU_SAR: Security audit review

5.1.1.1.2.1 FAU_SAR.1 Audit review

FAU_SAR.1.1

The TSF shall provide [**the authorized Domain administrators, System administrators, Read-Only System Administrators, and Read-Only Domain Administrators**] with the capability to read [**all auditable events that are recorded**] 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.

5.1.1.1.2.2 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1

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

5.1.1.1.2.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1

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

5.1.1.1.3 FAU_SEL: Security audit event selection

5.1.1.1.3.1 FAU_SEL.1 Selective audit

FAU_SEL.1.1

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

a) [event type];

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

5.1.1.1.4 FAU_STG: Security audit event storage

5.1.1.1.4.1 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1

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

5.1.1.1.5 FIA_ATD: User attribute definition

5.1.1.1.5.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1

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

a) User identity;

b) Authentication data;

c) Authorisations; and

d) [**No additional attributes**]].

5.1.1.1.6 FIA_UAU: User authentication

5.1.1.1.6.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1

The TSF shall allow [**the establishment of a connection**] 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.

5.1.1.1.7 FIA_UID: User identification

5.1.1.1.7.1 FIA_UID.1 Timing of identification

FIA_UID.1.1

The TSF shall allow [**the establishment of a connection**] 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.

5.1.1.2 FMT: Security Management

5.1.1.2.1 FMT_MOF: Management of functions in TSF

5.1.1.2.1.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to [modify the behaviour] of the functions of System data collection, analysis and reaction to [**authorized System Administrators and Domain Administrators**].

5.1.1.2.2 FMT_MTD: Management of TSF data

5.1.1.2.2.1 FMT_MTD.1a Management of TSF data

FMT_MTD.1a.1

The TSF shall restrict the ability to [query] [**and add System and audit data, and shall restrict the ability to query and modify all other TOE data**]] to [**authorized System Administrators**].

5.1.1.2.2.2 FMT_MTD.1b Management of TSF data

FMT_MTD.1b.1

The TSF shall restrict the ability to [query] [**System and audit data, and shall restrict the ability to query all other TOE data**] to [**authorized Read-Only System Administrators, Domain Administrators, and Read-Only Domain Administrators**].

5.1.1.2.3 FMT_SMF: Specification of management functions

5.1.1.2.3.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [

1. **Management of user accounts;**
2. **Management of audit data and audit configurations;**
3. **Management of system data;**
4. **Management of Security Policies**;
5. **Management of authentication lockout].**

5.1.1.2.4 FMT_SMR: Security management roles

5.1.1.2.4.1 FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the **following** roles**: authorised Domain administrators, System administrators, and** [**Read-Only System Administrators, and Read-Only Domain Administrators**].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.1.1.3 FPT: Protection of the TSF

5.1.1.3.1 FPT_ITT: Internal TOE TSF data transfer

5.1.1.3.1.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1

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

5.1.1.4 IDS: IDS Component Requirements

5.1.1.4.1 IDS_SDC: System Data Collection

5.1.1.4.1.1 IDS_SDC.1 System Data Collection (EXP)

IDS_SDC.1.1

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

a) [network traffic, security configuration changes]; and

b) [**No additional events**].

IDS_SDC.1.2

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

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

b) The additional information specified in the *Details* column of Table 5: System Events.

Component	Event	Details
IDS_SDC.1 (Sensor)	Network traffic	Protocol, source address, destination address
IDS_SDC.1 (Sensor)	Security configuration changes	Source address, destination address

Table 5: System Events

5.1.1.4.2 IDS_ANL: Analyser analysis

5.1.1.4.2.1 IDS_ANL.1 Analyser analysis (EXP)

IDS_ANL.1.1

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

a) [signature]; and

b) [**Protocol Anomaly, Backdoor, Traffic Anomaly, Layer 2, and Denial of Service (DoS)**].

IDS_ANL.1.2

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

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

b. [**any actions taken, identification of data destination, protocol, device, severity, category, sub category, packet data, log ID**].

5.1.1.4.3 IDS_RCT: Analyser react

5.1.1.4.3.1 IDS_RCT.1a Analyser react (EXP)

IDS_RCT.1a.1

When deployed in the Passive Sniffer Mode configuration, the System shall send an alarm to [**the administrators defined in the security policy**] and take [**no additional actions**] when an intrusion is detected.

5.1.1.4.3.2 IDS_RCT.1b Analyser react (EXP)

IDS_RCT.1b.1

When deployed in any of the Active Gateway Mode configurations, the System shall send an alarm to [**the administrators defined in the security policy**] and take [**action to drop, block, or ignore the intrusion attempt depending on the actions defined within the security policy**] when an intrusion is detected.

5.1.1.4.4 IDS_RDR: Restricted Data Review

5.1.1.4.4.1 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1

The System shall provide [**authorized Domain administrators, System administrators, Read-Only System Administrators, and Read-Only Domain Administrators**] with the capability to read [**any intrusions detected based on signature, Protocol Anomaly, Backdoor, Traffic Anomaly, Layer 2, and Denial of Service (DoS)**] from the System data.

IDS_RDR.1.2

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

IDS_RDR.1.3

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

5.1.1.4.5 IDS_STG: System Data Storage

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

IDS_STG.1.1

The System shall protect the stored System data from unauthorised deletion.

IDS_ STG.1.2

The System shall protect the stored System data from **unauthorized** modification.

IDS_ STG.1.3

The System shall ensure that [**when the audit storage becomes 80% full, the most recent**] System data **within the area occupying 80% of the audit storage** will be maintained when the following conditions occur: [System data storage exhaustion].

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

IDS_STG.2.1

The System shall [overwrite the oldest stored System data] and send an alarm if the storage capacity has been reached.

5.1.2 IT Environment Security Functional Requirements

5.1.2.1.1 FAU_STG: Security audit event storage

5.1.2.1.1.1 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1

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

FAU_STG.2.2

The TSF shall be able to [detect] unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3

The TSF shall ensure that [**when the audit storage becomes 80% full, the most recent**] audit records **within the area occupying 80% of the audit storage** will be maintained when the following conditions occur: [audit storage exhaustion].

5.1.2.1.2 FPT_RVM: Reference mediation

5.1.2.1.2.1 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1

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

5.1.2.1.3 FPT_SEP: Domain Separation

5.1.2.1.3.1 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1

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

FPT_SEP.1.2

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

5.1.2.1.4 FPT_STM: Time stamps

5.1.2.1.4.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1

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

5.2 Security Assurance Requirements for the TOE

EAL 2 – Structurally tested

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis, and independent testing based upon more detailed TOE specifications.

5.2.1 ACM: Configuration Management

Configuration management (CM) is one method or means for establishing that the functional requirements and specifications are realized in the implementation of the TOE. CM meets these objectives by requiring discipline and control in the processes of refinement and modification of the TOE and the related information. CM systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorized.

5.2.1.1 ACM_CAP.2: Configuration items

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Unique identification of the configuration items leads to a clearer understanding of the composition of the TOE, which in turn helps to determine those items which are subject to the evaluation requirements for the TOE.

Developer action elements:

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

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

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

5.2.2 ADO: Delivery and Operation

Delivery and operation provides requirements for correct delivery, installation, generation, and start-up of the TOE.

5.2.2.1 ADO_DEL.1: Delivery procedures

The requirements for delivery call for system control and distribution facilities and procedures that detail the measures necessary to provide assurance that the security of the TOE is maintained during distribution of the TOE. For a valid distribution of the TOE, the procedures used for the distribution of the TOE address the threats identified in the PP/ST relating to the security of the TOE during delivery.

Developer action elements:

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

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

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

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

5.2.2.2 ADO_IGS.1: Installation generation and start-up procedures

Installation, generation, and start-up procedures are useful for ensuring that the TOE has been installed, generated, and started up in a secure manner as intended by the developer. The requirements for installation, generation and start-up call for a secure transition from the TOE's implementation representation being under configuration control to its initial operation in the user environment.

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

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

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures

result in a secure configuration.

5.2.3 ADV: Development

The development class encompasses four families of requirements for representing the TSF at various levels of abstraction from the functional interface to the implementation representation. The development class also includes a family of requirements for a correspondence mapping between the various TSF representations, ultimately requiring a demonstration of correspondence from the least abstract representation through all intervening representations to the TOE summary specification provided in the ST. In addition, there is a family of requirements for a TSP model, and for correspondence mappings between the TSP, the TSP model, and the functional specification. Finally, there is a family of requirements on the internal structure of the TSF, which covers aspects such as modularity, layering, and minimization of complexity.

5.2.3.1 ADV_FSP.1: Informal functional specification

The functional specification is a high-level description of the user-visible interface and behavior of the TSF. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all the TOE security functional requirements are addressed.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

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

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 ADV_HLD.1: Descriptive high-level design

The high-level design of a TOE provides a description of the TSF in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide. The high-level design requirements are intended to provide assurance that the TOE provides an architecture appropriate to implement the TOE security functional requirements.

The high-level design refines the functional specification into subsystems. For each subsystem of the TSF, the high-level design describes its purpose and function, and identifies the security functions contained in the subsystem. The interrelationships of all subsystems are also defined in the high-level design. These interrelationships will be represented as external interfaces for data flow, control flow, etc., as appropriate.

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

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

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.3 ADV_RCR.1: Informal correspondence demonstration

The correspondence between the various TSF representations (i.e. TOE summary specification, functional specification, high-level design, low-level design, and implementation representation) addresses the correct and complete instantiation of the requirements to the least abstract TSF representation provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

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

5.2.4 AGD: Guidance Documents

The guidance documents class provides the requirements for user and administrator guidance documentation. For the secure administration and use of the TOE it is necessary to describe all relevant aspects for the secure application of the TOE.

5.2.4.1 AGD_ADM.1: administrator guidance

Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. Because the secure operation of the TOE is dependent upon the correct performance of the TSF, persons responsible for performing these functions are trusted by the TSF. Administrator guidance is intended to help administrators understand the security functions provided by the TOE, including both those functions that require the administrator to perform security-critical actions and those functions that provide security-critical information.

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the

security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

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

5.2.4.2 AGD_USR.1: User guidance

User guidance refers to material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE's external interfaces. User guidance describes the security functions provided by the TSF and provides instructions and guidelines, including warnings, for its secure use.

The user guidance provides a basis for assumptions about the use of the TOE and a measure of confidence that non-malicious users, application providers and others exercising the external interfaces of the TOE will understand the secure operation of the TOE and will use it as intended.

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

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

5.2.5 ATE: Tests

The class "Tests" encompasses four families: coverage (ATE_COV), independent testing (e.g. functional testing performed by evaluators) (ATE_IND), and functional tests (ATE_FUN). Testing helps to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified. Testing may also be directed toward the internal structure of the TSF, such as the testing of subsystems and modules against their specifications.

The aspects of coverage and depth have been separated from functional tests for reasons of increased flexibility in applying the components of the families. However, the requirements in these three families are intended to be applied together.

The independent testing family has dependencies on the other families to provide the necessary information to support the requirements, but is primarily concerned with independent evaluator actions.

The emphasis in this class is on confirmation that the TSF operates according to its specification. This will include both positive testing based on functional requirements, and negative testing to check that undesirable behavior is absent. This class does not address penetration testing, which is directed toward finding vulnerabilities that enable a user to violate the security policy. Penetration testing is based upon an analysis of the TOE that specifically seeks to identify vulnerabilities in the design and implementation of the TSF, and is addressed separately as an aspect of vulnerability assessment in the class AVA.

5.2.5.1 ATE_COV.1: Evidence of coverage

In this component, the objective is to establish that the TSF has been tested against its functional specification. This is to be achieved through an examination of developer evidence of correspondence.

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

5.2.5.2 ATE_FUN.1: Functional testing

Functional testing performed by the developer establishes that the TSF exhibits the properties necessary to satisfy the functional requirements of its PP/ST. Such functional testing provides assurance that the TSF satisfies at least the security functional requirements, although it cannot establish that the TSF does no more than what was specified. The family "Functional tests" is focused on the type and amount of documentation or support tools required, and what is to be demonstrated through developer testing. Functional testing is not limited to positive confirmation that the required security functions are provided, but may also include negative testing to check for the absence of particular undesired behavior (often based on the inversion of functional requirements).

The objective is for the developer to demonstrate that all security functions perform as specified. The developer is required to perform testing and to provide test documentation.

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

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

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

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

5.2.5.3 ATE_IND.2: Independent testing – sample

The objective is to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests.

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.6 AVA: Vulnerability Assessment

The class addresses the existence of exploitable covert channels, the possibility of misuse or incorrect configuration of the TOE, the possibility to defeat probabilistic or permutational mechanisms, and the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.

5.2.6.1 AVA_SOF.1: Strength of TOE security function evaluation

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

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

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.2.6.2 AVA_VLA.1: Developer vulnerability analysis

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorized access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorized capabilities of other users.

A vulnerability analysis is performed by the developer to ascertain the presence of obvious security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the TOE.

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

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

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.3 Strength of Function Claim

5.3.1 Minimum Strength of Function Claim

This ST claims a minimum strength of function level of SOF-Basic for the TOE security functional requirements.

5.3.2 Explicit Strength of Function Claims

The TOE claims an explicit strength of function level of SOF-basic for the security functional requirement FIA_UAU.1.

6.0 TOE Summary Specification

6.1 TOE Security Functions

This statement of TOE security functions describes the IT security functions in terms of how these functions satisfy the TOE security functional requirements. Each TOE security function statement identifies the security functional requirements that are satisfied by that TOE security function. Each security function, as a minimum, contributes to the satisfaction of at least one TOE security functional requirement.

The following table lists the security functions that are identified for this TOE.

Table 6: TOE Security Functions

TOE SECURITY FUNCTIONS
Auditing
Identification & Authentication
Security Management
Self Protection
Intrusion Detection & Prevention

6.1.1 Auditing

The Auditing security function is implemented within the Sensor, NSM Server, and NSM UI components of the IDP 4.0 & NSM 2006.1. The Sensor provides the capability to generate audit data and provide a temporary storage of the audit data generated until the audit data is successfully transferred to the NSM Server. The NSM Server provides the capability to generate audit events as well as the capability to store audit event generated by both the Sensor and the NSM Server as well. In addition, the NSM Server provides a means for only authorized users to be allowed to view the audit data stored in an interpretable manner. The NSM UI provides a means for the authorized Read-Only Administrator and the authorized Read/Write Administrator to select data to be audited, as well as, the capability to sort the audit data that may be viewed through the NSM UI.

FAU_GEN.1 Audit data generation

The Auditing security function provides the capability to generate an audit trail based on the following auditable events:

1. Start-up and shutdown of audit functions
2. Access to System
3. Access to the TOE and System data
4. Reading of information from the audit records
5. Unsuccessful attempts to read information from the audit records
6. All modifications to the audit configuration that occur while the audit collection functions are operating
7. All use of the authentication mechanism
8. All use of the user identification mechanism
9. All modifications in the behavior of the functions of the TSF
10. All modifications to the values of TSF data
11. Modifications to the group of users that are part of a role

The Auditing security function also includes in the audit record for each auditable event, the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

FAU_SAR.1 Audit review

The Auditing security function provides the authorized Read-Only Administrator and the authorized Read/Write Administrator with the capability to view the auditable events recorded. The Auditing security function also displays the auditable events in a manner that is interpretable by both the authorized Read-Only Administrator and the authorized Read/Write Administrator.

FAU_SAR.2 Restricted audit review

The Auditing security function prohibits read-access to the audit trail for all users except for the authorized Read-Only Administrator and the authorized Read/Write Administrator by restricting access to the NSM Server to only those authorized administrators identified.

FAU_SAR.3 Selectable audit review

The Auditing security function provides the ability to sort audit data based on the date, time, subject identity, type of event, and success or failure of each related event. This capability is provided by the NSM UI of the IDP.

FAU_SEL.1 Selective audit

The Auditing security function provides the capability to select the audit events that are allowed to be recorded based on the type of event. Event types include attack, config, and traffic. The event types are referred to as event categories within the IDP guidance documentation.

FAU_STG.2 Guarantees of audit data availability

The Auditing security function prevents unauthorized deletion of audit records by requiring users to be successfully authenticated before allowing access to the NSM Server. The Auditing security function also detects modifications to the audit records by generating an MD5 checksum for each archived audit record file. The NSM UI then provides a utility for verifying the checksum of the archived audit record files. The Auditing security function additionally ensures that when the audit storage becomes exhausted, that only the oldest audit record files are purged to ensure adequate disk space for the more recent auditable events.

FAU_STG.4 Prevention of audit data loss

The Auditing security function ensures that when the NSM Server storage space reaches a minimum of 512 MB of existing free space, that the oldest stored audit record files are purged and the existing free space is overwritten with new audit data. The NSM Server verifies the amount of existing free space every 300 seconds. In addition, a security alarm is sent to an administrator to provide a notification that the storage space has reached a minimum of 512 MB of existing free space so that the administrator may take the appropriate actions to ensure adequate storage space for future audit records. The values of existing free space, how often to verify existing free space, and the administrator(s) assigned to receive the alerts about existing free space are configurable through the global preferences. However, the default configuration of IDP 4.0 & NSM 2006.1 specifies for logs to be purged after reaching 512 MB of existing free space, for existing free space to be checked every 300 seconds, and has no administrator assigned to receive alerts.

6.1.2 Identification & Authentication

The Identification & Authentication security function is implemented only within the NSM Server component of the IDP 4.0 & NSM 2006.1. In general, the Identification & Authentication security function provides a means for users to be identified and authenticated in a secure manner.

FIA_ATD.1 User attribute definition

The Identification & Authentication security function provides the capability to manage the user attributes for the authorized Read-Only Administrator and the authorized Read/Write Administrator roles. The security attributes managed by the TOE include users' identity; authentication data; and authorizations. The capability to manage such user attributes is granted only to the authorized Read/Write Administrator role. The authorized Read-Only Administrator role is only provided the capability to view the user attributes, with the exception of the authentication data. The user attributes defined for these roles are stored on the NSM Server and are managed through the NSM UI.

FIA_UAU.1 Timing of authentication & FIA_UID.1 Timing of identification

The Identification & Authentication security function provides the capability to identify and authenticate the authorized Read-Only Administrator and the authorized Read/Write Administrator roles. The Identification & Authentication security function restricts the actions that may be performed prior to user identification and authentication by allowing only the ability to establish a connection to the NSM Server.

6.1.3 Security Management

The Security Management security function is implemented only within the NSM Server component of the IDP 4.0 & NSM 2006.1. The NSM UI also supports the Security Management security function by providing an interface to invoke the defined Security Management security function capabilities, with the exception for maintaining the role authorized System administrator. The authorized System administrator role is managed from the NSM Server by establishing an HTTPS connection to the Sensor and invoking the Appliance Configuration Manager (ACM), which allows for authentication data of the admin and root accounts on the Sensor to be modified.

FMT_MOF.1 Management of security functions behaviour

The Security Management security function provides the capability to restrict the ability to modify the behavior of the functions of System data collection, analysis and reaction to authorised System administrators and Domain administrators. Users associated with the authorised System administrator and Domain administrator roles have the ability to modify the security policies that determine how System data is analyzed, displayed, and reacted to. Users with the authorized Read-Only System administrator and Read-Only Domain administrator roles only have the ability to view the security policies that affect how the System data is analyzed, displayed, and reacted to.

FMT_MTD.1a Management of TSF data

The Security Management security function provides the capability to restrict the ability to query and add System and audit data and to restrict the ability to query and modify all other TOE data to the authorized System Administrator role. The authorized Domain Administrator, Read-Only System Administrator and Read-Only Domain Administrator roles only provide the capability to query System, audit, and TOE data, yet are restricted from modifying such data.

FMT_MTD.1b Management of TSF data

The Security Management security function provides the capability to restrict the ability to query System and audit data and to restrict the ability to query all other TOE data to the authorized Domain Administrator, Read-Only System Administrator and Read-Only Domain Administrator roles.

FMT_SMF.1 Specification of Management Functions

The Security Management security function provides the capability to manage user accounts, audit data, audit configurations, and security policies. The management capabilities are provided by the NSM Server yet is accessed through the NSM UI with the exception for the management of the authorised System administrator role. The authentication data of the authorised System administrator role may only be managed from the ACM.

FMT_SMR.1 Security roles

The Security Management security function provides the capability to maintain roles for authorised System administrators, authorised Domain administrators, authorised Read-Only System administrators, and authorised Read-Only Domain administrators. The authorised System administrator, authorised Domain administrator, authorised Read-Only System administrator, and authorised Read-Only Domain administrator roles are maintained using the NSM UI component of the IDP 4.0 & NSM 2006.1.

In general, the authorized System administrator role provides the capability to view and modify the Sensor and NSM Server configurations and audit records. The authorised Domain administrator, authorized Read-Only Domain administrator and authorized Read-Only System administrator roles provide the capability only to view

the Sensor and NSM Server configurations and audit records. The authorised System administrator role provides the capability to view and modify the configurations of the underlying operating system of the NSM Server. The authorised System administrator role is comprised of the root account that is established on the underlying operating system of the NSM Server.

6.1.4 Self Protection

FPT_ITT.1 Basic internal TSF data transfer protection

The Self Protection security function provides a communication path between the IDP Sensor and NSM Server components of the TOE that protects TSF data from disclosure during transmission. This is established when the IDP Sensor and NSM Server are initially installed. When the IDP Sensor is installed and has been configured with an IP address to the management interface which can be reached by the NSM Server, the NSM Server communicates o the IDP Sensor by initially establishing an SSH connection to the IDP Sensor. Within this SSH session, the NSM Server creates an OTP for the IDP Sensor.

The IDP Sensor then communicates with the NSM Server using this OTP established to exchange certificates. Once the secure connection is established between the IDP Sensor and NSM Server, all further communication is transmitted using the secure channel by encrypting the data using the certificates that were exchanged. The IDP Sensor will not allow for the transmission of any System data until this secure channel has been established.

FPT_RVM.1 Non-bypassability of the TSP

The Self Protection security function ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. This is accomplished by verifying that the set of permitted activities defined within the role(s) associated with the user allows the requested operation to be performed prior to allowing the operation to be performed.

FPT_SEP.1 TSF domain separation

The Self Protection security function provides the Sensor a security domain for its own execution that protects it from interference and tampering of any untrusted subjects by requiring no additional user process to exist on the underlying system in which the sensor resides and by providing separate interfaces for the sensing and management of the sensor.

The Self Protection security function provides the NSM Server a security domain for its own execution that protects it from interference and tampering of any untrusted subjects by requiring no additional user process to exist on the underlying system in which the NSM Server resides.

The Self Protection security function provides the NSM UI a security domain for its own execution that protects it from interference and tampering of any untrusted subjects by executing the NSM UI in a sandbox using Java technology.

FPT_STM.1 Reliable time stamps

The Self Protection security function provides the Sensor a reliable timestamp for each audit record using the Linux Kernel installed on the Sensor. The Self Protection security function provides the NSM Server a reliable timestamp for each audit record using a system call to the underlying operating system in which the NSM Server resides on.

6.1.5 Intrusion Detection & Prevention

IDS_SDC.1 System Data Collection (EXP)

The Intrusion Detection & Prevention security function provides the Sensor the sensing capabilities to collect service requests, network traffic, and security configuration changes. The Intrusion Detection & Prevention security function provides the NSM Server the scanning capabilities to collect detected malicious code, service configuration, detected known vulnerabilities using the Profiler. For each event in which data is collected, both the Sensor and NSM Server associate the Date and time of the event, type of event, source identity, the outcome (success or failure) of the event, any alarms generated, attack type, any actions taken, identification of data destination, protocol, sensor device address, sensor device VIN, sensor inbound interface, sensor outbound interface, severity, category, sub category, packet data, log ID.

IDS_ANL.1 Analyser analysis (EXP)

The Intrusion Detection & Prevention security function provides the Sensor analyzing capabilities using signature, Protocol Anomaly, Backdoor, Traffic Anomaly, IP Spoofing, Layer 2, and Denial of Service (DoS) analyzing methods on all IDS data collected by the sensor.

IDS_RCT.1a Analyser react (EXP)

The Intrusion Detection & Prevention security function, when in the Passive Sniffer Mode configuration, provides the Sensor the capability to alarm an administrator in the event that an intrusion has been detected if the intrusion matches an intrusion in the defined security policy and is tagged to send an alarm.

IDS_RCT.1b Analyser react (EXP)

The Intrusion Detection & Prevention security function, when in any of the Active Gateway Mode configurations, provides the Sensor the capability to alarm an administrator in the event that an intrusion has been detected if the intrusion matches an intrusion in the defined security policy and is tagged to send an alarm. However, the Intrusion Detection & Prevention security function also provides the ability to drop, block, or ignore an intrusion attempt depending on the actions defined within the security policy.

IDS_RDR.1 Restricted Data Review (EXP)

The Intrusion Detection & Prevention security function provides the NSM Server the ability to restrict capability to read audit logs, security policies, profiler data, and user account information from the System data to only the authorized Read/Write Administrators and authorized Read-Only Administrators. The NSM UI also assists by displaying the audit logs, security policies, profiler data, and user account information in a manner suitable for the authorized Read/Write Administrators and authorized Read-Only Administrators to interpret the information.

IDS_STG.1 Guarantee of System Data Availability (EXP) & IDS_STG.2 Prevention of System data loss (EXP)

The Intrusion Detection & Prevention security function provides the Sensor and NSM Server with the capability to protect the stored System data from unauthorized modification or deletion by requiring users to be successfully authenticated before allowing any access to system data.

The Intrusion Detection & Prevention security function also protects the System data by ensuring that the most recently generated System data is made available when the storage repository containing the System data reaches an %80 level of capacity. At such point, the oldest stored System data will be deleted and the available space occupied by the deleted System data is then made available for new system data to be recorded and stored. An administrator defined within the global preferences is also notified with an alarm notifying the administrator that the storage repository containing the System data has reached an %80 level of capacity.

6.2 Assurance Measures

Table 7: TOE Assurance Measures

TOE ASSURANCE MEASURES \ TOE ASSURANCE REQUIREMENTS	ACM_CAP.2: Configuration items	ADO_DEL.1: Delivery procedures	ADO_IGS.1: Installation generation and start-up procedures	ADV_FSP.1: Informal functional specification	ADV_HLD.1: Descriptive high-level design	ADV_RCR.1: Informal correspondence demonstration	AGD_ADM.1: administrator guidance	AGD_USR.1: User guidance	ATE_COV.1: Evidence of coverage	ATE_FUN.1: Functional testing	ATE_IND.2: Independent testing – sample	AVA_SOF.1: Strength of TOE security function evaluation	AVA_VLA.1: Developer vulnerability analysis
Concepts & Examples Guide: NetScreen-IDP Fundamentals							X	X					
Hardware Guide: NetScreen-IDP 10 (650)			X				X	X					
Hardware Guide: NetScreen-IDP 100 & 500 (1650)			X				X	X					
Hardware Guide: NetScreen-IDP 100, 500, & 1000			X				X	X					
Juniper Networks IDP 4.0 & NSM 2006.1 Configuration Management System	X												
Juniper Networks IDP 4.0 & NSM 2006.1 Delivery Procedures		X											
Juniper Networks IDP 4.0 & NSM 2006.1 Functional Specification & Correspondence Analysis				X		X							
Juniper Networks IDP 4.0 & NSM 2006.1 High-Level Design					X								
Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	X	X	X	X	X	X	X	X	X	X	X	X	X
Juniper Networks IDP 4.0 & NSM 2006.1 Testing Documentation									X	X	X		
Juniper Networks IDP 4.0 & NSM 2006.1 Vulnerability and Strength of Function Analysis												X	X
High Availability QuickStart Guide: NetScreen-IDP 3.0			X					X					
QuickStart Guide: NetScreen-IDP 3.0			X					X					
RAID Mirroring: IDP 100, 500 (1650)			X					X					
Upgrade Guide: NetScreen-IDP 3.0			X					X					

6.2.1 Configuration Management

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

- Juniper Networks IDP 4.0 & NSM 2006.1 Configuration Management System
- Juniper Networks IDP 4.0 & NSM 2006.1 Security Target

These documents satisfy the following assurance requirement:

- ACM_CAP.2: Configuration items

6.2.2 Delivery

Juniper Networks provides delivery documentation that identifies the procedures necessary for delivering the TOE to the end-user in a secure manner that assures the end-user in receiving the TOE in the state in which it had passed evaluation.

This documentation provides descriptions of the delivery procedures, measures to ensure delivery assurance (including TOE identification, TOE integrity, TOE availability, and TOE confidentiality), and the delivery process (including packaging, storage, and shipping). These activities are documented in:

- Juniper Networks IDP 4.0 & NSM 2006.1 Delivery Procedures
- Juniper Networks IDP 4.0 & NSM 2006.1 Security Target

These documents satisfy the following assurance requirement:

- ACM_CAP.2: Configuration itemsADO_DEL.1: Delivery procedures

6.2.3 Installation Generation and Start-up Procedures

Juniper Networks provides guidance in the installation and initialization procedures. The installation and generation procedures describe the steps necessary to install the TOE in accordance with the evaluated configuration. These activities are documented in:

- Hardware Guide: NetScreen-IDP 10 (650)
- Hardware Guide: NetScreen-IDP 100 & 500 (1650)
- Hardware Guide: NetScreen-IDP 100, 500, & 1000
- Juniper Networks IDP 4.0 & NSM 2006.1 Security Target
- High Availability QuickStart Guide: NetScreen-IDP 3.0
- QuickStart Guide: NetScreen-IDP 3.0
- RAID Mirroring: IDP 100, 500 (1650)
- Upgrade Guide: NetScreen-IDP 3.0

These documents satisfy the following assurance requirement

- ADO_IGS.1: Installation generation and start-up procedures

6.2.4 Development

Juniper Networks provides descriptions of the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST). These descriptions are provided in the design documentation for the TOE. The design documentation includes:

- Juniper Networks IDP 4.0 & NSM 2006.1 Functional Specification & Correspondence Analysis
- Juniper Networks IDP 4.0 & NSM 2006.1 High-Level Design
- Juniper Networks IDP 4.0 & NSM 2006.1 Security Target

These documents satisfy the following assurance requirements:

- ADV_FSP.1: Informal functional specification
- ADV_HLD.1: Descriptive high-level design
- ADV_RCR.1: Informal correspondence demonstration

6.2.5 Guidance

Juniper Networks provides administrator guidance in the installation, initialization, and administration procedures. These procedures describe the steps necessary to install McAfee Incorporated IDS products in accordance with the evaluated configuration.

The administrator guidance is documented in:

- Concepts & Examples Guide: NetScreen-IDP Fundamentals
- Hardware Guide: NetScreen-IDP 10 (650)
- Hardware Guide: NetScreen-IDP 100 & 500 (1650)
- Hardware Guide: NetScreen-IDP 100, 500, & 1000
- Juniper Networks IDP 4.0 & NSM 2006.1 Security Target
- High Availability QuickStart Guide: NetScreen-IDP 3.0
- QuickStart Guide: NetScreen-IDP 3.0
- RAID Mirroring: IDP 100, 500 (1650)
- Upgrade Guide: NetScreen-IDP 3.0

Since there are no users who are not a member of an administrative role, these documents satisfy the following assurance requirements:

- AGD_ADM.1: administrator guidance
- AGD_USR.1: User guidance

6.2.6 Tests

Juniper Networks provides documentation of how the functional specification has been appropriately tested. These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. The test documentation and evidence of test coverage is documented in:

- Juniper Networks IDP 4.0 & NSM 2006.1 Security Target
- Juniper Networks IDP 4.0 & NSM 2006.1 Testing Documentation

These documents satisfy the following assurance requirements:

- ATE_COV.1: Evidence of coverage
- ATE_FUN.1: Functional testing
- ATE_IND.2: Independent testing – sample

6.2.7 Vulnerability Assessment

The claim made in this Security Target document is SOF-Basic. The TOE includes a probabilistic or permutational function, specifically the password mechanism. The password used at administrator login from a locally connected console is the only probabilistic or permutational function on which the strength of the authentication mechanism depends. Juniper Networks performs vulnerability and strength of function analyses of the TOE to identify weaknesses that can be exploited in the TOE. The vulnerability analysis and strength of function analysis is documented in:

- Juniper Networks IDP 4.0 & NSM 2006.1 Security Target
- Juniper Networks IDP 4.0 & NSM 2006.1 Vulnerability and Strength of Function Analysis

These documents satisfy the following assurance requirements:

- AVA_SOF.1: Strength of TOE security function evaluation
- AVA_VLA.1: Developer vulnerability analysis

7.0 PP Claims

7.1 PP Reference

This ST complies with all security requirements, security objectives, and security environment statements for the defined TOE and its environment as they are stated within Intrusion Detection System System Protection Profile, version 1.5.

7.1.1 IT Security Requirement Statements

The following IT security requirement statements are stated within this ST as specified within the Intrusion Detection System System Protection Profile, version 1.5:

IT Security Assurance Requirements

- ACM_CAP.2: Configuration items
- ADO_DEL.1: Delivery procedures
- ADO_IGS.1: Installation generation and start-up procedures
- ADV_FSP.1: Informal functional specification
- ADV_HLD.1: Descriptive high-level design
- ADV_RCR.1: Informal correspondence demonstration
- AGD_ADM.1: administrator guidance
- AGD_USR.1: User guidance
- ATE_COV.1: Evidence of coverage
- ATE_FUN.1: Functional testing
- ATE_IND.2: Independent testing – sample
- AVA_SOF.1: Strength of TOE security function evaluation
- AVA_VLA.1: Developer vulnerability analysis

IT Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_SAR.1 Audit review
- FAU_SAR.2 Restricted audit review
- FAU_SAR.3 Selectable audit review
- FAU_SEL.1 Selective audit
- FAU_STG.2 Guarantees of audit data availability
- FAU_STG.4 Prevention of audit data loss
- FIA_ATD.1 User attribute definition
- FIA_UAU.1 Timing of authentication
- FIA_UID.1 Timing of identification
- FMT_MOF.1 Management of security functions behaviour
- FMT_MTD.1a Management of TSF data
- FMT_MTD.1b Management of TSF data
- FMT_SMR.1 Security roles
- FPT_ITT.1 Basic internal TSF data transfer protection
- FPT_RVM.1 Non-bypassability of the TSP
- FPT_SEP.1 TSF domain separation
- FPT_STM.1 Reliable time stamps
- IDS_SDC.1 System Data Collection (EXP)
- IDS_ANL.1 Analyser analysis (EXP)
- IDS_RCT.1a Analyser react (EXP)
- IDS_RCT.1b Analyser react (EXP)
- IDS_RDR.1 Restricted Data Review (EXP)

- IDS_STG.1 Guarantee of System Data Availability (EXP)
- IDS_STG.2 Prevention of System data loss (EXP)

7.2 PP Tailoring

This section identifies the security requirements, security objectives, or security environment statements that are tailored from their original specification in the Intrusion Detection System System Protection Profile, version 1.5.

7.2.1 Modified PP Items

The following table identifies items that were modified from the original specification within the PP.

Table 8: Modified PP Items

Modified Item:	Rationale:
Table 4: FMT_MDT.1	The first column of the row “FMT_MDT.1” was changed to state “FMT_MTD.1a”.
FMT_MOF.1.1	This requirement was modified to change the assignment operation from “authorized System administrators” to “authorised System Administrators and Domain Administrators”.
FMT_SMR.1.1	This requirement was modified to change the assignment operation from “authorised administrator, authorised System administrators, and” to “authorised Domain administrators, System administrators, and”.
.IDS_SDC.1.2	This requirement was modified to change the table reference from “Table 3 System Events” to “Table 5: System Events”.
IDS_RCT.1.1	This requirement was iterated to define analyzer reactions when the IDP is configured in Sniffer Mode (IDS_RCT.1a) versus Active Gateway Mode (IDS_RCT.1b).
IDS_RCT.1a.1	This iterated requirement was modified from “The System shall send an alarm to” to “When deployed in the Passive Sniffer Mode configuration, the System shall send an alarm to” to identify the Analyser reaction when the TOE is configured in Sniffer Mode.
IDS_RCT.1b.1	This iterated requirement was modified from “The System shall send an alarm to” to “When deployed in the Active Gateway Mode configuration, the System shall send an alarm to” to identify the Analyser reaction when the TOE is configured in Active Gateway Mode.
IDS_STG.1.2	This requirement was modified to change the text, “from modification” to “from unauthorized modification”.
IDS_STG.1.3	This requirement was modified to change the text, “System data will be maintained when” to “System data within the area occupying 80% of the audit storage will be maintained when”.

7.2.2 Removed PP Items

The following table identifies items that were removed from the original specification within the PP.

Table 9: Removed PP Items

Item Removed:	Rationale:
O.EXPORT	This requirement was removed per Precedent Document PD-0097, Compliance with IDS System PP Export Requirements, since this TOE objective was erroneously replicated into the system PP.
FIA_AFL.1	This requirement was removed per Precedent Document PD-0097, Compliance with IDS System PP Export Requirements, since the TOE does not allow contact from external IT products.
FPT_ITA.1	This requirement was removed per Precedent Document PD-0097, Compliance with IDS System PP Export Requirements, since the TOE does not communicate with IDS componenets outside the IDS system TOE
FPT_ITC.1	This requirement was removed per Precedent Document PD-0097, Compliance with IDS System PP Export Requirements, since the TOE does not communicate with IDS componenets outside the IDS system TOE
FPT_ITI.1	This requirement was removed per Precedent Document PD-0097, Compliance with IDS System PP Export Requirements, since the TOE does not communicate with IDS componenets outside the IDS system TOE

7.3 PP Additions

The following security requirement or security objective statements are identified as being additional to the security requirement and security objective statements that are already stated within Intrusion Detection System System Protection Profile, version 1.5:

Table 10: PP Additions

Item Added:	Rationale:
FMT_SMF.1	This SFR was added to satisfy a dependency added to FMT_MOF.1 by International Interpretation RI #65.
FPT_ITT.1	This requirement was added per Precedent Document PD-0097, Compliance with IDS System PP Export Requirements, since the TOE of the IDS system is distributed, those communications must be protected

8.0 Rationale

This section presents the evidence used in the ST evaluation to support the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements. This section also demonstrates that any PP conformance claims are valid.

8.1 Security Objectives Rationale

Table 11: Mapping of Objectives to Security Environment

ENVIRONMENT \ OBJECTIVES	O.ACCESS	O.AUDITS	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	OE.AUDIT_PROTECTION	OE.PROTECT	OE.TIME	O.CREDEN	O.INSTAL	O.INTROP	O.PERSON	O.PHYCAL
A.ACCESS																	X		
A.ASCOPE																	X		
A.DYNMIC																	X	X	
A.LOCATE																			X
A.MANAGE																		X	
A.NOEVIL															X	X			X
A.NOTRST															X				X
A.PROTCT																			X
T.COMDIS	X				X					X			X						
T.COMINT	X				X			X		X			X						
T.FACCNT		X																	
T.FALACT											X								
T.FALASC				X															
T.FALREC				X															
T.IMPCON	X		X		X											X			
T.INADVE		X					X												
T.INFLUX									X										
T.LOSSOF	X				X			X		X									
T.MISACT		X					X												
T.MISUSE		X					X												
T.NOHALT	X			X	X	X	X												
T.PRIVIL	X				X					X									
T.SCNCFG						X													
T.SCNMLC						X													
T.SCNVUL						X													
P.ACCACT		X			X									X					
P.ACCESS	X				X					X		X							
P.ANALYZ				X															
P.DETECT		X				X	X							X					
P.INTGTY								X											
P.MANAGE	X		X		X					X					X	X		X	

ENVIRONMENT \ OBJECTIVES	O.ACCESS	O.AUDITS	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	OE.AUDIT_PROTECTION	OE.PROTECT	OE.TIME	O.CREDEN	O.INSTAL	O.INTROP	O.PERSON	O.PHYCAL
P.PROTCT									X				X						X

8.1.1 Assumptions

Table 12: Justification for Assumptions Meeting Security Objectives

A.ACCESS *The TOE has access to all the IT System data it needs to perform its functions.*	The **O.INTROP** objective ensures the TOE has the needed access.
A.ASCOPE *The TOE is appropriately scalable to the IT System the TOE monitors.*	The **O.INTROP** objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DYNMIC *The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.*	The **O.INTROP** objective ensures the TOE has the proper access to the IT System. The **O.PERSON** objective ensures that the TOE will be managed appropriately.
A.LOCATE *The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.*	The **O.PHYCAL** objective provides for the physical protection of the TOE.
A.MANAGE *There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.*	The **O.PERSON** objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL *The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.*	The **O.INSTAL** objective ensures that the TOE is properly installed and operated and the **O.PHYCAL** objective provides for physical protection of the TOE by authorized administrators. The **O.CREDEN** objective supports this assumption by requiring protection of all authentication data.
A.NOTRST *The TOE can only be accessed by authorized users.*	The **O.PHYCAL** objective provides for physical protection of the TOE to protect against unauthorized access. The **O.CREDEN** objective supports this assumption by requiring protection of all authentication data.

A.PROTCT *The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.*	The **O.PHYCAL** objective provides for the physical protection of the TOE hardware and software.

8.1.2 Threats

Table 13: Justification for Threats Countered By Security Objectives

T.COMDIS *An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.*	The **O.IDAUTH** objective provides for authentication of users prior to any TOE data access. The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The **O.PROTCT** objective addresses this threat by providing TOE self-protection. The **OE.PROTECT** objective addresses this threat by utilizing IT environment security mechanisms that provide for protection of the TOE.
T.COMINT *An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.*	The **O.IDAUTH** objective provides for authentication of users prior to any TOE data access. The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The **O.INTEGR** objective ensures no TOE data will be modified. The **O.PROTCT** objective addresses this threat by providing TOE self-protection. The **OE.PROTECT** objective addresses this threat by utilizing IT environment security mechanisms that provide for protection of the TOE.
T.FACCNT *Unauthorized attempts to access TOE data or security functions may go undetected.*	The **O.AUDITS** objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.FALACT *The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.*	The **O.RESPON** objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALASC *The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.*	The **O. IDANLZ** objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.FALREC *The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.*	The **O.IDANLZ** objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.IMPCON *An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.*	The **O.INSTAL** objective states the authorized administrators will configure the TOE properly. The **O.EADMIN** objective ensures the TOE has all the necessary administrator functions to manage the product. The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INADVE *Inadvertent activity and access may occur on an IT System the TOE monitors.*	The **O.AUDITS** and **O.IDSENS** objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.INFLUX *An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.*	The **O.OFLOWS** objective counters this threat by requiring the TOE handle data storage overflows.
T.LOSSOF *An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.*	The **O.IDAUTH** objective provides for authentication of users prior to any TOE data access. The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The **O.INTEGR** objective ensures no TOE data will be deleted. The **O.PROTCT** objective addresses this threat by providing TOE self-protection.
T.MISACT *Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.*	The **O.AUDITS** and **O.IDSENS** objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.MISUSE *Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.*	The **O.AUDITS** and **O.IDSENS** objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.NOHALT *An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.*	The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The **O.IDSCAN**, **O.IDSENS**, and **O.IDANLZ** objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.
T.PRIVIL *An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.*	The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The **O.PROTCT** objective addresses this threat by providing TOE self-protection.
T.SCNCFG *Improper security configuration settings may exist in the IT System the TOE monitors.*	The **O.IDSCAN** objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change.
T.SCNMLC *Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.*	The **O.IDSCAN** objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL *Vulnerabilities may exist in the IT System the TOE monitors.*	The **O.IDSCAN** objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability.

8.1.3 Organizational Security Policies

Table 14: Justification for OSPs Satisfied By Security Objectives

P.ACCACT *Users of the TOE shall be accountable for their actions within the IDS.*	The **O.AUDITS** objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The **O.IDAUTH** objective supports this objective by ensuring each user is uniquely identified and authenticated. The **OE.TIME** objective supports this policy by providing accurate time stamps from the IT environment.
P.ACCESS *All data collected and produced by the TOE shall only be used for authorized purposes.*	The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The **O.PROTCT** objective addresses this policy by providing TOE self-protection. The **OE.AUDIT_PROTECTION** objective supports this policy by using the storage protection mechanisms of the IT environment.
P.ANALYZ *Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.*	The **O.IDANLZ** objective requires analytical processes be applied to data collected from Sensors and Scanners.
P.DETECT *Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.*	The **O.AUDITS**, **O.IDSENS**, and **O.IDSCAN** objectives address this policy by requiring collection of audit, Sensor, and Scanner data. The **OE.TIME** objective supports this policy by providing accurate time stamps from the IT environment.
P.INTGTY *Data collected and produced by the TOE shall be protected from modification.*	The **O.INTEGR** objective ensures the protection of data from modification.
P.MANAGE *The TOE shall only be managed by authorized users.*	The **O.PERSON** objective ensures competent administrators will manage the TOE and the **O.EADMIN** objective ensures there is a set of functions for administrators to use. The **O.INSTAL** objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The **O.CREDEN** objective requires administrators to protect all authentication data. The **O.PROTCT** objective addresses this policy by providing TOE self-protection.
P.PROTCT *The TOE shall be protected from unauthorized accesses and disruptions of TOE data and*	The **O.OFLOWS** objective counters this policy by requiring the TOE

functions.	handle disruptions. The **O.PHYCAL** objective protects the TOE from unauthorized physical modifications. The **OE.PROTECT** objective supports this policy by providing IT environment security mechanisms that provide for protection of the TOE.

8.2 Security Requirements Rationale

8.2.1 Security Requirements Coverage

8.2.1.1 Security Functional Requirements

Table 15: Mapping of SFRs to Security Objectives

TOE SFRs \ OBJECTIVES	O.ACCESS	O.AUDITS	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	OE.AUDIT_PROTECTION	OE.PROTECT	OE.TIME	O.CREDEN	O.INSTAL	O.INTROP	O.PERSON	O.PHYCAL
FAU_GEN.1 Audit data generation		X																	
FAU_SAR.1 Audit review			X																
FAU_SAR.2 Restricted audit review	X				X														
FAU_SAR.3 Selectable audit review			X																
FAU_SEL.1 Selective audit		X	X																
FAU_STG.2 Guarantees of audit data availability	X				X			X	X	X		X							
FAU_STG.4 Prevention of audit data loss		X							X										
FIA_ATD.1 User attribute definition					X														
FIA_UAU.1 Timing of authentication	X				X														
FIA_UID.1 Timing of identification	X				X														
FMT_MOF.1 Management of security functions behaviour	X				X					X									
FMT_MTD.1a Management of TSF data	X				X			X		X									
FMT_MTD.1a Management of TSF data	X				X			X		X									
FMT_SMF.1 Specification of Management Functions	X				X														
FMT_SMR.1 Security roles					X														
FPT_ITT.1 Basic internal TSF data transfer protection								X											
FPT_RVM.1 Non-bypassability of the TSP		X	X		X			X		X			X						
FPT_SEP.1 TSF domain separation		X	X		X			X		X			X						
FPT_STM.1 Reliable time stamps		X												X					
IDS_SDC.1 System Data Collection (EXP)						X	X												
IDS_ANL.1 Analyser analysis (EXP)				X															
IDS_RCT.1a Analyser react (EXP)											X								
IDS_RCT.1b Analyser react (EXP)											X								
IDS_RDR.1 Restricted Data Review (EXP)	X		X		X														
IDS_STG.1 Guarantee of System Data Availability (EXP)	X				X			X	X	X									
IDS_STG.2 Prevention of System data loss (EXP)									X										

Table 16: Justification for Security Objectives to be met by the TOE SFRs

O.ACCESS *The TOE must allow authorized users to access only appropriate TOE functions and data.*	The TOE is required to restrict the review of audit data to those granted with explicit read-access [**FAU_SAR.2**]. The System is required to restrict the review of System data to those granted with explicit read-access [**IDS_RDR.1**]. The TOE is required to protect

	the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**]. The System is required to protect the System data from any modification and unauthorized deletion [**IDS_STG.1**]. Users authorized to access the TOE are defined using an identification and authentication process [**FIA_UID.1**, **FIA_UAU.1**]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [**FMT_MOF.1 & FMT_SMF.1**]. Only authorized administrators of the System may query and/or add System and audit data, and authorized administrators of the TOE may query and/or modify all other TOE data [**FMT_MTD.1a, FMT_MTD.1b**].
O.AUDITS *The TOE must record audit records for data accesses and use of the System functions.*	Security-relevant events must be defined and auditable for the TOE [**FAU_GEN.1**]. The TOE must provide the capability to select which security-relevant events to audit [**FAU.SEL.1**]. The TOE must prevent the loss of collected data in the event the audit trail is full [**FAU_STG.4**]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [**FPT_RVM.1**]. The TSF must be protected form interference that would prevent it from performing its functions [**FPT_SEP.1**]. Time stamps associated with an audit record must be reliable [**FPT_STM.1**].
O.EADMIN *The TOE must include a set of functions that allow effective management of its functions and data.*	The TOE must provide the ability to review and manage the audit trail of the System [**FAU_SAR.1**, **FAU_SAR.3**, **FAU_SEL.1**]. The System must provide the ability for authorized administrators to view all System data collected and produced [**IDS_RDR.1**]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [**FPT_RVM.1**]. The TSF must be protected from interference that would prevent it from performing its functions [**FPT_SEP.1**].
O.IDANLZ *The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).*	The Analyzer is required to perform intrusion analysis and generate conclusions [**IDS_ANL.1**].
O.IDAUTH *The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.*	The TOE is required to restrict the review of audit data to those granted with explicit read-access [**FAU_SAR.2**]. The System is required to restrict the review of System data to those granted with explicit read-access [**IDS_RDR.1**]. The TOE is required to protect the stored audit records from unauthorized deletion [**FAU_STG.2**]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [**IDS_STG.1**]. Security attributes of subjects used to enforce the authentication policy of the TOE must be defined [**FIA_ATD.1**]. Users authorized to access the TOE are defined using an identification and authentication process [**FIA_UID.1**, **FIA_UAU.1**]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [**FMT_MOF.1**]. Only authorized administrators of the System may query and/or add System and audit data, and authorized administrators of the TOE may query and/or modify all

	other TOE data [**FMT_MTD.1a, FMT_MTD.1b**]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [**FMT_SMR.1**]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [**FPT_RVM.1**]. The TSF must be protected from interference that would prevent it from performing its functions [**FPT_SEP.1**].
O.IDSCAN *The Scanner must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.*	A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [**IDS_SDC.1**].
O.IDSENS *The Sensor must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.*	A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [**IDS_SDC.1**].
O.INTEGR *The TOE must ensure the integrity of all audit and System data.*	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**]. The System is required to protect the System data from any modification and unauthorized deletion [**IDS_STG.1**]. Only authorized administrators of the System may query and/or add audit and System data [**FMT_MTD.1a, FMT_MTD.1b**]. The TOE must protect TSF data from unauthorized disclosure during transmission between the IDP Sensor, NSM Server, and NSM UI components of the TOE [**FPT_ITT.1**]. The TOE must ensure that all functions to protect the data are not bypassed [**FPT_RVM.1**]. The TSF must be protected from interference that would prevent it from performing its functions [**FPT_SEP.1**].
O.OFLOWS *The TOE must appropriately handle potential audit and System data storage overflows.*	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**]. The TOE must prevent the loss of audit data in the event that its audit trail is full [**FAU_STG.4**]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [**IDS_STG.1**]. The System must prevent the loss of System data in the event that storage capacity is reached [**IDS_STG.2**].
O.PROTCT *The TOE must protect itself from unauthorized modifications and access to its functions and data.*	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [**IDS_STG.1**]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [**FMT_MOF.1**]. Only authorized administrators of the System may query and/or add System and audit data, and authorized administrators of the TOE may query and/or modify all other TOE data [**FMT_MTD.1a, FMT_MTD.1b**]. The TOE must ensure that all functions are invoked and succeed before each function may

	proceed [**FPT_RVM.1**]. The TSF must be protected from interference that would prevent it from performing its functions [**FPT_SEP.1**].
O.RESPON *The TOE must respond appropriately to analytical conclusions.*	The TOE is required to respond accordingly in the event an intrusion is detected [**IDS_RCT.1a & IDS_RCT.1b**].
OE.AUDIT_PROTECTION *The IT Environment will provide the capability to protect audit information.*	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**].
OE.PROTECT *The IT environment will protect itself and the TOE from external interference or tampering.*	The IT environment must ensure that all functions are invoked and succeed before each function may proceed [**FPT_RVM.1**]. The TSF must be protected from interference that would prevent it from performing its functions [**FPT_SEP.1**].
OE.TIME *The IT Environment will provide reliable timestamps to the TOE.*	The IT environment is required to provide accurate time stamps for all audit and System data [**FPT_STM**].

8.2.1.2 Security Functional Requirements Dependencies

Table 17: Security Functional Requirements Dependencies

Requirements:	Dependencies:	Satisfied:
FAU_GEN.1 Audit data generation	FPT_STM.1	*yes*
FAU_SAR.1 Audit review	FAU_GEN.1	*yes*
FAU_SAR.2 Restricted audit review	FAU_SAR.1	*yes*
FAU_SAR.3 Selectable audit review	FAU_SAR.1	*yes*
FAU_SEL.1 Selective audit	FAU_GEN.1, FMT_MTD.1a FMT_MTD.1b	*yes*
FAU_STG.2 Guarantees of audit data availability	FAU_GEN.1	*yes*
FAU_STG.4 Prevention of audit data loss	FAU_GEN.1	*yes*
FIA_ATD.1 User attribute definition	NONE	*yes*
FIA_UAU.1 Timing of authentication	FIA_UID.1	*yes*
FIA_UID.1 Timing of identification	NONE	*yes*
FMT_MOF.1 Management of security functions behaviour	FMT_SMF.1, FMT_SMR.1	*yes*
FMT_MTD.1a Management of TSF data	FMT_SMF.1, FMT_SMR.1	*yes*
FMT_MTD.1a Management of TSF data	FMT_SMF.1, FMT_SMR.1	*yes*
FMT_SMF.1 Specification of Management Functions	NONE	*yes*
FMT_SMR.1 Security roles	FIA_UID.1	*yes*
FPT_ITT.1 Basic internal TSF data transfer protection	NONE	*yes*
FPT_RVM.1 Non-bypassability of the TSP	NONE	*yes*
FPT_SEP.1 TSF domain separation	NONE	*yes*
FPT_STM.1 Reliable time stamps	NONE	*yes*
IDS_SDC.1 System Data Collection (EXP)	NONE	*yes*
IDS_ANL.1 Analyser analysis (EXP)	NONE	*yes*
IDS_RCT.1a Analyser react (EXP)	NONE	*yes*
IDS_RCT.1b Analyser react (EXP)	NONE	*yes*
IDS_RDR.1 Restricted Data Review (EXP)	NONE	*yes*

Requirements:	Dependencies:	Satisfied:
IDS_STG.1 Guarantee of System Data Availability (EXP)	NONE	*yes*
IDS_STG.2 Prevention of System data loss (EXP)	NONE	*yes*

8.2.2 Security Requirements Justification

This section demonstrates that the choice of security requirements is justified.

8.2.2.1 Justification of Unsatisfied Dependencies

There are no unsatisfied dependencies identified for the security requirements of TOE.

8.2.2.2 Justification of Explicitly Stated Requirements

Justification for the requirements explicitly stated within this ST is provided within the IDSSPP.

8.2.2.3 Internal Consistency of SFRs

The IT security requirements defined for the TOE are stated in a manner in which they do not conflict with each other. Therefore, no justification is needed for conflicting IT security requirements.

8.2.2.4 EAL Justification

Juniper Networks has chosen to pursue a Common Criteria evaluation because of the government customer requirements that are mandated by NSTISS Policy 11. This policy requires a Common Criteria certification for all products to be used within systems used for entering, processing, storing, displaying, or transmitting national security information.

Juniper Networks has specifically chosen an EAL2 evaluation assurance level to meet the requirements mandated by the DoD and Air Force divisions of the government in accordance with the USDoD NSTISSP #11 Interpretation and the USAF CIO Memorandum.

This ST contains the assurance requirements from the CC EAL2 assurance package. This assurance package ensures good commercial development practices to provide a low to moderate level of assurance. While the System may monitor a hostile environment, it is expected to be located within a non-hostile environment and embedded in or protected by other products designed to address threats that correspond with the intended environment. The security environment also assumes that the TOE components are physically protected. The TOE is also restricted from remote administration, which prevents offering any opportunity for an attacker to bypass the security policies without physical access. Therefore, the EAL 2 assurance package selected provides an appropriate level of assurance in the security functions offered by the TOE.

8.2.3 Validation of Strength-Of-Function Claims

IDP and NSM are targeted at a generalized IT environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a low attack potential. As such, minimum and explicit strength of function claims of ‘SOF-basic’ is appropriate for the intended environment.

The TOE (specifically, the TOE’s password mechanism under FIA_UAU.1) meets or exceeds the minimum strength of function claim of SOF-basic. The TOE requires user defined authentication tokens (i.e., passwords) that can be analyzed via probabilistic or permutational means. The TOE requires that the minimum password length used to authenticate a user assigned to the System Administrator, Read-only System Administrator, Domain Administrator, or Read-only Domain Administrator role be equal to or greater than 9 characters. The password may contain any combination of alphabetics, numerics, or special characters.

8.3 TOE Summary Specification Rationale

8.3.1 Security Functions Meet SFRs

Table 18: Mapping of TOE SFRs to TOE Security Functions

	Auditing	Identification & Authentication	Security Management	Self Protection	Intrusion Detection & Prevention
FAU_GEN.1 Audit data generation	X				
FAU_SAR.1 Audit review	X				
FAU_SAR.2 Restricted audit review	X				
FAU_SAR.3 Selectable audit review	X				
FAU_SEL.1 Selective audit	X				
FAU_STG.2 Guarantees of audit data availability	X				
FAU_STG.4 Prevention of audit data loss	X				
FIA_ATD.1 User attribute definition		X			
FIA_UAU.1 Timing of authentication		X			
FIA_UID.1 Timing of identification		X			
FMT_MOF.1 Management of security functions behaviour			X		
FMT_MTD.1a Management of TSF data			X		
FMT_MTD.1a Management of TSF data			X		
FMT_SMF.1 Specification of Management Functions			X		
FMT_SMR.1 Security roles			X		
FPT_ITT.1 Basic internal TSF data transfer protection				X	
FPT_RVM.1 Non-bypassability of the TSP				X	
FPT_SEP.1 TSF domain separation				X	
FPT_STM.1 Reliable time stamps				X	
IDS_SDC.1 System Data Collection (EXP)					X
IDS_ANL.1 Analyser analysis (EXP)					X
IDS_RCT.1a Analyser react (EXP)					X
IDS_RCT.1b Analyser react (EXP)					X
IDS_RDR.1 Restricted Data Review (EXP)					X
IDS_STG.1 Guarantee of System Data Availability (EXP)					X
IDS_STG.2 Prevention of System data loss (EXP)					X

Table 19: Rationale for Security Functions Satisfying SFRs

Security Functions	SFRs	Rationale
Auditing	FAU_GEN.1	The TOE implements audit data generation for events related to operations performed by IDP 4.0 & NSM 2006.1. These events include the start-up and shutdown of audit functions, access to System, access to the TOE and System data, reading of information from the audit records, unsuccessful attempts to read information from the audit records, all modifications to the audit configuration that occur while the audit collection functions are operating, all use of the authentication mechanism, all use of the user identification mechanism, all modifications in the behavior of the functions of the TSF, all modifications to the values of TSF data, and modifications to the group of users that are part of a role.
	FAU_SAR.1	The TOE implements audit review by providing the authorized Read-Only Administrator and the authorized Read/Write Administrator with the capability to view the auditable events recorded in a manner that is interpretable.
	FAU_SAR.2	The TOE implements restricted audit review by restricting access to view the audit records to the authorized Read-Only Administrator and the authorized Read/Write Administrator.
	FAU_SAR.3	The TOE implements selectable audit review by providing the authorized Read-Only Administrator and the authorized Read/Write Administrator with the capability to sort audit data based on the date, time, subject identity, type of event, and success or failure of each related event from within the NSM UI.
	FAU_SEL.1	The TOE implements selective auditing by providing the capability to select the audit events that are allowed to be recorded based on the type of event, such as attack, config, and traffic events.
	FAU_STG.2	The TOE guarantees audit data availability by preventing unauthorized access to the audit data, providing integrity checking capabilities of the audit data, and ensuring the availability of the most recent audit data upon audit data storage exhaustion.
	FAU_STG.4	The IT Environment prevents audit data loss by providing the capability to ensure the availability of the most recent audit data upon audit data storage exhaustion.
Identification & Authentication	FIA_ATD.1	The TOE implements the association of security attributes to users by providing the capability to maintain users' identity, authentication data, and authorizations.
	FIA_UAU.1	The TOE implements user authentication by providing the capability for users to authenticate to IDP 4.0 & NSM 2006.1.
	FIA_UID.1	The TOE implements user identification by providing the capability for users to be identified to IDP 4.0 & NSM 2006.1.
Security Management	FMT_MOF.1	The TOE implements the management of security functions behavior by providing the capability to restrict the ability to modify the behavior of the functions of System data collection, analysis and reaction to authorised Read/Write administrators.

Security Functions	SFRs	Rationale
	FMT_MTD.1a	The TOE implements management of TSF data by providing the capability to restrict the ability to query and add System and audit data and to restrict the ability to query and modify all other TOE data to the authorized System Administrator role.
	FMT_MTD.1b	The TOE implements management of TSF data by providing the capability to restrict the ability to query System and audit data and to restrict the ability to query all other TOE data to the authorized Read-Only System Administrators, Domain Administrators, and Read-Only Domain Administrators.
	FMT_SMF.1	The TOE implements the specification of management functions by providing the capability to manage user accounts, audit data, audit configurations, and security policies.
	FMT_SMR.1	The TOE implements security management roles by providing roles for an authorized Read-Only Administrator and the authorized Read/Write Administrator.
Self Protection	FPT_ITT.1	The TOE implements the capability to encrypt all System data transmitted between the IDP Sensor, NSM Server, and NSM UI components of the TOE.
	FPT_RVM.1	The IT Environment implements non-bypass ability of the TOE security policy by requiring users to be successfully authenticated prior to allowing any other TSF-mediated actions to be performed.
	FPT_SEP.1	The IT Environment implements domain separation by providing the capability to manage the TOE on an interface that is inaccessible from the interface that is used to monitor traffic.
	FPT_STM.1	The IT Environment implements reliable time stamping by providing the capability to directly request and retrieve the time stamp for each audit event directly from the underlying operating system or kernel.
Intrusion Detection & Prevention	IDS_SDC.1	The TOE implements system data collection by providing the sensing capabilities to collect service requests, network traffic, and security configuration changes, and the scanning capabilities to collect detected malicious code, service configuration, detected known vulnerabilities.
	IDS_ANL.1	The TOE implements an analyzer analysis by providing analyzing capabilities using signature, Protocol Anomaly, Backdoor, Traffic Anomaly, IP Spoofing, Layer 2, and Denial of Service (DoS) analyzing methods to detect intrusions.
	IDS_RCT.1a	The TOE implements an analyzer reaction from within the Passive Sniffer Mode configuration by providing the capability to send an alarm to an administrator upon the detection of an intrusion.
	IDS_RCT.1b	The TOE implements an analyzer reaction from within any of the Active Gateway Mode configurations by providing the capability to send an alarm to an administrator upon the detection of an intrusion and either drop, block, or ignore the intrusion depending on the actions configured within the security policy.

Security Functions	SFRs	Rationale
	IDS_RDR.1	The TOE implements restricted data review by restricting capability to read audit logs, security policies, profiler data, and user account information from the System data to only the authorized Read/Write Administrators and authorized Read-Only Administrators.
	IDS_STG.1	The TOE guarantees system data availability by preventing unauthorized access to the system data, providing integrity checking capabilities of the system data, and ensuring the availability of the most recent system data upon system data storage exhaustion.
	IDS_STG.2	The TOE prevents system data loss by providing the capability to ensure the availability of the most recent system data upon audit data storage exhaustion.

8.3.2 Assurance Measures Meet Assurance Requirements

This section demonstrates that the claim is justified that the stated assurance measures are compliant with the assurance requirements.

Table 20: Rationale for Assurance Measures Satisfying SARs

Assurance Requirements	Assurance Measures	Rationale
ACM_CAP.2	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document provides a unique identifier for the TOE.
	Juniper Networks IDP 4.0 & NSM 2006.1 Configuration Management System	This document lists the configuration items that comprise the TOE and describes the methods used for identifying them.
ADO_DEL.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document provides a unique identifier for the TOE and identification of the TOE components to be delivered.
	Juniper Networks IDP 4.0 & NSM 2006.1 Delivery Procedures	This document provides procedures for the delivery method of the TOE to the consumer.
ADO_IGS.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies unique TOE identifier, the TOE components to be installed, and the required configuration(s) for the TOE.
	Concepts & Examples Guide: NetScreen-IDP Fundamentals	These documents describe the steps necessary for secure installation, generation, and start-up of the TOE.
	Hardware Guide: NetScreen-IDP 10 (650)	
	Hardware Guide: NetScreen-IDP 100 & 500 (1650)	
	Hardware Guide: NetScreen-IDP 100, 500, & 1000	
	High Availability QuickStart Guide: NetScreen-IDP 3.0	
	QuickStart Guide: NetScreen-IDP 3.0	
	RAID Mirroring: IDP 100, 500 (1650)	
	Upgrade Guide: NetScreen-IDP 3.0	
ADV_FSP.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies the security functions that are covered by the functional specification.
	Juniper Networks IDP 4.0 & NSM 2006.1 Functional Specification & Correspondence Analysis	This document describes the TSF and the external interfaces to the TOE security functions.
ADV_HLD.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies the security functions that are covered by the high-level design.
	Juniper Networks IDP 4.0 & NSM 2006.1 High-Level Design	This document groups the security functions claimed in the ST into logical subsystems. This document also describes the TOE subsystems, their interfaces, and any mechanisms required by the TOE IT environment.
ADV_RCR.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies the security functions that are covered by the correspondence.
	Juniper Networks IDP 4.0 & NSM 2006.1 Functional Specification & Correspondence Analysis	This document identifies the interfaces that are to be mapped to security functions and also provides this analysis.

Assurance Requirements	Assurance Measures	Rationale
AGD_ADM.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies the TOE unique identifier, any security configurations required, and assumptions to be made.
	Concepts & Examples Guide: NetScreen-IDP Fundamentals	These documents provide administrative guidance to the TOE administrators with detailed, accurate information of how to administer the TOE in a secure manner.
	Hardware Guide: NetScreen-IDP 10 (650)	
	Hardware Guide: NetScreen-IDP 100 & 500 (1650)	
	Hardware Guide: NetScreen-IDP 100, 500, & 1000	
	High Availability QuickStart Guide: NetScreen-IDP 3.0	
	QuickStart Guide: NetScreen-IDP 3.0	
	RAID Mirroring: IDP 100, 500 (1650)	
	Upgrade Guide: NetScreen-IDP 3.0	
AGD_USR.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies the TOE unique identifier, any security configurations required, and assumptions to be made.
	Concepts & Examples Guide: NetScreen-IDP Fundamentals	These documents provide user guidance to the TOE users with the necessary background and specific information on how to correctly use the TOE's protection functions.
	Hardware Guide: NetScreen-IDP 10 (650)	
	Hardware Guide: NetScreen-IDP 100 & 500 (1650)	
	Hardware Guide: NetScreen-IDP 100, 500, & 1000	
	High Availability QuickStart Guide: NetScreen-IDP 3.0	
	QuickStart Guide: NetScreen-IDP 3.0	
	RAID Mirroring: IDP 100, 500 (1650)	
	Upgrade Guide: NetScreen-IDP 3.0	
ATE_COV.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies and describes the TOE security functions that are to be mapped to individual test cases.
	Juniper Networks IDP 4.0 & NSM 2006.1 Testing Documentation	This document shows the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. The testing coverage is provided within the testing procedures document as it is listed here.
ATE_FUN.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies and describes the TOE and the TOE security functions that are to be tested.
	Juniper Networks IDP 4.0 & NSM 2006.1 Testing Documentation	This document provides a test plan, test procedure descriptions, expected test results and actual test results for testing the claimed security functionalities of the TOE.
ATE_IND.2	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies and describes the TOE and the TOE security functions that are to be tested.
	Juniper Networks IDP 4.0 & NSM 2006.1 Testing Documentation	Independent testing requires Juniper Networks to provide the TOE suitable for testing and Juniper Networks has fulfilled this requirement.

Assurance Requirements	Assurance Measures	Rationale
AVA_SOF.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies any strength of function claims made for the TOE for which a strength of function analysis may be required.
	Juniper Networks IDP 4.0 & NSM 2006.1 Vulnerability and Strength of Function Analysis	This document provides an analysis of any strength of function claims within this ST.
AVA_VLA.1	Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	This document identifies the TOE components and configuration(s) for which obvious vulnerabilities may be identified.
	Juniper Networks IDP 4.0 & NSM 2006.1 Vulnerability and Strength of Function Analysis	This document identifies any obvious vulnerabilities pointed out in any of the TOE evaluation deliverables or identified within a public domain (i.e. website).

8.4 PP Claims Rationale

The differences between this ST and the IDSSPP v1.5 are identified and described within section 5.1.1.2.2.2 of this ST.

9.0 Annex A

Annex A provides a list of acronyms, terms, and references used throughout this document.

9.1 Acronyms

9.1.1 CC-Specific Acronyms

CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

9.1.2 TOE-Specific Acronyms

IDS	Intrusion Detection System
IDP	Intrusion Detection & Prevention system

9.2 Terms

9.2.1 CC-Specific Terms

These terms are drawn from section 2.3 of CC Part 1.

Assets	Information or resources to be protected by the countermeasures of a TOE.
Assignment	The specification of an identified parameter in a component.
Assurance	Grounds for confidence that an entity meets its security objectives.
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.
Authentication data	Information used to verify the claimed identity of a user.
Authorized user	A user who may, in accordance with the TSP, perform an operation.
Class	A grouping of families that share a common focus.
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.
Connectivity	The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
Element	An indivisible security requirement.
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Family	A grouping of components that share security objectives but may differ in emphasis or rigor.

Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.
Guidance documentation	Guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in section 6.2 of this ST.
Human user	Any person who interacts with the TOE.
Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Informal	Expressed in natural language.
Internal communication channel	A communication channel between separated parts of TOE.
Internal TOE transfer	Communicating data between separated parts of the TOE.
Inter-TSF transfers	Communicating data between the TOE and the security functions of other trusted IT products.
Iteration	The use of a component more than once with varying operations.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
Organizational security policies	One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.
Package	A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.
Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Reference monitor	The concept of an abstract machine that enforces TOE access control policies.
Reference validation mechanism	An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
Security attribute	Characteristics of subjects, users, objects, information, and/or resources that is used for the enforcement of the TSP.

Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Selection	The specification of one or more items from a list in a component.
Semiformal	Expressed in a restricted syntax language with defined semantics.
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
SOF-basic	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.
SOF-high	A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential.
Subject	An entity within the TSC that causes operations to be performed.
System	A specific IT installation, with a particular purpose and operational environment.
Target of Evaluation (TOE)	An IT product or system and its associated guidance documentation that is the subject of an evaluation.
TOE resource	Anything useable or consumable in the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Functions Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
TOE security policy model	A structured representation of the security policy to be enforced by the TOE.
Transfers outside TSF control	Communicating data to entities not under control of the TSF.

Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.
Trusted path	A means by which a user and a TSF can communicate with necessary confidence to support the TSP.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.

9.2.2 TOE-Specific Terms

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

Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection (ID)	Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
Intrusion Detection System (IDS)	A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
Intrusion Detection System Analyzer (Analyzer)	The component of an IDS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).
Intrusion Detection System Scanner (Scanner)	The component of an IDS that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
Intrusion Detection System Sensor (Sensor)	The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.
Network	Two or more machines interconnected for communications.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packet Sniffer	A device or program that monitors the data traveling between computers on a network.
Scanner data	Data collected by the Scanner functions.
Scanner functions	The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data)
Security	A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
Sensor data	Data collected by the Sensor functions.
Sensor functions	The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data).
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
System data	Data collected and produced by the System functions.
System functions	Functions performed by all IDS component (i.e., Analyzer functions, Scanner functions, and Sensor functions).
Trojan Horse	An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.
Virus	A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability	Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

9.3 Interpretations

9.3.1 International Interpretations

No international (CCIMB) interpretations are included within this ST.

9.3.2 National Interpretations

No national (NIAP) interpretations are included within this ST.

9.4 Document References

Title	Version	Date	Author
Concepts & Examples Guide: NetScreen-IDP Fundamentals, P/N: 093-1356-000	3.0 Rev. A	N/A	Juniper Networks
Hardware Guide: NetScreen-IDP 10 (650), P/N: 093-1357-000	3.0 Rev. A	N/A	Juniper Networks
Hardware Guide: NetScreen-IDP 100 & 500 (1650), P/N: 093-1358-000	3.0 Rev. A	N/A	Juniper Networks
Hardware Guide: NetScreen-IDP 100, 500, & 1000, P/N: 093-1359-000	3.0 Rev. A	N/A	Juniper Networks
Juniper Networks IDP 4.0 & NSM 2006.1 Configuration Management System	TBD	TBD	Veridyn Inc.
Juniper Networks IDP 4.0 & NSM 2006.1 Delivery Procedures	TBD	TBD	Veridyn Inc.
Juniper Networks IDP 4.0 & NSM 2006.1 Functional Specification & Correspondence Analysis	TBD	TBD	Veridyn Inc.
Juniper Networks IDP 4.0 & NSM 2006.1 High-Level Design	TBD	TBD	Veridyn Inc.
Juniper Networks IDP 4.0 & NSM 2006.1 Security Target	0.7 Rev. 7	11/1/2006	Veridyn Inc.
Juniper Networks IDP 4.0 & NSM 2006.1 Testing Documentation	TBD	TBD	Veridyn Inc.
Juniper Networks IDP 4.0 & NSM 2006.1 Vulnerability and Strength of Function Analysis	TBD	TBD	Veridyn Inc.
High Availability QuickStart Guide: NetScreen-IDP 3.0, P/N: 093-1360-000	3.0 Rev. A	N/A	Juniper Networks
QuickStart Guide: NetScreen-IDP 3.0, P/N: 093-1361-000	3.0 Rev. A	N/A	Juniper Networks
RAID Mirroring: IDP 100, 500 (1650), P/N: 093-1364-000	3.0 Rev. A	N/A	Juniper Networks
Upgrade Guide: NetScreen-IDP 3.0, P/N: 093-1365-000	3.0 Rev. A	N/A	Juniper Networks