NitroSecurity Intrusion Prevention System Version 7.1.3 Security Target

Version 1.0

05/25/07

Prepared for:

NitroSecurity, Inc

12030 Sunrise Valley Drive, Suite 180
Reston, VA. 20191

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Table of Contents

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is NitroSecurity Intrusion Prevention System provided by NitroSecurity, Inc. The TOE is an intrusion detection and prevention system that can detect network intrusion attempts and react by actively recording and/or blocking such attempts.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by the TOE and IT environment, and the organizational policy that the TOE must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and IT environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and IT Environment that supports the TOE, and details the assurance requirements.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – NitroSecurity Intrusion Prevention System Version 7.1.3 Security Target

ST Version – Version 1.0

ST Date – 05/25/07

TOE Identification –

- NitroSecurity IPS 7.1.3 running on any one of the following supported appliance models:
  - NS-IPS-150-2BTX, NS-IPS-300-2BTX, NS-IPS-300-4BTX, NS-IPS-300-2SX, NS-IPS-300-4SX, NS-IPS-300R-2BTX, NS-IPS-300R-4BTX, NS-IPS-300R-2SX, NS-IPS-300R-2BSX, NS-IPS-300R-4SX, NS-IPS-300R-4BSX, NS-IPS-620R-2BTX, NS-IPS-620R-4BTX, NS-IPS-620R-8BTX, NS-IPS-620R-2SX, NS-IPS-620R-2BSX, NS-IPS-620R-4SX, NS-IPS-620R-4BSX, NS-IPS-1220R-2BTX, NS-IPS-1220R-4BTX, NS-IPS-1220R-8BTX, NS-IPS-1220R-2SX, NS-IPS-1220R-2BSX, NS-IPS-1220R-4SX, NS-IPS-1220R-4BSX
- NitroSecurity ESM 7.1.3 running on any one of the following supported appliance models:
  - NS-ESS-10, NS-ESS-R-10, NS-ESS-XP-5, NS-ESS-XP-10, NS-ESS-R-100, NS-ESM-R-NRC-2200, NS-ESM-R-NRC-4200, NS-ESS-XP-5, NS-ESS-XP-10

TOE Developer – NitroSecurity, Inc.

Evaluation Sponsor – NitroSecurity, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

1.2 Conformance Claims

This TOE is conformant to the following Common Criteria (CC) specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
    - Part 3 Conformant
    - EAL 3

The TOE is further conformant to the following Protection Profile (PP):

- U.S. Government Intrusion Detection System System Protection Profile (IDSSPP), Version 1.6, April 4, 2006

1.3 Conventions

This section specifies the formatting information used in the ST.

The following conventions have been applied in this document:

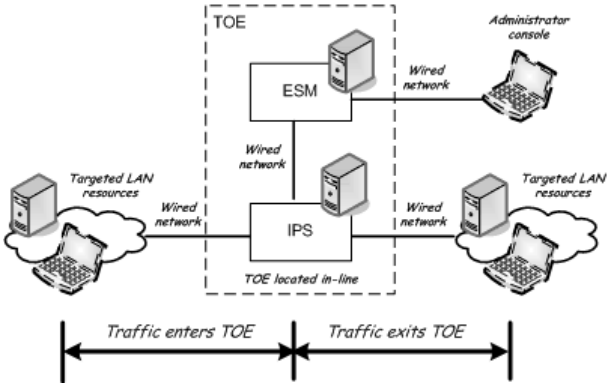
- Security Functional Requirements (SFRs) – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Explicitly stated SFRs (i.e., those not found in Part 2 of the CC) are identified with "(EXP)" following the identification of the new functional class/name (i.e., Intrusion Detection System (IDS)) and the associated family descriptor. Example: Analyzer analysis (EXP) (IDS_ANL.1)
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

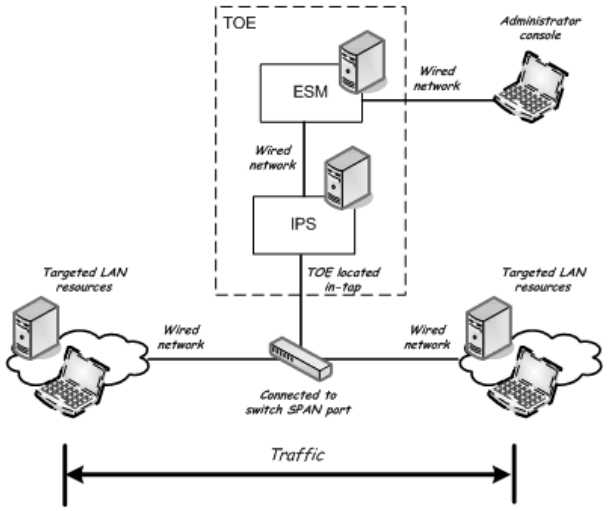
The TOE is NitroSecurity Intrusion Prevention System (IPS) version 7.1.3. The TOE includes two hardware appliance components called the NitroSecurity IPS (also called "NitroSecurity Intrusion Protection System", or "IPS") and the NitroSecurity ESM (also called "NitroSecurity NitroView ESM", or "ESM", or "Enterprise Security Manager").

The TOE is an intrusion detection and prevention system that can detect network intrusion attempts and react by actively recording and/or blocking such attempts. The TOE can pass, drop, and log packets as they arrive, based on administrator-configurable rules. When the TOE is performing intrusion detection, it is said to be operating in an "IDS mode". When the TOE is performing intrusion prevention, it is said to be operating in an "IPS" mode.

The general concept of operation of the TOE in *an in-line network location operating in either an IPS mode or in an alerts-only mode* is depicted in the figure below:



The general concept of operation of the TOE in *an in-tap network location operating in an IDS mode* is depicted in the figure below:



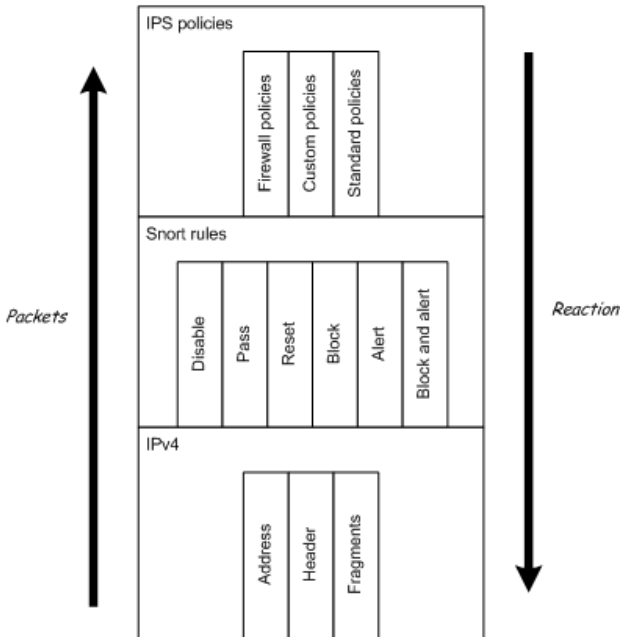
The remainder of this section summarizes the TOE architecture.

2.1 TOE Overview

The TOE passes, drops, and logs packets as they arrive, based on configurable rules. The TOE may be individually configured with rules, notification definitions, modes, variables and other parameters. There are three rule types:

- *Firewall Policy rules* include those the IPS will test against when a packet is examined.
- *Standard Policy rules* include deep-packet inspection rules that evaluate the contents of a packet and compare them with the signatures associated with the rule.
- *Custom Policy rules* include administrator-modified firewall and standard policy rules.

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

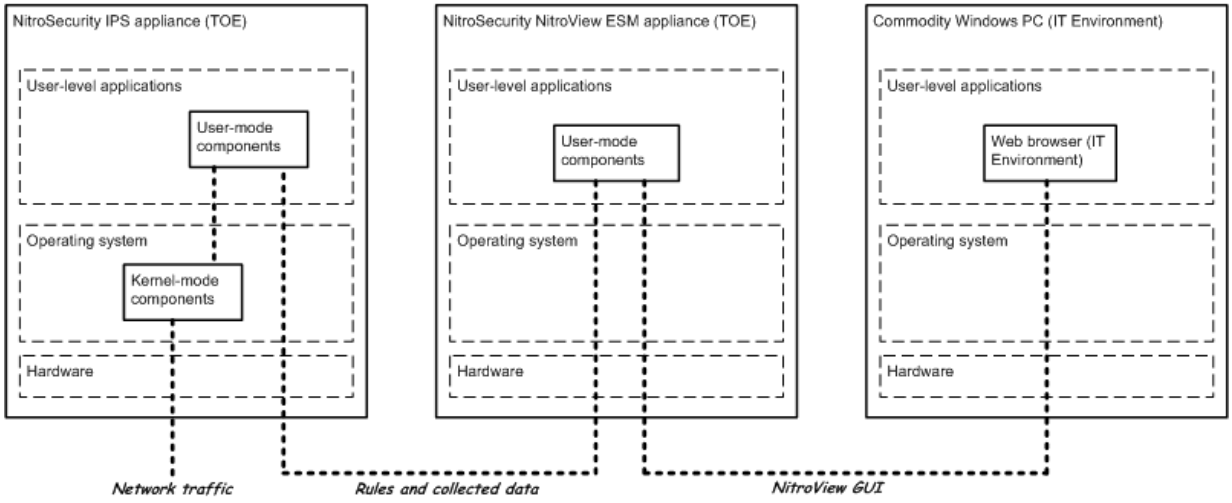


When a network packet enters the TOE through one of the physical network interfaces when the TOE is either in an in-line or an in-tap network location, the packet is first inspected using a packet-based firewall to look for any firewall rule matches (packet headers). If a match is found that will cause an alert, the firewall passes the information to a daemon in the alert module for logging to the alerts database. If the packet was not dropped, it is passed to the policy engine for deeper inspection (packet contents). The first policy engine check is done by a plug-in that determines if the packet is a control channel packet from the Enterprise Security Manager (ESM) destined for this Intrusion Protection System IPS. If it is, the packet is dropped, since processing of control channel packets is done by the support module, otherwise, it begins trying to match the policy rules. If a match is found, a direct connection is made to the alerts database in the alert module for logging. If the packet has gone through both firewall and deep packet inspection without being dropped, it is sent out of the TOE through the second physical interface of that traffic path.

2.2 TOE Architecture

The TOE can be described in terms of the following components:

- *NitroSecurity IPS* – A hardware appliance that provides network intrusion detection and prevention services for an enterprise type network. Includes the following components:
  - NitroSecurity hardware appliance
  - NitroSecurity Hardened Linux operating system
  - User- and Kernel-mode components that perform IDS and IPS functions
- *NitroSecurity ESM* – A hardware appliance that provides web-based administrator console interfaces that can be used to manage NitroSecurity IPS services and collected data that are accessible using a web browser in the IT Environment. Includes the following components:
  - NitroSecurity hardware appliance
  - NitroSecurity Hardened Linux operating system
  - User-mode components that provide web-based GUI administrative interfaces



The intended environment of the TOE can be described in terms of the following components:

- *Targeted IT systems* – send and receive monitored network traffic
- *Web browser* – used to access TOE administrative interfaces, including displaying alerts
- *SMTP, SNMP, syslog servers* – can receive alerts generated by the TOE
- *Certificate authority server* – Provides digital certificates to support the web-based GUI
- *NTP server* – Used to set TOE hardware clock (specifically, the ESM appliance clock)

The ESM appliance provides a GUI to administer the IPS. It is accessed using a web browser on a system in the IT Environment. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction. The administrator console can also be used to manage audit data and users. System data consists of results from IDS scanning, sensing, and analyzing tasks. The ESM appliance encrypts commands using a proprietary stackless control protocol sent from the ESM to the IPS. HTTPS is also used to protect the connection between the web browser in the IT Environment and the ESM appliance. The ESM offers HTTP v1.0 and v1.1 using SSL v2.0 and v3.0 or TLS v1.0 to web browsers. It is up to the web browser to request a particular combination of HTTP and SSL/TLS versions.

2.2.1 Physical Boundaries

The TOE consists of the following components:

- NitroSecurity IPS 7.1.3 running on supported appliance models
- NitroSecurity ESM 7.1.3 running on supported appliance models

2.2.2 Logical Boundaries

The security functions provided by the TOE include:

- Security audit
- Identification and authentication
- Security management
- TSF protection
- Intrusion detection

2.2.2.1 Security audit

Both IPS and ESM appliances generate audit records when security-relevant events occur. Auditable events generated by the IPS are sent at regular administrator-configured intervals for storage and review by the ESM appliance. Audit records are stored in an audit trail on the ESM appliance. The audit trail is physically protected by the ESM appliance hardware. The audit trail is protected from unauthorized logical access by restricting access to ESM web-based GUI interface that can read from the audit trail

See the corresponding section in the TSS for more detailed information.

2.2.2.2 Identification and authentication

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

See the corresponding section in the TSS for more detailed information.

2.2.2.3 Security management

The ESM appliance provides a GUI to administer the IPS appliance. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction. The administrator console can also be used to manage audit data and users. System data consists of results from IDS scanning, sensing, and analyzing tasks.

See the corresponding section in the TSS for more detailed information.

2.2.2.4 TSF protection

The TOE restricts access to its interfaces by requiring users to log into the ESM appliance using its GUI, and by encrypting commands sent from the ESM appliance to the IPS appliance. HTTPS is also used to protect the connection between the web browser in the IT Environment and the ESM appliance. The TOE relies on NitroSecurity appliance hardware in general to ensure the TSP is enforced and to provide for domain separation.

See the corresponding section in the TSS for more detailed information.

2.2.2.5 Intrusion detection

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

See the corresponding section in the TSS for more detailed information.

2.3 TOE Documentation

NitroSecurity offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of the system security features. Refer to Section 6.2 for information about these and other evidence assurance documents associated with the TOE.

3. Security Environment

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. There are no modifications to the security environment of the PP.

3.1 Assumptions

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

3.1.1 Intended Usage Assumptions

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

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

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

3.1.2 Physical Assumptions

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

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

3.1.3 Personnel Assumptions

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

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

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

3.2 Threats

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

3.2.1 TOE Threats

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

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

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

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

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

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

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

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

3.2.2 IT System Threats

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

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

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

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

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

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

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

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

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

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

3.3 Organizational Security Policies

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

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

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

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

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

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

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

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

4. Security Objectives

There are no modifications to the security objectives of the PP.

4.1 Information Technology (IT) 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.

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

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

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

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

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

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

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

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

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

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

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

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

4.2 Security Objectives for the IT Environment

This section identifies the security objectives of the TOEs supporting environment.

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

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

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

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

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

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

5. IT Security Requirements

5.1 TOE Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security Audit	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: Identification and Authentication	FIA_ATD.1: User Attribute Definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MTD.1: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions [1]
	FMT_SMR.1: Security Roles
FPT: Protection of the TOE Security Functions	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: IDS Component requirements	IDS_ANL.1: Analyzer analysis (EXP)
	IDS_RCT.1: Analyzer react (EXP)
	IDS_RDR.1: Restricted Data Review (EXP)
	IDS_SDC.1: System Data Collection (EXP)
	IDS_STG.1: Guarantee of System Data Availability (EXP)
	IDS_STG.2: Prevention of System data loss (EXP)

Table 1 TOE Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***basic***] level of audit; and c) [**Access to the System and access to the TOE and System data**].

[1] SFR added to address International Interpretation.

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	
FAU_STG.4	Actions taken due to the audit storage failure.	
FIA_UAU.2	All use of the authentication mechanism	User identity, location
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 2: Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST**, [the additional information specified in the Details column of Table 2 Auditable Events].**

5.1.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **[system administrators and general users that possess permissions that allow access]** with the capability to read **[all audit information]** 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.

Application note: Permissions that may be assigned general users by system administrators such as Event Management and Reporting permissions that allow access to audit information are defined in section 6.1.2.

5.1.1.3 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.4 Selectable Audit Review (FAU_SAR.3)

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***].

Application note: The administrator console interfaces that can be used to sort audit data do not include a separate type of event field. However, there is a "status" field provided by the administrator console that corresponds to IPS component status event types (which include critical, warning, and informational event types).

5.1.1.5 Selective Audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [***event type***;]
b) [**no additional attributes**].

5.1.1.6 Guarantees of Audit Data Availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.
FAU_STG.2.2 The TSF shall be able to [***detect***] unauthorized modifications to the audit records.
FAU_STG.2.3 The TSF shall ensure that [**the most recent, limited by available storage space**] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***]**.**

5.1.1.7 Prevention of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall **[*overwrite the oldest stored audit records*]** and **[send an alarm]** if the audit trail is full**.**

Application note: Actions the TOE takes if the audit trail becomes full are defined in section 6.1.1.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [
a) User identity;
b) Authentication data;
c) Authorisations
d) Groups
e) Alarm notification data].

5.1.2.2 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.3 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.3 Security Management (FMT)

5.1.3.1 Management of Security Functions Behavior (FMT_MOF.1)

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**].

Application note: Authorized System administrators in this instance refers to general users that have been assigned permissions such as Add/Delete Devices and Add/Delete Policies permissions that allow changing configuration options of the System that are defined in section 6.1.2.

5.1.3.2 Management of TSF Data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***query*** [**and add System data and audit data, and shall restrict the ability to query and modify all other TOE data**] to [**authorized administrators**].

5.1.3.3 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a.) **Add/Delete general users – Add/remove general user accounts**
b.) **Assign/Remove general user permissions – Assign/remove permissions to/from general user accounts**
c.) **Add/Delete Devices - Add/remove IPS devices to/from the system.**
d.) **Add/Delete Policies - Add/remove rule policies to/from the system.**
e.) **Custom Rules and Variables - Add, modify and delete custom rules and variables.**
f.) **Device Management - Configure settings and perform operations on IPS devices.**
g.) **ESM Configuration - Configure settings and perform operations on the ESM device.**
h.) **Event Management - Management of alert and flow data in addition to all rights of Reporting.**
i.) **Notifications - Add, modify and delete notifications and event forwarding destinations.**
j.) **Policy Administration - Manage policy settings for IPS devices.**
k.) **Reporting - Execute reports and retrieve alert, flow and log data from the IPS devices.**
l.) **System Management - Configure system wide settings.**
m.) **View Management - Add, modify and delete views in addition to all rights of Reporting.]**

5.1.3.4 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the **following** roles **[authorized administrator, authorized System administrators, and [general users]]**.

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

Application note: The authorized administrator role corresponds to the single system administrator account that can be used to create general user accounts. The authorized System administrator role corresponds to general user accounts that have been assigned one or more permissions by the authorized administrator. The general user role corresponds to general user accounts that have not been assigned any permissions by the authorized administrator.

5.1.4 Protection of the TOE Security Functions (FPT)

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

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

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

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.4.3 TSF domain separation (FPT_SEP.1)

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.

5.1.4.4 Reliable time stamps (FPT_STM.1a)

FPT_STM.1a.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.5 IDS Component requirements (EXP)

5.1.5.1 Analyzer analysis (EXP) (IDS_ANL.1)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:
a) **[*signature*]**; and
b) **[the following additional traffic analysis techniques:**
- **Protocol anomaly analysis**
- **Behavioral anomaly analysis**
- **Stateful protocol analysis]**. (EXP)

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:
a) Date and time of the result, type of result, identification of data source; and,
b) **[no additional information about the result]** (EXP)

5.1.5.2 Analyzer react (EXP) (IDS_RCT.1)

IDS_RCT.1.1 The System shall send an alarm to [**one or more of the following alarm destinations:**
a) **Administrator console**
b) **Email**
c) **Syslog**
d) **SNMP]**
and take [**one or more of the following actions:**
a) **Drop packet**
b) **Drop session**
c) **TCP reset**
d) **Log packet data**]
when an intrusion is detected. (EXP)

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

IDS_RDR.1.1 The System shall provide [**system administrators and general users that possess permissions that allow access**] with the capability to read [**all System data**] from the System data. (EXP)

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

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

Application note: Permissions that may be assigned general users by system administrators such as Event Management and Reporting permissions that allow access to audit information are defined in section 6.1.2.

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

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):
a) **[*network traffic*]**; and
b) [**no other defined events**] (EXP)

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 the following table, System Events. (EXP)

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address

Table 3: System Events

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

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion. (EXP)
IDS_STG.1.2 The System shall protect the stored System data from modification. (EXP)
IDS_STG.1.3 The System shall ensure that **[the most recent, limited by available storage space]** System data will be maintained when the following conditions occur: ***[System data storage exhaustion]***. (EXP)

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

IDS_STG.2.1 The System shall **[*overwrite the oldest stored System data*]** and send an alarm if the storage capacity has been reached.

5.2 IT Environment Security Functional Requirements

This section defines the security functional requirements for the IT Environment against which the TOE has been evaluated. Requirements have been copied from version 2.3 of the applicable Common Criteria documents

Requirement Class	Requirement Component
FPT: Protection of the TSF	FPT_STM.1b: Reliable time stamps

5.2.1 Protection of the TSF (FPT)

5.2.1.1 Reliable time stamps (FPT_STM.1b)

FPT_STM.1b.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own **and TOE** use.

5.3 TOE Security Assurance Requirements

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.3: Authorisation controls
	ACM_SCP.1: TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.2: Security enforcing high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 4 EAL 3 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Authorisation controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.3.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.8c The CM plan shall describe how the CM system is used.
ACM_CAP.3.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 TOE CM coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

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

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

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

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

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

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

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1c The presentation of the high-level design shall be informal.
ADV_HLD.2.2c The high-level design shall be internally consistent.
ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

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

ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

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

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.

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

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

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

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.

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

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

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

5.3.5 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.
ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.
ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
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.

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

5.3.6.4 Independent testing - sample (ATE_IND.2)

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

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.
AVA_MSU.1.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

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

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.
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.
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.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
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.

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.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security Audit

Both IPS and ESM appliances generate a log containing audit event information:

- *event log* – these are events not relating to alerts and traffic, such as management events, i.e. this is the audit log
  - Generated by both ESM (when using GUI) and IPS (when receiving commands from ESM)[2]
  - Records generated by IPS are sent to ESM periodically in batches for storage and review on ESM
  - Maximum event log size on both IPS and ESM is one million records on all supported IPS and ESM appliance models

The ESM provides web-based GUI interfaces to configure auditable events. Events are grouped into categories that correspond to sets of ESM GUI dialogs, menus, and screens which can be turned on or off as follows:

- Authentication category
- Backup category
- Blacklist category
- Device category
- Event Forwarding category
- Health Monitor category
- Notifications category
- Policy category
- Rule Server category
- System category
- Views category

The auditable event types include:

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	
FAU_STG.4	Actions taken due to the audit storage failure.	
FIA_UAU.2	All use of the authentication mechanism	User identity, location
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	User identity, location
FMT_MOF.1	All modifications in the behavior of the	

[2] *Auditable events generated by both IPS and ESM : Database backup, Sending blacklist entries to device, Event forwarding errors, Device alert retrieval, Device flow retrieval, Device log retrieval, Auto learn retrieval, Notification errors, Apply policy to device, Rules and software download, Appliance health type events.*

Component	Event	Details
	functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Each audit record includes date and time of the event, type of event, subject (i.e. administrative user for administrator console-initiated actions, or IPS or ESM components if IPS or ESM appliance-initiated action) identity, and the outcome (success or failure) of the event. The subject identity is found in the name field, the event type is replaced by status (critical, warning, and informational) and the outcome is the description field. Events in the separate logs can be correlated by subject identity. The audit trail is physically protected by the ESM runtime hardware. The audit trail is protected from unauthorized logical access by restricting access to ESM web-based GUI interface that can read from the audit trail. There are no interfaces (not ESM web-based GUI interfaces or otherwise) to modify audit records stored in the audit trail.

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

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

- FAU_GEN.1: The TOE generates audit events for the basic level of audit. Note that the IDS_SDC and IDS_ANL requirements address the recording of results from IDS scanning, sensing, and analyzing tasks (i.e., System data).
- FAU_SAR.1: The TOE provides administrator console interfaces that can be used by authorized administrators and general users that possess permissions that allow access to read the audit trail.
- FAU_SAR.2: The TOE restricts access to the audit trail to authorized administrators and general users that possess permissions that allow access to read the audit trail using administrator console interfaces.
- FAU_SAR.3: The TOE provides administrator console interfaces that can be used to sort audit data. The administrator console interfaces that can be used to sort audit data do not include a separate type of event field. However, there is a “status” field provided by the administrator console that corresponds to IPS component status event types (which include critical, warning, and informational event types).
- FAU_SEL.1: The TOE provides administrator console interfaces that can be include or exclude auditable events based on event type.
- FAU_STG.2: The TOE restricts administrator console interfaces that can be used to delete audit data. The TOE provides administrator console interfaces that can be used to detect modifications (administrators can compare system activity reports based on audit data generated at different points in time).
- FAU_STG.4: The TOE generates an alarm using a configured mechanism (see section 6.1.5 for a description of notification mechanisms), and begins overwriting the oldest stored audit records when the audit trail becomes full. Note that the TOE does not stop collecting or producing System data.

6.1.2 Identification and Authentication

There is a single system administrator account that can be used to create what are called general user accounts. The system administrator may grant general users other privileges by creating access groups and assigning users to these groups. However, there are operations such as creating general user accounts that only the system administrator account can perform even if a general user were to be assigned all available privileges. Group membership and the permissions assigned to the group by the administrator determine what ESM web-based GUI interfaces a user may access. The ESM appliance stores user account information on the ESM appliance. User account information is physically protected by the ESM runtime appliance hardware. User account information includes username, password, and group information.

Assignable permissions include:

- Add/Delete Devices - Add/remove IPS devices to/from the system.
- Add/Delete Policies - Add/remove rule policies to/from the system.
- Custom Rules and Variables - Add, modify and delete custom rules and variables.
- Device Management - Configure settings and perform operations on IPS devices.
- ESM Configuration - Configure settings and perform operations on the ESM device.
- Event Management - Management of alert and flow data in addition to all rights of Reporting.
- Notifications - Add, modify and delete notifications and event forwarding destinations.
- Policy Administration - Manage policy settings for IPS devices.
- Reporting - Execute reports and retrieve alert, flow and log data from the IPS devices.
- System Management - Configure system wide settings.
- View Management - Add, modify and delete views in addition to all rights of Reporting.

When a user attempts to log into the ESM web-based GUI interface, a username and password are required. The ESM appliance authenticates user identities using the entered passwords using its own password mechanism. The ESM web-based GUI interface provides interfaces for users to change their own passwords. The ESM appliance requires passwords to be at least eight characters from the printable character set. Passwords must also include at least one uppercase letter, one punctuation mark, and one digit. The ESM appliance GUI enforces these password composition rules.

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

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

- FIA_ATD.1: The TOE maintains user identities, authentication data, authorization, group information, and alarm notification data.
- FIA_UAU.2: The TOE offers no TSF-mediated functions until the user is authenticated. Note that the password mechanism can meet or exceed SOF-basic when passwords of certain lengths are used.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

6.1.3 Security Management

The ESM appliance provides a GUI to administer the IPS appliance. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction. The administrator console can also be used to manage audit data and users. System data consists of results from IDS scanning, sensing, and analyzing tasks. Management functions correspond to the list of assignable permissions that can be found in section 6.1.2, and also include the functions of creating general users and assigning them permissions by the system administrator.

The TOE has two types of user accounts: system administrator and general user. The system administrator may grant general users other privileges by creating access groups and assigning users to these groups. The system administrator is the only user that has access to all areas of the system. Users must be added to the system to have access to TOE and its devices, policies, and their associated privileges. The system administrator is considered the authorized administrator. General users are considered the authorized System administrators.

The TOE restricts access to its interfaces by requiring users to log into the ESM appliance using its GUI, and by encrypting commands sent from the ESM appliance to the IPS appliance. HTTPS is also used to protect the connection between the web browser in the IT Environment and the ESM appliance.

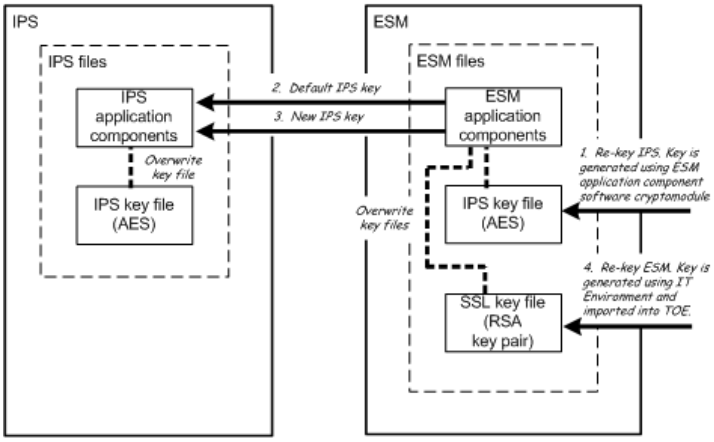
The Security management function is designed to satisfy the following security functional requirements:

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

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

6.1.4 Protection of the TSF

The TOE restricts access to its interfaces by requiring users to log into the ESM appliance using its GUI, and by encrypting commands sent from the ESM appliance to the IPS appliance. HTTPS is also used to protect the connection between the web browser in the IT Environment and the ESM appliance. The ESM supports HTTP v1.0 and v1.1 using SSL v2.0 and v3.0 or TLS v1.0. The TOE relies on NitroSecurity appliance hardware to ensure the TSP is enforced and to provide for domain separation. The TOE additionally encrypts communication between Console and IPS appliances using a proprietary stackless control protocol called SEM (Secure Encrypted Management), which uses encrypted commands packaged in packet payloads, together with a specific token in the payload that indicates the packet is a control packet.



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

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

- FPT_ITT.1: The TOE encrypts commands sent from the ESM appliance to the IPS appliance. HTTPS is also used to protect the connection between the web browser in the IT Environment and the ESM appliance.
- FPT_RVM.1, FPT_SEP.1: The TOE maintains a security domain by relying on its implementation as a appliance hardware. Its hardware appliance component protects the TOE from external physical interference or tampering, including providing separate physical interfaces to separate network traffic.
- FPT_STM.1: The TOE hardware appliance includes its own hardware clock which provides reliable time stamps for use in audit and collected data records. The TOE clock may be set using an NTP server in the IT Environment.

6.1.5 Intrusion detection (EXP)

The IPS is an Open System Interconnection (OSI) Layer 2 device and does not have an IP address. The device will not respond to pings, traceroutes, or any other high level mechanics, nor will it respond to ARP requests or any other low level mechanics. The TOE can be installed in the following locations in the network architecture of the IT environment:

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

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

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

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

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

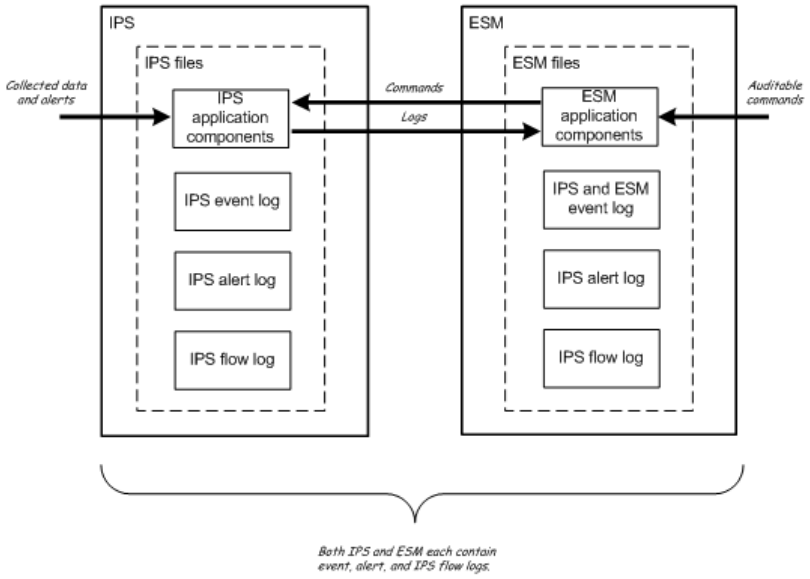
When the TOE is located in-tap it can operate in what is called an *IDS mode*. IDS mode (also called passive operating mode) consists of the TOE being located in-tap while functioning as an IDS, i.e. the TOE can monitor network traffic but not affect it. The IPS is placed on a span port of a switch using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

The TOE performs signature analysis, protocol anomaly analysis, behavioral anomaly analysis, and stateful protocol analysis on collected network traffic data and records corresponding network traffic event data when operating in any one of its operating modes.

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

Administrator console provides the ability to examine analytical conclusions drawn by the TOE that describe the conclusion and identifies the information used to reach the conclusion. Both IPS and ESM appliances generate two types of logs to store collected data event information:

- *traffic alert log* – these are events that occur when packets match a rule, i.e. this is collected data
  - Records generated by IPS are sent to ESM periodically in batches for storage on ESM
  - Maximum log size on both IPS and ESM depends on appliance model:
    - Maximum traffic alert log size on all supported IPS models is ten million records
    - Maximum traffic alert log size on supported ESM models depends on model, ranging from 250 million to 750 million records.
- *traffic flow log* – these are events that occur when connections are made between targeted IT systems in general (i.e. a flow is not associated with an IDS rule), i.e. this is collected data
  - Records generated by IPS are sent to ESM periodically in batches for storage on ESM
  - Maximum log size on both IPS and ESM depends on appliance model:
    - Maximum traffic alert log size on all supported IPS models is ten million records
    - Maximum traffic alert log size on supported ESM models depends on model, ranging from 250 million to 750 million records.



The TOE generates alarms based on rules that are triggered by packet decoding and detection processing. The IPS receives a request for alerts from the ESM containing the date of the last retrieved alert. All alerts since the date passed are retrieved and passed back to the ESM. The IPS can also be configured to automatically send out Syslog messages and SNMP traps when an alert is triggered. The IPS receives configuration data for Syslog servers and SNMP managers from the ESM, including an alert rate. This data is used for sending Syslog messages and SNMP traps whenever an alert is logged, not to exceed the specified rate. The IPS can generate email (including email for pagers) SNMP traps, syslog, and text log files. The alarm mechanisms used when reacting to collected data may also be used when reacting to audit mechanism events, if the TOE has been configured to do so.

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

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

- IDS_SDC.1: The TOE collects network traffic data for use in scanning, sensing, and analysing functions, acting as an IDS sensor. Note that different types of network traffic can be collected depending on the TOE's location within a network. Also note that host-based events may be collected for network switches.
- IDS_ANL.1: The TOE performs signature analysis, protocol anomaly analysis, behavioral anomaly analysis, and stateful protocol analysis on collected network traffic data and records corresponding network traffic event data when operating in any one of its operating modes (active mode, stealth mode, or passive mode). Note that the administrator console provides the ability to examine analytical conclusions drawn by the TOE that describe the conclusion and identifies the information used to reach the conclusion.
- IDS_RCT.1: The TOE provides the ability to generate alarms and notify an authorized administrator using a configured notification mechanism when an intrusion is detected. The TOE also provides the ability to automatically pass or reject packets (and connections) based on rule configuration when an intrusion is detected.
- IDS_RDR.1: The TOE provides authorized administrators and general users that possess permissions that allow access the ability to review results from IDS scanning, sensing, and analysing tasks (i.e., System data) using the administrator console.
- IDS_STG.1: The TOE ensures that the most recent system data is always able to be recorded, when the system data storage space is exhausted, the oldest events stored in the system data store will be overwritten.
- IDS_STG.2: The TOE prevents loss in new/current event data by overwriting the oldest events stored in the log when the system data storage capacity is exhausted. When this occurs and alarm is generated and sent to the authorized administrator using a configured notification mechanism.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by NitroSecurity ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. NitroSecurity ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. NitroSecurity performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, configuration management documentation, and security flaws.

These activities are documented in:

- NitroSecurity Intrusion Prevention System Version 7.1.3 Configuration Management. Plan

The Configuration management assurance measure satisfies the following EAL 3 assurance requirements:

- ACM_CAP.3

- ACM_SCP.1

6.2.2 Delivery and operation

NitroSecurity provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. NitroSecurity's delivery procedures describe all applicable procedures to be used to detect modification to the TOE. NitroSecurity also provides documentation that describes the steps necessary to install NitroSecurity appliances in accordance with the evaluated configuration.

These activities are documented in:

- NitroSecurity NitroView Installation and Setup Guide Release 7.1.3, part number NS-75602002713

The Delivery and operation assurance measure satisfies the following EAL 3 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

NitroSecurity has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- NitroSecurity 7.1.3 Design Document

The Development assurance measure satisfies the following EAL 3 assurance requirements:

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

6.2.4 Guidance documents

NitroSecurity provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- NitroSecurity NitroView User Guide Release 7.1.3, part number NS-75602001713

The Guidance documents assurance measure satisfies the following EAL 3 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

NitroSecurity ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. NitroSecurity applies security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure development of the TOE. NitroSecurity has a documented model of the TOE life cycle that ensures that the TOE is developed and maintained in a well-defined manner.

These activities are documented in:

- NitroSecurity 7.1.3 Life Cycle Document

The Life cycle support assurance measure satisfies the following EAL 3 assurance requirements:

- ALC_DVS.1

6.2.6 Tests

NitroSecurity has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. NitroSecurity has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- NitroSecurity - Test Plan
- NitroSecurity - Test Coverage Analysis
- NitroSecurity - Test Results

The Tests assurance measure satisfies the following EAL 3 assurance requirements:

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

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of the TOE and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. Furthermore, NitroSecurity has conducted a misuse analysis demonstrating that the provided guidance is complete.

NitroSecurity has conducted a SOF analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum SOF claim: SOF-Basic.

NitroSecurity performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- NitroSecurity - Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following EAL 3 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

The TOE conforms to IDSSPP.

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

This Security Target includes all of the Security Objectives from the PP, verbatim. Additionally, OE.TIME which was added per the IDSSPP errata sheet

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

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FAU_GEN.1	No changes.
FAU_SAR.1	*Assignment* – completed the assignment.
FAU_SAR.2	No changes.
FAU_SAR.3	No changes.
FAU_SEL.1	No changes.
FAU_STG.2	*Selection* – completed the selection. *Assignment* – completed the assignment.
FAU_STG.4	*Selection* – completed the selection. *Assignment* – completed the assignment.
FIA_AFL.1	*Removed* – the requirement was removed from the ST since the TOE does allow or support access from external IT products. Reference OD-0217/PD-0097.
FIA_ATD.1	*Assignment* – completed the assignment.
FIA_UAU.2	*Replaced* – the requirement was removed from the ST and replaced with FIA_UAU.2 given no mediated functions are otherwise available.
FIA_UID.2	*Replaced* – the requirement was removed from the ST and replaced with FIA_UID.2 given no mediated functions are otherwise available.
FMT_MOF.1	No changes.
FMT_MTD.1	*Assignment* – completed the assignment.
FMT_SMF.1	This requirement was added in this Security Target to satisfy FMT_MTD.1 and FMT_MOF.1 dependencies.
FMT_SMR.1	*Assignment* – completed the assignment.
FPT_ITA.1	*Removed* – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable. . Reference PD-0097
FPT_ITC.1	*Removed* – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable. Reference PD-0097
FPT_ITI.1	*Removed* – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable. Reference PD-0097
FPT_ITT.1	This requirement was added in this Security Target given that the TOE can protect communication between its components.
FPT_RVM.1	No changes.
FPT_SEP.1	No changes.

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FPT_STM.1a	No changes.
FPT_STM.1b	This requirement was added in this Security Target given that the TOE hardware clock can be set using an NTP server in the IT Environment.
IDS_ANL.1	*Selection* – completed the selection. *Assignment* – completed the assignment.
IDS_RCT.1	*Assignment* – completed the assignment.
IDS_RDR.1	*Assignment* – completed the assignment.
IDS_SDC.1	*Selection* – completed the selection. *Assignment* – completed the assignment.
IDS_STG.1	*Selection* – completed the selection *Assignment* – completed the assignment.
IDS_STG.2	*Selection* – completed the selection.

8. Rationale

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

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

There are no modifications to the security objectives of the PP.

The security objective rationale is presented in Section 7.1 and Section 7.2 of the IDSSPP. Additionally, OE.TIME which was added per the IDSSPP errata sheet, maps to the P.ACCACT and P.DETECT policies which require audit and system data to be generated and include a timestamp.

All of the assumptions, threats, and security objectives have been reproduced from the IDSSPP to this ST.

8.2 Security Requirements Rationale

The security requirements rationale is presented in Section 7.3 of the IDSSPP.

All of the security functional requirements have been reproduced from the IDSSPP to this ST, except as noted below:

The following security functional requirements were added to the ST:

- FIA_UAU.2: Added given no mediated functions are available prior to login.

- FIA_UID.2: Added given no mediated functions are available prior to login.
- FMT_SMF.1: Added to address FMT_MTD.1 and FMT_MOF.1 dependencies.
- FPT_ITT.1: Added to reflect product functionality

The following security functional requirements were removed from the ST:

- FIA_AFL.1: Removed from the ST since the TOE does allow or support access from external IT products
- FIA_UAU.1: Removed from the ST since no mediated functions are available prior to login.
- FIA_UID.1: Removed from the ST since no mediated functions are available prior to login.
- FPT_ITA.1: Removed from the ST since the TOE does not transmit data to external IT products, and therefore this requirement is not applicable
- FPT_ITC.1: Removed from the ST since the TOE does not transmit data to external IT products, and therefore this requirement is not applicable
- FPT_ITI.1: Removed from the ST since the TOE does not transmit data to external IT products, and therefore this requirement is not applicable

The additional SFRs map to existing objectives as follows:

- FMT_SMF.1: Maps to O.EADMIN to summarize provided admin functions.
- FPT_ITT.1: Maps to O.EXPORT to protect communication between TOE components
- FPT_STM.1b: Maps to OE.TIME to provide a reliable time stamp to the TOE.

8.3 Security Assurance Requirements Rationale

NitroSecurity has elected to pursue a more rigorous assurance level, increased from EAL2 as specified in IDSSPP to EAL3, as specified in section 1.2 of this ST. The TOE meets all the IDSSPP Functional Requirements as so stated for EAL2. EAL3 was selected as the assurance level because the TOE is a commercial product whose users require a moderate to high level of independently assured security. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL3 is appropriate to provide the assurance necessary to counter the limited potential for attack.

8.4 Strength of Functions Rationale

There are no modifications to the strength of function claimed in the PP. The relevant security functional requirement is FIA_UAU.2. The intent is that the password mechanism meets or exceeds SOF-basic and the evidence can be found in the strength of function analysis.

The strength of functions rationale is presented in Section 7.6 of the IDSSPP.

8.5 Requirement Dependency Rationale

There are no modifications to the security requirements of the PP with the exception of the following additions:

- FMT_SMF.1
- FPT_ITT.1
- FPT_STM.1b

The above addition does not introduce any additional dependencies.

The SFR dependency rationale is presented in Section 7.7 of the IDSSPP.

The following table demonstrates that all dependencies among the claimed security requirements are satisfied for EAL3 and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ACM_CAP.3	ALC_DVS.1	ALC_DVS.1
ACM_SCP.1	ACM_CAP.3	ACM_CAP.3
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ALC_DVS.1	none	none
ATE_COV.2	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_DPT.1	ADV_HLD.1 and ATE_FUN.1	ADV_HLD.2 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_MSU.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.2
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.2 and AGD_ADM.1 and AGD_USR.1

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements beyond those in the PP.

The explicitly stated requirements rationale is presented in Section 7.5 of the IDSSPP.

8.7 TOE Summary Specification Rationale

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

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. The table below demonstrates the relationship between security requirements and security functions.

	Security Audit	Identification and Authentication	Security Management	Protection of the TOE Security Functions	IDS COMPONENT REQUIREMENTS (IDS)
FAU_GEN.1	**x**				
FAU_SAR.1	**x**				
FAU_SAR.2	**x**				
FAU_SAR.3	**x**				
FAU_SEL.1	**x**				
FAU_STG.2	**x**				
FAU_STG.4	**x**				
FIA_ATD.1		**x**			
FIA_UAU.2		**x**			
FIA_UID.2		**x**			
FMT_MOF.1			**x**		
FMT_MTD.1			**x**		
FMT_SMF.1			**x**		
FMT_SMR.1			**x**		
FPT_RVM.1				**x**	
FPT_SEP.1				**x**	
FPT_STM.1				**x**	
IDS_ANL.1					**x**
IDS_RCT.1					**x**
IDS_RDR.1					**x**
IDS_SDC.1					**x**
IDS_STG.1					**x**
IDS_STG.2					**x**

Table 5 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.