NIKSUN®, Inc.

NetDetector®/NetVCR® 2005

Security Target

Document ID

NK-CC-ST-NDV2005-1.5

Date

February 18, 2005

Author(s)

Darryle Merlette, CISSP

NIKSUN, Inc.

WWW.NIKSUN.COM

Table of Contents

1 Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the NIKSUN® NetDetector®/NetVCR® 2005 Target of Evaluation (TOE). It is based on the *Common Criteria for Information Technology Security Evaluation (CC), Version 2.1* , the ISO/IEC JTC 1/SC 27 N, *Guide for the Production of Protection Profiles and Security Targets, Version 0.9*, and all interpretations through March 15, 2004. The language used is consistent with the CC, hence spelling conforms to internationally accepted English.

1.1 Security Target Identification

This section contains labeling and descriptive information for the ST and TOE to which it refers.

1.1.1 Security Target Name

NIKSUN NetDetector/NetVCR 2005 Security Target v1.5, February 18, 2005, authored by Darryle Merlette, CISSP.

1.1.2 TOE Reference

NIKSUN NetDetector/NetVCR 2005 build 3.1sp2_3.

1.1.3 Evaluation Assurance Level

Evaluation Assurance Level (EAL) 2.

1.2 Security Target Overview

This Security Target defines the requirements for the NIKSUN NetDetector/NetVCR appliance Version 2005 TOE. NIKSUN appliances are network-based monitors that consist of a hardware platform upon which various software platform and application modules are loaded[1]. The platform allows a coherent set of CC compliant functional security requirements to be satisfied. In addition, the analysis functions provided by the application modules allow for a set of explicitly stated functional requirements to also be claimed. These modules have application to network security (eg., intrusion and anomaly detection and detailed network forensics) as well as network performance (eg., quality of service (QoS) metrics, capacity planning, and real-time/post-event network troubleshooting). Hence, the NetDetector/NetVCR

[1] The application software modules come preloaded on an appliance and are not sold separately.

2005 TOE represents a full-function appliance that consolidates applications for security and performance, in a single solution. The NIKSUN product line also includes separate appliances for security and performance (NetDetector and NetVCR respectively) which each represent a functional subset of the TOE, but they are not being individually evaluated.

A NIKSUN appliance will passively and non-intrusively record all packets from a monitored network while simultaneously generating and storing multi-level statistics which enable "drill-down" analysis from the link layer to the application layer. The NetDetector/NetVCR application modules utilize the warehoused data to perform advanced features such as statistical anomaly/QoS detection, security and performance signature detection, application and session reconstruction (web, email, IM, FTP, Telnet), scheduled or on-demand reporting, and multi-format data import/export. A web-based graphical user interface (GUI) provides a convenient standard client access to the management, configuration, and application features[2].

In order to provide a mapping between the Security Environment and the Security Requirements of NIKSUN NetDetector/NetVCR 2005, this document includes the following sections:

- Section 1: Security Target Introduction – This is the current section which introduces and identifies the components and layout of the ST.
- Section 2: TOE Description – This section provides an overview of the TOE security functions, the TOE architecture, and the physical and logical boundaries.
- Section 3: TOE Security Environment – This section describes the assumptions, threats, and policies which impact the TOE and its environment.
- Section 4: Security Objectives – This section details the security objectives that are satisfied by the TOE and its operating environment.
- Section 5: IT Security Requirements – This section presents the Security Functional Requirements (SFRs), explicitly stated requirements, and the Security Assurance Requirements (SARs) that are met by the TOE.
- Section 6: TOE Summary Specification – This section describes how the TOE satisfies the IT Security Requirements and objectives.
- Section 7: Protection Profile Claims – This section includes any conformance claims to registered

[2] There is also a command line interface (CLI) for initial setup and selected administrative tasks. See Section 2 for how the CLI is restricted in the evaluated configuration.

Protection Profiles.

- Section 8: Rationale – This section demonstrates the consistency, completeness, and suitability of the security objectives, requirements, and summary specification.

1.3 Conformance Claims

1.3.1 Common Criteria Conformance

The NIKSUN NetDetector/NetVCR 2005 TOE is compliant with the Common Criteria (CC) Version 2.1, functional requirements (Part 2) extended, conformant to Part 3 and the assurance package selected is EAL 2 Conformant. EAL 2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of a readily available and complete development record. It provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

1.3.2 Protection Profile Conformance

The NIKSUN NetDetector/NetVCR 2005 TOE does not claim conformance to any registered Protection Profiles (PP).

1.4 Conventions

The CC allows several operations to be performed on security requirements; **refinement**, **selection**, **assignment**, and **iteration** are defined in paragraph 2.1.4 of Part 2 of the CC. Assignment, selection, and iteration are used in this ST.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by <u>underlined text</u>.

The **iteration** operation is used when a component is repeated with varying operations. Iterations are noted by following the requirement with an iteration number enclosed in parentheses: eg. FAU_SAR.1(**2**). The title of the component is also appended with ".<iteration #>".

1.5 Terminology

The following terminology is used throughout this ST (Acronyms are defined in Section 9):

Administrator – Highest level role through the GUI.

Advanced User – Intermediate level role through the GUI.

Appliance User – Basic level role through the command line.

group – A defined set of privileges/permissions to which users can be assigned.

management interface – The network interface through which remote (GUI) access occurs.

monitoring interface – The passive network interface that records network traffic.

recording interface – Same as monitoring interface.

role – Same as group.

root – The main default Superuser account on the command line.

Superuser – The highest authority administrative group on the command line.

User – Low level role through the GUI.

vcr – The default Appliance User account on the command line.

2 TOE Description

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

2.1 Product Type and Architecture

The NIKSUN NetDetector/NetVCR 2005 is a network surveillance and analysis product for security and performance monitoring. A NetDetector/NetVCR 2005 appliance is composed of the following parts:

- Data Capture Engine
- User Interface Engine
- Application Modules
    - Security: Reconstruction, Anomaly, Signature

    AND

    - Performance: QoS, RTX

The Data Capture Engine (DCE) provides the core platform that collects data packets from tapped networks and stores them to disk. It simultaneously computes statistical metadata and stores that information to disk as well. Executables to query the data (for use by the User Interface Engine and Application Modules) are also included. The DCE is based on a custom-built, hardened version of the

FreeBSD operating system. In terms of TOE security functions, the DCE plays a key role in system and audit data collection and availability, protection of system and audit data, the CLI, analysis, reaction, and time stamps.

The User Interface Engine (UIE) is responsible for all static and dynamic content related to the GUI. This includes such sub-components as the web server, CGI engine, servlet engine, and applets. Screens related to Configuration, Traffic Analysis, Event Viewing, and Data Management are under direct control of the UIE. Much of the data presented in these screens result from queries to the DCE. The UIE also provides the engine that allows application-specific screens to be rendered. Since the GUI is the primary means of interacting with the product following installation, the UIE is also responsible for the main Identification and Authentication (I&A), Security Management, and audit review functionality.

The Application Modules provide more specific functionality which corresponds to the explicitly stated requirements in Section 5. These modules include Anomaly, Signature, Reconstruction, QoS and RTX.

Security modules:
The security modules – Anomaly, Signature, and Reconstruction – provide the NetDetector aspect of TOE functionality. The Anomaly module will track and alert on statistical thresholds defined by authorised users. It will take query results from the DCE and yield output for rendering by the UIE in the Event Viewer. It can also produce alerts via email and SNMP trap. The Signature module behaves similarly in that it takes query results from the DCE (in this case, raw packet data), looks for specific patterns on which to alert, and presents its output in the Event Viewer. The Signature module can also send out its alerts via Syslog. The Reconstruction module is a specialized component that allows TCP and network application session flows to be reconstructed from raw data derived from the DCE and rendered by the UIE as an application would present them. Complete web pages, emails with attachments, instant messaging sessions, FTP with data files, Telnet, and other ASCII based TCP sessions are handled by this module.

Performance modules:
The performance modules – QoS and RTX – provide the NetVCR aspect of TOE functionality. The QoS module tracks and alerts on statistical thresholds related to quality-of-service metrics as defined by authorised users. It queries the DCE and presents results in the Event Viewer via the UIE. It can send alerts via SNMP trap and Syslog. The RTX module (RTX stands for “Real Time eXperts”) reads packets from the DCE looking for performance-relevant patterns on which to trigger. Results are sent to the Event

Viewer and can also raise alerts via SNMP trap and Syslog.

Figure 1 depicts the appliance architecture which has been described here.

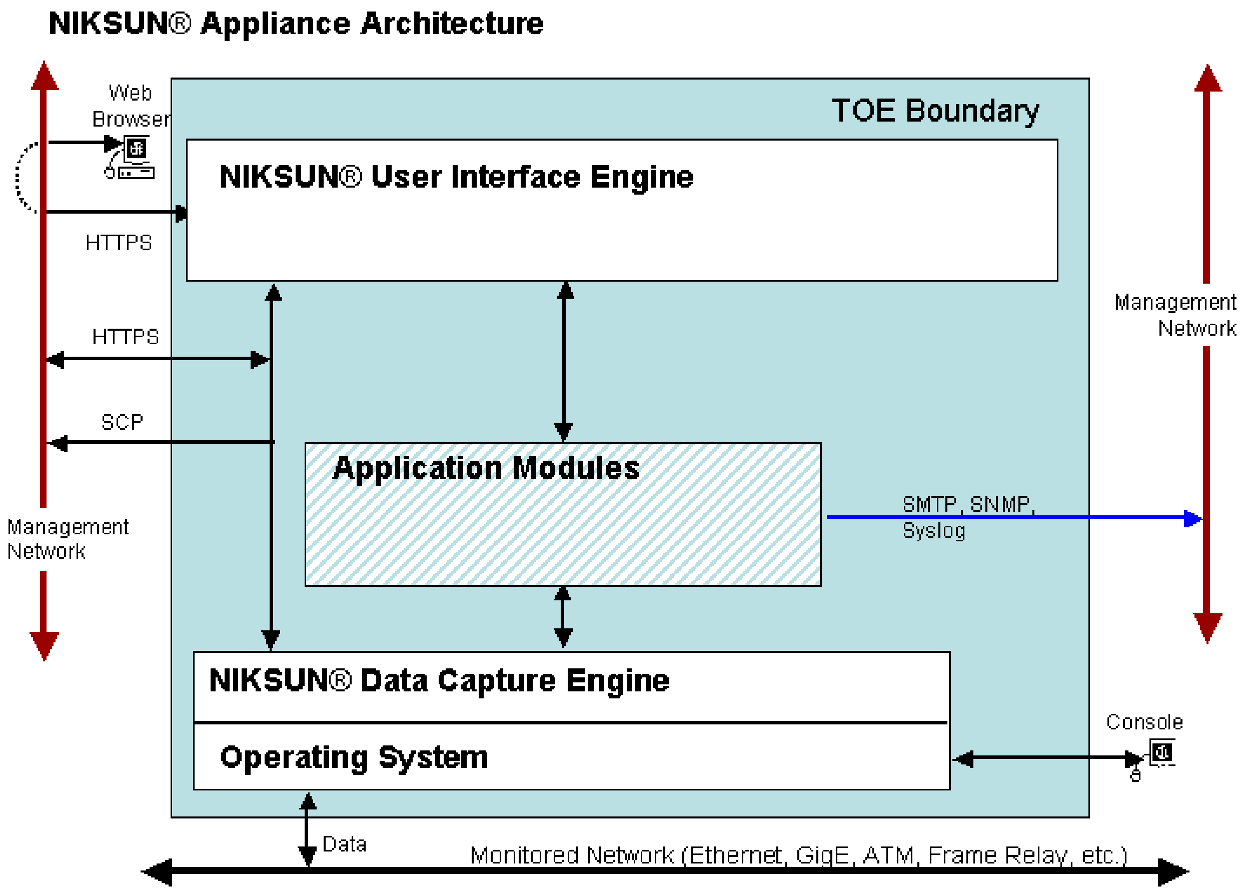
NIKSUN® Appliance Architecture
Web Browser
TOE Boundary
NIKSUN® User Interface Engine
HTTPS
HTTPS
SCP
Application Modules
Management Network
Management Network
SMTP, SNMP, Syslog
NIKSUN® Data Capture Engine
Operating System
Console
Data
Monitored Network (Ethernet, GigE, ATM, Frame Relay, etc.)

Figure 1 – NIKSUN Appliance architecture and TOE boundary.

2.2 Physical Scope and Boundary

The physical scope and boundaries of the TOE are defined by the physical boundaries of the NIKSUN Appliance. The appliance encapsulates all of the hardware items (eg., Intel motherboard, NICs, disks). The disks are preloaded with all of the software components (DCE, UIE, Application Modules) as well as the OS.

The client machine used for web access and the CLI console (keyboard and monitor) are outside the physical scope. The appliance and console are expected to be co-located along with the switches/hubs/taps to which the management and monitoring interfaces are connected. The web client may or may not be co-located.

Appliance:
NIKSUN appliances are available in several form factors depending on the type of network being monitored and the amount of storage desired: 1000/2000/5000 series.

The 1000-series appliances comprise a 1 unit (1 RU) rack-mountable chassis, a motherboard with a single CPU (at least 2.4 GHz), 1 GB RAM, Ethernet port, keyboard/monitor/mouse connectors, a single network interface card (NIC – could be multi-port) for monitoring, and 72 GB – 146 GB of disk storage.

The 2000-series appliances comprise a 2 RU rack-mountable chassis, a motherboard with a dual CPU (at least 2.4 GHz each), at least 2 GB RAM, Ethernet port, keyboard/monitor/mouse connectors, up to 2 NICs (could be multi-port) for monitoring, and 144 GB – 876 GB of disk storage.

The 5000-series appliances comprise a 5 RU rack-mountable chassis, a motherboard with a dual CPU (at least 2.4 GHz each), at least 2 GB RAM, Ethernet port, keyboard/monitor/mouse connectors, up to 4 NICs (could be multi-port) for monitoring, and 584 GB – 1.46 TB of disk storage.

SCSI, RAID, or Fibre Channel controllers can be used for managing storage[3]. NIC cards can be selected for tapping 10/100 Ethernet, Gigabit Ethernet, T1/E1, T3/E3/DS3, V.35/X.21, FDDI/HSSI, OC-3, or OC-12 networks. Specialised drivers in the DCE are responsible for reading data from the NICs and writing it to disk in real-time.

Regardless of the appliance hardware, all software loaded is identical and built from common source code trees.

2.3 Logical Scope and Boundary

The logical boundary of the TOE includes all the NIKSUN components that reside within the physical boundary, as depicted in the shaded area of Figure 1, as well as the interfacing components. The logical components include the web-based GUI, the CLI, and the appliance itself. The behaviour of both the GUI

[3] Fibre Channel controller is reserved for external storage, which can go well beyond the 1.46 TB limit imposed by the internal appliance. This configuration is not part of the evaluation.

and CLI is determined by the appliance software, which in turn depends on the execution environment provided by the OS. The custom-built OS is based on FreeBSD 4.2. In addition to NIC and other device drivers, the OS provides such services as bootup, initialization, file system, process scheduling, auditing, time stamps, and TCP/IP stack and protocol implementation.

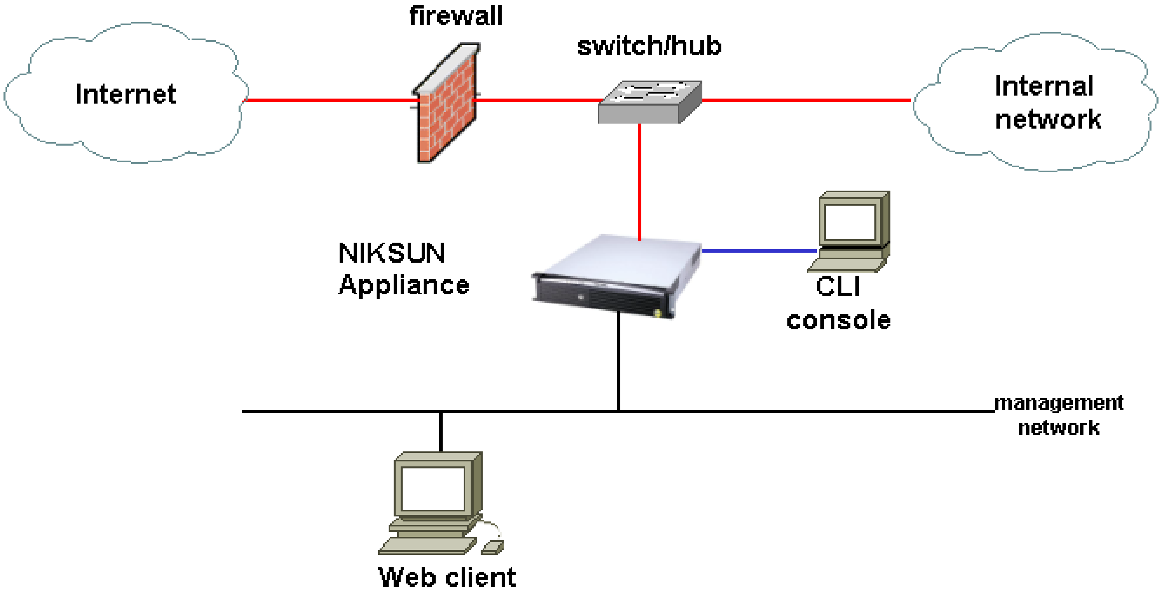

Figure 2 – Evaluated TOE Configuration

The evaluated configuration for the TOE is shown in **Figure 2**. In this configuration a 2U appliance (NKN-2411-FE-2HDX-292 featuring dual CPUs, 2 GB RAM, 10/100 Ethernet Management Interface, CD-ROM and Floppy Drives with 292 GB Storage configured for monitoring 2 HDX Fast Ethernet links) has a management interface attached to a separate and secured management network shared by the web client, and a recording interface that is plugged into a hub or the span/mirrored port of a switch through which traffic to/from the Internet and internal network flows. This represents one of the most typical configurations utilised in practice.

Web Client:

The web client machine can be any workstation running Windows 2000 and a Java-enabled browser (IE/Netscape 6.x) with Java plug-in 1.4.1. In addition, Javascript and Cookies should be enabled and the browser should be configured to not load from its cache.

Console:
The console is a standard PC monitor and keyboard attached to the appropriate connectors on the appliance.

The following items are also capabilities of NIKSUN appliances, but are outside the scope of the evaluated configuration:

- External authentication with TACACS+ and RADIUS servers.
- Remote access to the CLI through the management interface via SSH, Telnet, and FTP.
- Internal RAID controller.
- External SAN storage via Fibre Channel.
- Time synchronising with an external NTP server.

Furthermore, there is a built-in firewall (ipfw) provided by the OS that is not being separately evaluated.

3 TOE Security Environment

The purpose of this section is to identify the following:

1. Assumptions (A) about the TOE's operational environment.
2. Threats (T) to the IT systems addressed by either the TOE or the environment.
3. Organisational Security Policies (P) imposed to address security needs.

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 collection, analysis, detection, storage, and presentation of network traffic.

A.SCOPE
The TOE is appropriately scalable to the IT Systems the TOE monitors.

3.1.2 Physical Assumptions

A.LOCATE

The TOE will be located within a controlled access facility, intended to prevent unauthorised physical access.

A.INSTALL

The TOE will be properly installed and configured according to guidance documentation.

3.1.3 Personnel Assumptions

A.ADMIN

One or more competent individuals will be assigned as authorised administrators to manage the TOE and the security information it contains.

A.NOEVIL

An authorised administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRUST

The TOE shall only be accessed by authorised users.

3.1.4 Connectivity Assumptions

A.IFACE

The management interface of the TOE will be connected to a secured, separate network from the recording interfaces.

3.2 Threats

The following are threats identified for the TOE and the environment it monitors. There are threats that the TOE itself is responsible for addressing, as well as threats that the TOE Operational Environment must address. For all threats an unsophisticated level of expertise is assumed for the attackers.

3.2.1 TOE Threats

The threats listed here are those addressed by a compliant TOE.

T.COMINT

An unauthorised user may attempt to compromise the integrity of the data collected, analyzed and produced by the TOE by bypassing a security mechanism.

T.COMDIS

An unauthorised user may attempt to disclose the data collected, analyzed and produced by the TOE by bypassing a security mechanism.

T.LOSSOF

An unauthorised user may attempt to remove or destroy data collected, analyzed and produced by the TOE by searching through the filesystem and deleting the relevant files or copying them to a removable medium.

T.NOHALT

An unauthorised user may attempt to compromise the continuity of the TOE's collection and analysis functions by halting execution of the TOE.

T.PRIVIL

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

T.IMPCON

The TOE may be susceptible to improper configuration by an authorised or unauthorised user, causing potential intrusions to go undetected.

T.INFLUX

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

T.FACCNT

Unauthorised attempts to access TOE data or security functions by unauthorised users may go undetected.

3.2.2 TOE Environment Threats

The threats listed here are addressed by procedural and/or administrative controls carried out within the operating environment of the TOE.

T.MISUSE

An unauthorised user may gain access or cause activity indicative of misuse on an IT System the TOE monitors which goes undetected.

T.INADVE

An authorised or unauthorised user may cause inadvertent activity or access on an IT System the TOE monitors which goes undetected.

T.MISACT

An authorised or unauthorised user may produce malicious activity, such as the introduction of Trojan horses, viruses, worms, and other malware on an IT System the TOE monitors which goes undetected.

T.FALACT

The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity on the IT Systems the TOE monitors.

T.FALREC

The TOE may fail to recognise vulnerabilities or inappropriate activity based on the data it has collected on the IT Systems the TOE monitors.

T.EXPORT

An authorised user of the TOE may export information from the TOE to an IT System such that it can be accessed by unauthorised users.

3.3 Organisational Security Policies

This section identifies the Organisational Security Policies (P) applicable to the TOE and its environment:

P.DETECT

All network events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious attack of IT System assets must be collected.

P.ANALYZ

Analytical processes and information to derive conclusions about intrusions (past, present, future) must be applied to the network data collected, and appropriate response actions taken.

P.ACCACT

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

P.MANAGE

The TOE shall only be managed by authorised users.

P.ACCESS

All data collected, analyzed, generated, and produced by the TOE shall only be used for authorised purposes.

P.INTGTY

Data collected, analyzed, generated, and produced by the TOE shall be protected from unauthorised modification.

P.PROTCT

The TOE shall be protected from unauthorised accesses and disruptions of the following: analysis and response activities, collection activities, and TOE data and functions.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The following are the TOE security objectives, which are satisfied by technical countermeasures implemented by the TOE:

O.IDSENS

The TOE must collect and store network events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious attack within the IT environment.

O.IDANLZ

The TOE must apply analytical processes and information to collected data to derive conclusions about intrusions (past, present, future).

O.AUDITS

The TOE must record audit records for configuration changes and use of the System functions.

O.EXPORT

The TOE will ensure the confidentiality of its data when it is transferred across a network.

O.IDAUTH

The TOE must uniquely identify all users, and will authenticate the claimed identity before granting access to the TOE facilities.

O.RESPON

The TOE must respond appropriately to analytical conclusions based on the collected data.

O.INTEGR

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

O.EADMIN

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

O.OFLOWS

The TOE must appropriately handle potential audit and system data storage overflows.

O.PROTCT

The TOE must protect itself from unauthorised modifications and access to its functions and data.

O.RBAC

The TOE must prevent users from gaining access to and performing operations on the resources for which their role is not explicitly authorised.

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives, usually by procedural or administrative measures.

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

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

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

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.INTROP
The TOE is interoperable with the IT system it monitors.

5 IT Security Requirements

This section details the Security Functional Requirements (SFRs) that are provided by the TOE and the IT environment. These requirements are derived verbatim from Part 2 of the CC. This section also includes some explicitly stated and extended requirements. For clarity, the extended requirements contain the text (EXP) in the title.

5.1 TOE Security Functional Requirements

5.1.1 Security Audit

5.1.1.1 FAU_ADG.1 Audit Data Generation (EXP)

[Note: Applies only to actions done through the GUI]

Hierarchical to: No other components.

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

a) All auditable events for the not specified level of audit; and
b) [Access to reconstructed TOE data, and import/export of TOE data].

Table 1 – Auditable Events

Component	Event	Details
FAU_ADG.1	Access to reconstructed TOE data, and import/export of TOE data	User identity, interval of data accessed
FAU_STG.4	Actions taken due to storage failure	
FIA_UAU.1	Use of the authentication mechanism (including unsuccessful)	User identity, location
FIA_UID.1	Use (successful and unsuccessful) of the user identification mechanism, including the user identity provided	User identity, location
FMT_MOF.1	Modifications in the behavior of the functions of the TSF	User identity, location
FMT_MTD.1	Modifications to the values of TSF data	User identity, location
FMT_SMF.1	Use of the management functions	User identity, location
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

FAU_ADG.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 ST, [the additional information specified in the Details column of Table 1 – Auditable Events].

Dependencies: FPT_STM.1 Reliable time stamps

5.1.1.2 FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

FAU_GEN.2.1
The TSF shall be able to associate each auditable event with the identity of the user that caused the event**.**

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

5.1.1.3 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1
The TSF shall provide [Administrators, Advanced Users, and members of any group given explicit access rights by Administrators (GUI), and Superuser and Appliance User (CLI)] with the capability to read [all audit information in Table 1 – Auditable Events] from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.4 FAU_SAR.2 Restricted Audit Review

Hierarchical to: No other components.

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.

Dependencies: FAU_SAR.1 Audit review

5.1.1.5 FAU_STG.2 Guarantees of Audit Data Availability

Hierarchical to: FAU_STG.1

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

FAU_STG.2.2
The TSF shall be able to prevent unauthorised modifications to the audit records in the audit trail.

FAU_STG.2.3
The TSF shall ensure that [the latest audit log up to 2000 Kbytes of] audit records will be maintained when the following conditions occur: audit storage exhaustion.

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.6 FAU_STG.4 Prevention of Audit Data Loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1
The TSF shall overwrite the oldest stored audit records and [start a new audit log with a "logfile turnover" record] if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.2 Identification and Authentication

5.1.2.1 FIA_ATD.1 User Attribute Definition

[Note: These attributes apply to both GUI and CLI users]

Hierarchical to: No other components.

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

a) [User identity] ;
b) [Authentication data] ;
c) [Authorizations] ; and
d) [Password expiration information].

Dependencies: No dependencies

5.1.2.2 FIA_SOS.1(1) Verification of Secrets

[Note: Applies to GUI]

Hierarchical to: No other components.

FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [a minimum length of 6 characters including at least four alphabetic characters, one numeric and one special character].

Dependencies: No dependencies

5.1.2.3 FIA_SOS.1(2) Verification of Secrets

[Note: Applies to CLI]

Hierarchical to: No other components.

FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [a minimum length of 6 characters].

Dependencies: No dependencies

5.1.2.4 FIA_UAU.1 Timing of Authentication

[Note: Applies to GUI]

Hierarchical to: No other components.

FIA_UAU.1.1
The TSF shall allow [HTTPS session establishment] on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification

5.1.2.5 FIA_UAU.2 User Authentication Before Any Action

[Note: Applies to CLI]

Hierarchical to: FIA_UAU.1

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

Dependencies: FIA_UID.1 Timing of identification

5.1.2.6 FIA_UAU.7(1) Protected Authentication Feedback

[Note: Applies to GUI]

Hierarchical to: No other components.

FIA_UAU.7.1
The TSF shall provide only [the typed password masked with '*'s] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

5.1.2.7 FIA_UAU.7(2) Protected Authentication Feedback

[Note: Applies to CLI]

Hierarchical to: No other components.

FIA_UAU.7.1
The TSF shall provide only [a stationary cursor] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

5.1.2.8 FIA_UID.1 Timing of Identification

[Note: Applies to GUI]

Hierarchical to: No other components.

FIA_UID.1.1
The TSF shall allow [HTTPS session establishment] on behalf of the user to be performed before the user is identified.

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

Dependencies: No dependencies

5.1.2.9 FIA_UID.2 User Identification Before Any Action

[Note: Applies to CLI]

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies

5.1.3 Security Management

5.1.3.1 FMT_MOF.1(1) Management of Security Functions Behaviour

[Note: Applies to GUI]
Hierarchical to: No other components.

FMT_MOF.1.1
The TSF shall restrict the ability to determine the behaviour of, enable, disable, modify the behaviour of the functions [of TOE data collection, review, analysis, and reaction] to [Administrators and other groups given explicit configuration rights by Administrators].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.3.2 FMT_MOF.1(2) Management of Security Functions Behaviour

[Note: Applies to CLI]
Hierarchical to: No other components.

FMT_MOF.1.1
The TSF shall restrict the ability to enable, disable the functions [of TOE data collection] to [Superuser and Appliance User].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.3.3 FMT_MTD.1(1) Management of TSF Data

[Note: Applies to GUI]
Hierarchical to: No other components.

FMT_MTD.1.1
The TSF shall restrict the ability to change_default, query, modify, delete, [add] the [users, groups, permissions, alarm settings, reaction settings, recording parameters, interface properties] to [Administrators and other groups given such explicit rights by Administrators].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.3.4 FMT_MTD.1(2) Management of TSF Data

[Note: Applies to CLI]
Hierarchical to: No other components.

FMT_MTD.1.1
The TSF shall restrict the ability to change_default, [add] the [users, interface properties] to [Superuser].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.3.5 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1
The TSF shall be capable of performing the following security management functions: [authentication, authorisation, configuration of security functionality].

Dependencies: No Dependencies

5.1.3.6 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1
The TSF shall maintain the roles [Administrator, User, Advanced User, and other roles explicitly defined by Administrator members (GUI), and Superuser and Appliance User (CLI)].

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

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Protection of the TOE Security Functions

5.1.4.1 FPT_ITC.1 Inter-TSF Confidentiality During Transmission

Hierarchical to: No other components.

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

Dependencies: No dependencies

5.1.4.2 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

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.

Dependencies: No dependencies

5.1.4.3 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

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.

Dependencies: No dependencies

5.1.4.4 FPT_STM.1 Reliable Timestamps

Hierarchical to: No other components.

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

Dependencies: No dependencies

5.1.5 Explicitly Stated Requirements (NK-IDS)

A class of requirements has been explicitly written to cover the specialized functionality of the TOE. For ease and convenience of reference the class has been named NK-IDS[4], however, the functionality applies to both the security and performance analysis aspects of the TOE. For clarity, the requirement titles are labeled with (EXP).

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

Hierarchical to: No other components.

NK-IDS_SDC.1.1
The TOE shall be able to collect the following information from the targeted IT System resource(s):

a) network traffic; and
b) [none]. (EXP)

NK-IDS_SDC.1.2
At a minimum, the TOE shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) The additional information specified in the Details column of Table 2 – System Events. (EXP)

Dependencies: FPT_STM.1 Reliable time stamps

Table 2 – System Events for Data Collection

Component	Event	Details
NK-IDS_SDC.1	Network traffic	Protocol, source address, destination address, source port, destination port, payload

[4] These requirements are based in large part on the explicitly stated requirements in the following PPs: *IDS Sensor Protection Profile v1.1 12/10/2001* and *IDS Analyzer Protection Profile v 1.1 12/10/2001*. This inclusion does not represent any claim of PP conformance.

5.1.5.2 NK-IDS_ANL.1 Analyzer Analysis (EXP)

Hierarchical to: No other components.

NK-IDS_ANL.1.1
The TSF shall perform the following analysis function(s) on all network data received:

a) statistical, signature; and
b) [reconstruction (TCP sessions only)]. (EXP)

NK-IDS_ANL.1.2
The TSF 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) [Data destination, protocol, and severity (if applicable)]. (EXP)

Dependencies: NK-IDS_SDC.1 System Data Collection

5.1.5.3 NK-IDS_RCT.1 Analyzer React (EXP)

Hierarchical to: No other components.

NK-IDS_RCT.1.1
The TOE shall send an alarm to [the Event Viewer and any one (or none) of the following: email address(es), SNMP trap receiver(s), Syslog server(s)] and take [no other action] when an intrusion or anomaly is detected. (EXP)

Dependencies: NK-IDS_ANL.1 Analyzer Analysis

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

Hierarchical to: No other components.

NK-IDS_RDR.1.1
The TOE shall provide [Administrators, Advanced Users and any groups explicitly given permission by Administrators (GUI), and Superuser and Appliance User (CLI)] with the capability to read [packet payloads, analysis and event results] from the TOE data. (EXP)

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

NK-IDS_RDR.1.3
The TOE shall prohibit all users read access to it's data, except those users that have been granted explicit read-access. (EXP)

Dependencies: NK-IDS_SDC.1 System Data Collection
NK-IDS_ANL.1 Analyzer Analysis

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

[Note: Applies to Raw and Meta Data]
Hierarchical to: No other components.

NK-IDS_STG.1.1
The TOE shall protect the stored TOE data from unauthorised deletion. (EXP)

NK-IDS_ STG.1.2
The TOE shall protect the stored TOE data from unauthorised modification. (EXP)

NK-IDS_ STG.1.3
The TOE shall ensure that [archived and the most recent based on space management policy] data will be maintained when the following conditions occur: system data storage exhaustion. (EXP)

Dependencies: NK-IDS_SDC.1 System Data Collection

5.1.5.6 NK-IDS_STG.1(2) Guarantee of System Data Availability (EXP)

[Note: Applies to Event Data]
Hierarchical to: No other components.

NK-IDS_STG.1.1
The TOE shall protect the stored data from unauthorised deletion. (EXP)

NK-IDS_ STG.1.2
The TOE shall protect the stored data from unauthorised modification. (EXP)

NK-IDS_ STG.1.3
The TOE shall ensure that [at most the last 100,000 alarms of] TOE data will be maintained when the following conditions occur: system data storage exhaustion. (EXP)

Dependencies: NK-IDS_ANL.1 Analyzer Analysis

5.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL 2, derived from Part 3 of the CC. These requirements are summarised in Table 3 – Security Assurance Requirements for the TOE and described in more detail following the table:

Table 3 – Security Assurance Requirements for the TOE

Assurance Class	Assurance Component
ACM: Configuration Management	ACM_CAP.2 Configuration Items
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 Specifications
	ADV_HLD.1 Descriptive High-level Design
	ADV_RCR.1 Informal Correspondence Demonstration
AGD: Guidance Documents	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance
ATE: Tests	ATE_COV.1 Evidence of Coverage
	ATE_FUN.1 Functional Testing
	ATE_IND.2 Independent Testing -- Sample
AVA: Vulnerability Assessment	AVA_SOF.1 Strength of TOE Security Function Evaluation
	AVA_VLA.1 Developer Vulnerability Analysis

The developer (D) and content (C) specifications for the assurance requirements are detailed in the following sections.

5.2.1 Configuration Management (ACM)

5.2.1.1 ACM_CAP.2 Configuration Items

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

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

ACM_CAP.2.3D
The developer shall provide CM documentation.

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

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

ACM_CAP.2.3C
The CM documentation shall include a configuration list.
(Interp 003) The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.4C
The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C
The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C
The CM system shall uniquely identify all configuration items.

5.2.2 Delivery and Operation (ADO)

5.2.2.1 ADO_DEL.1 Delivery Procedures

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.

5.2.2.2 ADO_IGS.1 Installation, Generation, and Start-up Procedures

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
(Interp 051)The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

Dependencies: AGD_ADM.1 Administrator Guidance

5.2.3 Development (ADV)

5.2.3.1 ADV_FSP.1 Informal Functional Specifications

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.

Dependencies: ADV_RCR.1 Informal Correspondence Demonstration

5.2.3.2 ADV_HLD.1 Descriptive High-Level Design

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

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

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

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

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

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

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

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

Dependencies: ADV_FSP.1 Informal Functional Specifications
ADV_RCR.1 Informal Correspondence Demonstration

5.2.3.3 ADV_RCR.1 Informal Correspondence Demonstration

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.

5.2.4 Guidance Documents (AGD)

5.2.4.1 AGD_ADM.1 Administrator Guidance

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.

Dependencies: ADV_FSP.1 Informal Functional Specifications

5.2.4.2 AGD_USR.1 User Guidance

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.

Dependencies: ADV_FSP.1 Informal Functional Specifications

5.2.5 Tests (ATE)

5.2.5.1 ATE_COV.1 Evidence of Coverage

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

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

Dependencies: ADV_FSP.1 Informal Functional Specifications
ATE_FUN.1 Functional Testing

5.2.5.2 ATE_FUN.1 Functional Testing

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.

5.2.5.3 ATE_IND.2 Independent Testing

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.

Dependencies: ADV_FSP.1 Informal Functional Specifications
AGD_ADM.1 Administrator Guidance
AGD_USR.1 User Guidance
ATE_FUN.1 Functional Testing

5.2.6 Vulnerability Assessment (AVA)

5.2.6.1 AVA_SOF.1 Stength of TOE Security Function Evaluation

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.

Dependencies: ADV_FSP.1 Informal Functional Specifications
ADV_HLD.1 Descriptive High-Level Design

5.2.6.2 AVA_VLA.1 Developer Vulnerability Analysis

AVA_VLA.1.1D
(Interp 051) The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D
(Interp 051) The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1C
(Interp 051) 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.
(Interp 051) The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
(Interp 051) The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Dependencies: ADV_FSP.1 Informal Functional Specifications
ADV_HLD.1 Descriptive High-Level Design
AGD_ADM.1 Administrator Guidance
AGD_USR.1 User Guidance

6 TOE Summary Specification

This section describes the TOE security functions and assurance measures related to the TOE development that make it possible to meet the SFRs and SARs claimed in this document.

6.1 TOE Security Functions

The TOE provides the following security functions:

1. Identification and Authentication (NK_FIA)
2. Security Audit (NK_FAU)
3. Security Management (NK_FMT)
4. Protection of the TOE Security Functions (NK_FPT)
5. Data Collection and Storage (NK_SDC)
6. Data Analysis and Response (NK_ANL)

Each of these is discussed in more detail in the subsections which follow. By convention, the SFRs relevant to the functions being described are included in brackets, ie. [SFR id].

6.1.1 Identification and Authentication (NK_FIA)

There are two methods of gaining user access to the TOE: web GUI and CLI console. Both provide restricted access requiring identification and authentication [FIA_UAU.1, FIA_UAU.2, FIA_UID.1, FIA_UID.2]. Both are also intended for different purposes and hence maintain their own independent set of user attributes.

The web GUI is the primary means of accessing TOE functions. An embedded web server is addressable via a URL that presents a login screen. Other than HTTPS session establishment, no other functions are permitted prior to identification and authentication [FIA_UAU.1]. A user is identified by typing in a valid username into the proper field, and authenticated by typing in a valid password associated with the given username. Valid passwords are at least 6 characters in length and must include at least 4 alphabetic characters, 1 numeral and 1 special character [FIA_SOS.1(1)]. During authentication the typed password is echoed as a string of astericks ("*") [FIA_UAU.7(1)]. If the username and/or password is invalid, an Invalid Login screen briefly appears, followed by the Login screen being presented again. A link is also present which can be clicked to immediately access the login screen [FIA_UAU.1]. The Invalid Login message does not specify whether it was identification (ie., invalid username) or authentication (ie., invalid password) that caused the login failure [FIA_UAU.7(1)]. Any attempt to bypass the GUI login by typing a URL that addresses some direct functionality of the TOE will cause an Invalid Login screen to be presented. [FPT_RVM.1].

In addition to identity and authentication data, each GUI user is also associated with an authorization group and password expiration information [FIA_ATD.1]. When a user is authenticated via the GUI, the group membership is looked up and used to determine the parts of the TOE to which they have access. Icons, buttons, and links representing TOE functions for which they are not authorised are either not presented at all or are greyed-out (ie., disabled) [FPT_RVM.1].

Password expiration data is also used during authentication. If the password has already expired then the Invalid Login screen is presented [FIA_ATD.1, FIA_UAU.7(1)].

The CLI console is intended for initial installation and appliance troubleshooting. Normal operation of the TOE does not require access to the CLI, hence the evaluated configuration includes it only as a keyboard and monitor attached directly to the appliance in a physically protected area. CLI access occurs through a standard Unix login prompt requiring username/password [FIA_UAU.2, FIA_UID.2]. Valid passwords are at least 6 characters in length [FIA_SOS.1(2)]. In addition to username/password, the standard Unix-style login account properties are associated with each user, including group membership and password expiration [FIA_ATD.1]. During authentication, nothing is echoed to the screen as the password is typed (the cursor remains stationary) [FIA_UAU.7(2)]. If the username and/or password is invalid, a "login incorrect" message is output and the login prompt is given again [FIA_UAU.2, FIA_UID.2]. Following 4 consecutive invalid login attempts, the login prompt is delayed by a linearly increasing number of 5 second increments for each subsequent invalid login, eg., 5 seconds, 10 seconds, 15 seconds, 20 seconds, etc. By default, 10 consecutive invalid login attempts are allowed before being reset.

6.1.2 Security Audit (NK_FAU)

There are two main audit logs accessible through the GUI:

1. Activities Log
2. Export Log

The Activities Log is accessed through the Configuration screen. Entries get added to the log as a result of direct GUI user activity and include a timestamp, IP address of origin, user identity, a description of the event, and outcome (if applicable). All events indicated in Table 1 – Auditable Events get logged [FAU_ADG.1, FAU_GEN.2]. Table 4 – Auditable Event Specification contains additional details on the audit logging for each event.

Table 4 – Auditable Event Specification

Component	Event	Details	Specification
FAU_ADG.1	Access to reconstructed TOE data, and import/export of TOE data	User identity, interval of data accessed	See Details
FAU_STG.4	Actions taken due to storage failure		Turnover message is logged at start of new logfile
FIA_UAU.1	Use of the authentication mechanism	User identity, location	Successful and unsuccessful attempts are recorded
FIA_UID.1	Use of the user identification mechanism, including the user identity provided	User identity, location	Successful and unsuccessful attempts are recorded
FMT_MOF.1	Modifications in the behavior of the functions of the TSF	User identity, location	Add/delete/edit users and groups, start/stop recording and monitoring, add/enable/disable alarms, reboot, shutdown
FMT_MTD.1	Modifications to the values of TSF data	User identity, location	Edits to users, groups, alarms, recording parameters, management interface parameters

FMT_SMF.1	Use of the management functions	User identity, location	Edits to users, groups, alarms, recording parameters, management interface parameters
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity	Edits to user group membership through the GUI and CLI users becoming Superuser

The Export Log is also accessed through the Configuration screen. It logs user-scheduled and on-demand exports of TOE system data. Each entry contains a timestamp of the export begin time, a title/filename, the start/end time of the system data being exported, and a success/failure indicator [FAU_ADG.1].

The Activities Log and Export Log are presented in an easy-to-read table. By default, both logs can only be read by Administrators and Advanced Users. Administrators can, at their own discretion, create additional groups and grant them explicit read access to the audit logs as well [FAU_SAR.1(1), FAU_SAR.2].

No user through the GUI can directly write to, modify, or delete audit records. Audit records automatically get added sequentially to a log file as a result of GUI user activity. This auditing function is always enabled as long as the appliance is powered on and it cannot be disabled by the user. A log rotation mechanism is in place such that when the current logfile reaches a certain allowed maximum size, it is closed and renamed with a sequential number postfix (eg., log.0) and a new logfile is opened as the current log. When this occurs, a log turnover message is written as the last record of the old logfile and the first record of the new logfile. New audit records are then appended to the new logfile. When the number of old logfiles exceeds a certain number (4 for Activities logs and 7 for Export logs) the TOE will delete the oldest log to free up disk space [FAU_STG.2, FAU_STG.4].

These logs and additional logs – mostly having to do with OS activities, the web server, and system messages – are readable via the CLI by Superusers and Appliance Users [FAU_SAR.1(2)]. Audit review via the CLI is intended for appliance troubleshooting purposes only.

6.1.3 Security Management (NK_FMT)

TOE access is mediated by the authentication and authorisation mechanisms built into the GUI and CLI [FMT_SMF.1].

By default, the following roles are defined for the GUI: Administrator, Advanced User, User [FMT_SMR.1]. Each is explained in more detail below:

Administrator

This is the highest level role with full access rights to the TOE. This group can manage all of the security function behaviour and TSF data: users and roles; view/modify all configuration functions of the TOE; view all system data, analysis results, and audit logs; start/stop/modify recording; start/stop/configure detections and alarming; query/delete raw and generated data; import/export/reconstruct data. Administrators can also create new roles, and at their own discretion, grant them permission to manage some or all of the same security functions and TSF data (with the exception of user/role account management, which is only available to Adminstrators and can't be granted to other groups -- this prevents the possibility of privilege escalation scenarios) [FMT_MOF.1(1), FMT_MTD.1(1), FMT_SMF.1].

Advanced User

This is an intermediate level role with advanced analysis review capabilities (ie., packet payload and reconstruction results), data import/export permissions, and event data review and delete capabilities. Advanced Users are not authorised to modify any security function behaviour [FMT_MOF.1(1)].

User

This is the low level role with access to basic analysis and event data review capabilities. Users are not authorised to modify any security function behaviour, and cannot read packet payloads or reconstructed network traffic.

When an Administrator creates a new user, they must specify a password and assign the user to a group (in addition to the other attributes defined in FIA_ATD.1). Password specifications must be at least 6 characters in length and must include at least 4 alphabetic characters, 1 numeric and 1 special character [FIA_SOS.1(1)]. A given user can only belong to exactly one group. Modifying a user's properties to assign them to a new group will automatically remove them from their existing group [FMT_SMR.1]. Following successful authentication, a session is created where the user's role is looked up to determine which screens and functions they are permitted to access.

Management of TOE data also involves importing/exporting to external trusted systems. Data can be exported via FTP, SCP, and HTTPS and imported via FTP and HTTPS. In the case of HTTPS, the data is transferred to/from the client browsing machine. In order to maintain confidentiality, use of FTP for import/export is not authorised for the evaluated configuration. [FMT_MTD.1(1), FPT_ITC.1].

By default there are 2 groups defined for the CLI: Superuser and Appliance User. These 2 groups respectively correspond to 2 accounts: *root* and *vcr*. The root account is the standard Unix default member of the Superuser group with full administrative rights (read/write/execute) over the system. The vcr user is the single default Appliance User for the CLI. It has authorisation to do all the things one would normally need to do for backend troubleshooting and selected control of TOE functions and data (read/execute) without requiring the full power of root access. If necessary, it is possible for the vcr user to assume Superuser privileges via the su command. Invoking the su command will re-initiate the NK_FIA function before the vcr user is granted Superuser privileges.

A Superuser can change the password on existing CLI accounts, or create new CLI accounts[5] by specifying the attributes defined in FIA_ATD.1. Password specifications must be at least 6 characters in length [FIA_SOS.1(2)].

Many of the functions invoked through the GUI have command line equivalents that can be run from the root or vcr accounts. However, this is not the intended usage of these accounts – they are provided for initial installation and troubleshooting. Per guidance, the authorised security management activities through the CLI are starting/stopping data collection [FMT_MOF.1(2)] and query/delete of collected and generated TOE data [FMT_MTD.1(2)].

6.1.4 Protection of the TOE Security Functions (NK_FPT)

Data can enter into the TOE in only 3 ways: management interface, CLI console, or recording interface. This section describes the 3 interfaces and the protection mechanisms they involve.

Management Interface

This is the IP network addressable Ethernet interface through which web access occurs. During initial setup the management interface gets configured with an IP address, network mask, gateway address, and DNS address. Only Administrators through the GUI or Superusers through the CLI can modify these parameters. All remote communications through this interface are secured via HTTPS, which utilises SSL. This protects the data from disclosure as it is transmitted between the browser and appliance [FPT_ ITC.1].

[5] Since the appliance is not a generic server and the default accounts provide all that is needed for access and control, it is neither necessary nor recommended to create additional CLI accounts.

In addition to SSL protection, all access through the management interface requires identification and authentication before any other TOE functions can be invoked. Operators cannot bypass the identification and authentication mechanisms [FPT_RVM.1, FIA_UAU.1, FIA_UID.1, FIA_SOS.1(1)].

CLI Console
In the evaluated configuration the CLI is accessible only through a keyboard and monitor directly attached to the appliance. This collocation with the appliance means the console is in a physically protected area, thus restricting the possibility of unauthorised access. CLI access requires identification and authentication before any other TOE functions can be invoked. Operators cannot bypass these mechanisms [FPT_RVM.1, FIA_UAU.2, FIA_UID.2, FIA_SOS.1(2)].

Recording Interface
One or more recording interfaces provide the core means of system data collection. Recording interfaces are ports on network interface cards (NICs) which passively monitor network traffic. These interfaces do not include a TCP/IP stack and do not have routable IP addresses. Traffic recorded by these interfaces – potentially containing malicious code and attacks – is never executed and it gets stored in an area of the file system that is separate from all other TOE data and OS/system binaries [FPT_SEP.1].

Data coming in through recording interfaces (and audit records) rely on time stamps that get read from the system time maintained by the OS [FPT_STM.1]. This time is initially set during installation and can only be reset by the CLI Superuser.

6.1.5 Data Collection and Storage (NK_SDC)

Network data enters NIKSUN appliances through NICs in promiscuous mode that are attached to passive taps, span/mirrored switch ports, or hubs. NIKSUN appliances can monitor a wide range of LAN/MAN/WAN technologies, including 10/100 Ethernet, Gigabit Ethernet, T1, E1, V.35, X.21, DS3, T3, E3, HSSI, OC-3, and OC-12. Each protocol data unit (PDU) in the form of a frame, cell, or packet that is seen on the network gets copied, timestamped, and written directly to disk into a proprietary traffic stream data warehouse. This recording process happens continuously and results in long streams of raw packet data [NK-IDS_SDC.1].

Through the GUI, only Administrators and Advanced Users by default have the permission to actually view packet payload data (directly from the Packet Viewer screen or reassembled in the Application

Reconstruction screen). Administrators may also, at their own discretion, create additional roles with the ability to view packet payload data [NK-IDS_RDR.1]. Only Administrators can delete raw packet streams, start/stop the recording of data, and modify the behaviour of recording (eg., adding a filter to exclude certain traffic) [NK-IDS_STG.1(1), FMT_MOF.1(1)].

Through the CLI, the Superuser and Appliance Users can view packet data with the vcrdump command, and delete data with the vds command. These authorised users can also start/stop the recording of data [NK-IDS_RDR.1, FMT_MOF.1(2), FMT_MTD.1(2)].

Recorded data streams are indexed by timestamps, which provide chronology. This creates a condition such that once data has been written it is not possible to modify it [NK-IDS_STG.1(1)].

Since NIKSUN appliances are intended to operate in continuous recording mode, the "steady state" invariant condition is eventually one where available storage has been exhausted. There are two mechanisms which impact the guaranteed availability of system data in this case [NK-IDS_STG.1(1)]:

1. Space management policy: An automatic space management policy is enforced that will continuously delete the oldest data from the largest streams to free up space for new data to be continuously recorded. Hence, the most recently recorded data is guaranteed to be available (depending on the speed and utilization of the network being monitored and the amount of disk storage, "most recent" spans anywhere from "the last n hours" to "the last n months" of data).
2. Archiving: Administrators have the ability to archive selected streams of data. This removes the data from consideration in space management and guarantees it's availability indefinitely until it is either explicitly unarchived or deleted.

6.1.6 Data Analysis and Response (NK_ANL)

As packet data is recorded from monitoring interfaces, another process simultaneously analyses the data and produces aggregated, multi-level statistics [NK-IDS_ANL.1]. This statistical meta-data also gets written to disk in companion streams to the raw data. The same policies which apply to the deletion, modification, starting/stopping, space management, and archiving of the raw data streams also apply to the statistical meta-data streams [NK-IDS_STG.1(1)].

NIKSUN applications include basic Traffic Analysis screens that display plots and tables derived from queries to the statistical data. All GUI users in the default roles have the ability to view Traffic Analysis.

Administrators can, at their own discretion, create groups that do not have access to Traffic Analysis [NK-IDS_RDR.1].

The Application Modules provide the following additional analysis functions: Anomaly Detection, Signature Detection, Reconstruction, QoS, and RTX.

Anomaly Detection
Anomaly Detection is a subcomponent for security analysis. Only Administrators and any groups they give such explicit rights can add, edit, or delete anomaly alarms [FMT_MOF.1(1)]. Anomalies are tracked through user-defined thresholds on various parameters queried from the statistics. Such parameters include host scans, host floods, port scans, utilization, host pair bytes, and invalid IP addresses [NK-IDS_ANL.1]. As a result of an anomaly being detected, notification is presented automatically in the Event Viewer and optionally sent to a trusted email address or trusted SNMP trap receiver [NK-IDS_RCT.1]. The information contained in the notification includes date/time of alert, anomaly type, source and destination IP address(es), and severity [NK-IDS_ANL.1].

Signature Detection
Signature Detection is a subcomponent for security analysis and is implemented by an embedded open source Snort® IDS engine. Only Administrators and any groups they give such explicit rights can enable/disable detection, enable/disable signatures, and configure the behaviour, response, and analysis of the detection through the GUI. Through the CLI, only Superusers can enable/disable/add/edit individual signatures and configure the behaviour of detection. The signature detection operates by reading raw data streams and looking for particular patterns within packets [NK-IDS_ANL.1]. As a result of a signature being detected, notification is presented automatically in the Event Viewer and optionally sent to a trusted syslog server [NK-IDS_RCT.1]. The information contained in the notification includes date/time of alert, signature identification, source and destination IP addresses and ports, protocol, and severity [NK-IDS_ANL.1].

Application Reconstruction
Application Reconstruction is a subcomponent for security analysis. Since reconstruction operates on packet payloads, only Administrators and Advanced Users have access to view the results from the GUI by default [NK-IDS_RDR.1]. Reconstruction operates on TCP data flows, interpreting the data through the state machine of the given application protocol: HTTP, SMTP, POP3, IMAP4, FTP, IM, Telnet, etc

Snort® is a registered trademark of Sourcefire, Inc.

[NK-IDS_ANL.1]. Web pages, emails with attachments, IM chats, and FTP with file contents are all represented in much the same way as their applications would present them. String searches, ASCII dumps, HEX dumps, and packet views are also supported on the data.

QoS Monitoring

NetSLM is the QoS monitoring subcomponent for performance analysis. Only Administrators and any groups they give such explicit rights can add, edit, or delete QoS alarms [FMT_MOF.1(1)]. QoS alarms are tracked through user-defined thresholds on number of bytes, number of packets, utilization, and bit rate at the link, network, or transport layer [NK-IDS_ANL.1]. As a result of a QoS alarm being triggered, notification is presented automatically in the Event Viewer and optionally sent to a trusted syslog server or trusted SNMP trap receiver [NK-IDS_RCT.1]. The information contained in the notification includes date/time of alert, QoS metric, source and destination IP address(es), and severity [NK-IDS_ANL.1].

RTX

NetRTX is the Real Time Experts subcomponent for performance analysis. Only Administrators and any groups they give such explicit rights can enable/disable detection, enable/disable experts, and configure the behaviour, response, and analysis of the detection through the GUI. RTX is analogous to signature detection and operates by reading raw data streams and looking for particular performance-relevant patterns within packets [NK-IDS_ANL.1]. As a result of a pattern being found, notification is presented automatically in the Event Viewer and optionally sent to a trusted syslog server or trusted SNMP trap receiver [NK-IDS_RCT.1]. The information contained in the notification includes date/time of alert, identification, source and destination IP addresses and ports, protocol, and severity [NK-IDS_ANL.1].

The Event Viewer contains a running log of all alarms detected by the Anomaly, Signature, QoS, and RTX mechanisms. By default, Administrators, Advanced Users, and Users have read access and delete permission on all events in the Event Viewer [NK-IDS_RDR.1]. It is possible for Administrators to create groups that do not have any access to the Event Viewer. The Event Viewer keeps up to 100,000 of the latest events, and will delete the oldest events to make space for new events after the limit has been reached [NK-IDS_STG.1(2)].

6.2 TOE Security Assurance Measures

This section maps the EAL 2 CC assurance requirements with the assurance measures used for the development and maintenance of the TOE as described in Table 5 – Assurance Measures Mapped to

Security Assurance Requirements.

Table 5 – Assurance Measures Mapped to Security Assurance Requirements

Assurance Requirement	Assurance Measure
ACM_CAP.2 Configuration Items	A TOE reference unique to the version is provided, a CM system is used, and the following CM documentation is provided: • NK-ACM-CMS-NDV2005-1.3 NIKSUN Configuration Management System NetDetector/NetVCR 2005: Documents the CM systems and procedures used in the development of the TOE. • NK-ACM-CI-NDV2005-NKOS-1.2 Configuration Item List NetDetector/NetVCR 2005 NIKOS: Documents and lists the configuration items that comprise the NIKOS subsystem (integral to the DCE). • NK-ACM-CI-NDV2005-MERC-1.2 Configuration Item List NetDetector/NetVCR 2005 Mercury: Documents and lists the configuration items that comprise the Mercury subsystem (integral to the DCE). • NK-ACM-CI-NDV2005-APPS-1.2 Configuration Item List NetDetector/NetVCR 2005 Applications: Documents and lists the configuration items that comprise the Application modules within the TOE (includes UIE and Application modules).

ADO_DEL.1 Delivery Procedures	• NK-ADO-SDP-NDV-1.2 NIKSUN Secure Delivery Process: Describes the delivery procedures, including those necessary to maintain security when distributing the TOE to a user's site. • NK-ADO-MFG-x345-1.1 IBM xSeries 345 – 2U Chassis Manufacturing Directives: Describes the manufacturing procedures for a particular chassis. • NK-ADO-MFG-WV1/2-2.3 Intel SE7501WV2 (Westville) 1U/2U Chassis Manufacturing Guidelines: Describes the manufacturing procedures for a particular chassis.
ADO_IGS.1 Installation, Generation, and Start-up Procedures	• NIKSUN NetDetector/NetVCR 2005 Release Notes: Release specific notes that may be related to the secure installation, generation, and start-up of the TOE. • NIKSUN NetDetector/NetVCR 2005 Customer Installation Guide: Documents the steps necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1 Informal Functional Specifications	NK-ADV-FSP-NDV2005-1.7 Functional Specification for NIKSUN NetDetector/NetVCR 2005: Informally documents the functionality, TSF, and external interfaces to be internally consistent and completely representative.
ADV_HLD.1 Descriptive High-level Design	NK-ADV-HLD-NDV2005-1.5 High-level Design for NIKSUN NetDetector/NetVCR 2005: Informally documents the high level design of the TSF in terms of its subsystems and the security functionality each provides; identifies underlying hardware, firmware, software and protection mechanisms implemented; identifies TSF interfaces, including those externally visible. Additional hardware/firmware coverage is included in the NK-ADO-MFG documents.

ADV_RCR.1 Informal Correspondence Demonstration	NK-ADV-RCR-NDV2005-1.3 NIKSUN NetDetector/NetVCR 2005 Informal Correspondence Analysis: Documents the mapping between ST, FSP, and HLD to show that all relevant security functionality is covered from the more abstract to the less abstract representations.
AGD_ADM.1 Administrator Guidance	NIKSUN NetDetector/NetVCR 2005 User Guide: Embedded within the User Guide is Administrator guidance that describes all functions restricted to the administrator with the attending caveats, assumptions, security parameters, and procedures.
AGD_USR.1 User Guidance	NIKSUN NetDetector/NetVCR 2005 User Guide: Documents all functions available to users with the attending caveats, assumptions, parameters, procedures, and responsibilities.
ATE_COV.1 Evidence of Coverage	NK-ATE-STP-NDV2005-1.2 NIKSUN NetDetector/NetVCR 2005 System Test Plan: Embedded within the Test Plan is evidence of test coverage, mapping tests identified in the documentation with the FSP.
ATE_FUN.1 Functional Testing	• NK-ATE-STP-NDV2005-1.2 NIKSUN NetDetector/NetVCR 2005 System Test Plan: Documents the overall test plan for the TOE • NK-ATE-STS-NDV2005-1.2 NIKSUN NetDetector/NetVCR 2005 Test Specification: Describes test goals, procedures, scenarios, dependencies and expected results • NK-ATE-STR-NDV2005-1.1 Test Results: Documents actual test results
ATE_IND.2 Independent Testing	A TOE suitable for testing is provided along with necessary resources (eg., test data).
AVA_SOF.1 Strength of TOE Security Function Evaluation	NK-AVA-SOF-NDV2005-1.3 NIKSUN NetDetector/NetVCR 2005 Strength of Function Analysis: Provides an analysis showing that the strength of TOE security function claims are met or exceeded.

AVA_VLA.1 Developer Vulnerability Analysis	NK-AVA-VLA-NDV2005-1.2 NIKSUN NetDetector/NetVCR 2005 Vulnerability Assessment: Documents the obvious and known vulnerabilities and shows that they cannot be exploited in the intended environment for the TOE.

6.3 TOE Strength of Function Claims

The minimum strength of function claim for the TOE Security Function NK_FIA, in particular the TOE's password mechanism, is SOF-basic. Passwords are used for authentication and can be analysed using probability and/or permutation calculations. As specified by FIA_SOS.1, there is a minimum password length requirement imposed (6 characters) as well as an additional GUI password requirement for at least four alphabetic characters, one numeric and one special character.

7 Protection Profile Claims

The NIKSUN NetDetector/NetVCR 2005 TOE does not claim conformance to any registered PP.

8 Rationale

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

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement set forth in this document.

8.1.1 IT Security Objectives Rationale

This section shows that the security objectives are necessary and sufficient to address the security concerns. Table 6 – Mapping Security Environment to Objectives gives a mapping between the assumptions, threats, and OSPs and the security objectives, showing that each objective covers at least one assumption, threat, or policy and that each assumption, threat, or policy is covered by at least one objective.

Table 6 – Mapping Security Environment to Objectives

	O.IDSENS	O.IDANLZ	O.AUDITS	O.EXPORT	O.IDAUTH	O.RESPON	O.INTEGR	O.EADMIN	O.OFLOWS	O.PROTCT	O.RBAC	O.INSTAL	O.PHYCAL	O.PERSON	O.CREDEN	O.INTROP
A.ACCESS																X
A.SCOPE												X				X
A.LOCATE													X			
A.INSTALL												X				
A.ADMIN														X		
A.NOEVIL												X	X	X	X	
A.NOTRUST													X		X	
A.IFACE												X				X
T.COMINT					X		X			X	X					
T.COMDIS				X	X					X	X					
T.LOSSOF					X		X			X	X					
T.NOHALT			X		X					X	X					
T.PRIVIL			X		X					X	X					
T.IMPCON			X		X			X			X	X				
T.INFLUX									X							
T.FACCNT			X													
T.MISUSE	X		X													
T.INADVE	X		X													
T.MISACT	X		X													
T.FALACT						X										
T.FALREC		X														
T.EXPORT			X	X								X				
P.DETECT	X		X													
P.ANALYZ		X				X										
P.ACCACT			X		X						X					
P.MANAGE					X			X			X	X		X		
P.ACCESS					X					X	X					

	O.IDSENS	O.IDANLZ	O.AUDITS	O.EXPORT	O.IDAUTH	O.RESPON	O.INTEGR	O.EADMIN	O.OFLOWS	O.PROTCT	O.RBAC	O.INSTAL	O.PHYCAL	O.PERSON	O.CREDEN	O.INTROP
P.INTGTY							X									
P.PROTCT									X				X			

A.ACCESS
The TOE has access to all the IT System data it needs to perform collection, analysis, detection, storage, and presentation of network traffic.

O.INTROP ensures that the TOE interoperates with the environment in such a way to provide access to IT System data.

A.SCOPE
The TOE is appropriately scalable to the IT Systems the TOE monitors.

O.INSTAL ensures the proper installation of the TOE.
O.INTROP ensures that the TOE has the needed access.

A.LOCATE
The TOE will be located within a controlled access facility, intended to prevent unauthorised physical access.

O.PHYCAL provides for the physical protection of the TOE consistent with security and guidance.

A.INSTALL
The TOE will be properly installed and configured in accordance with guidance documentation.

O.INSTAL ensures the proper installation and management of the TOE.

A.ADMIN
One or more competent individuals will be assigned as Authorised Administrators to manage the TOE and the security information it contains.

O.PERSON ensures properly trained authorised administrators.

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

O.INSTAL ensures proper installation of the TOE. O.PHYCAL provides for physical protection of the TOE. O.PERSON ensures carefully chosen and trained administrators. O.CREDEN provides for the protection of access credentials.

A.NOTRUST
The TOE can only be accessed by authorised users.

O.PHYCAL provides for physical protection to guard against unauthorised access. O.CREDEN provides for the protection of access credentials.

A.IFACE
The management interface of the TOE will be connected to a secured, separate network from the

recording interfaces.

O.INSTAL provides for proper installation, management, and operation of the TOE consistent with IT security and guidance. O.INTROP ensures that the TOE is interoperable with the IT System it monitors.

T.COMINT

An unauthorised user may attempt to compromise the integrity of the data collected, analyzed and produced by the TOE by bypassing a security mechanism.

O.IDAUTH provides for the authentication of users before access to TOE data. O.RBAC builds on this by only permitting users with authorised roles to access TOE data. O.INTEGR ensures no TOE data will be subject to unauthorised modification. O.PROTCT provides for TOE self-protection.

T.COMDIS

An unauthorised user may attempt to disclose the data collected, analyzed and produced by the TOE by bypassing a security mechanism.

O.IDAUTH provides for the authentication of users before access to TOE data. O.RBAC builds on this by only permitting users with authorised roles to access TOE data. O.EXPORT ensures the confidentiality of TOE data will be maintained. O.PROTCT provides for TOE self-protection.

T.LOSSOF

An unauthorised user may attempt to remove or destroy data collected, analyzed and produced by the TOE by searching through the filesystem and deleting the relevant files or copying them to a removable medium.

O.IDAUTH provides for the authentication of users before access to TOE data. O.RBAC builds on this by only permitting users with authorised roles to access TOE data. O.INTEGR ensures the integrity of TOE data. O.PROTCT provides for TOE self-protection.

T.NOHALT

An unauthorised user may attempt to compromise the continuity of the TOE's collection and analysis functions by halting execution of the TOE.

O.IDAUTH provides for the authentication of users before access to TOE functions. O.RBAC builds on this by only permitting users with authorised roles to access TOE functions. O.AUDITS provides for accountability on the part of users who attempt to halt TOE functions. O.PROTCT provides for TOE self-protection.

T.PRIVIL

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

O.IDAUTH provides for the authentication of users before access to TOE functions. O.RBAC builds on this by only permitting users with authorised roles to access TOE functions. O.AUDITS provides for accountability on the part of users who attempt to exploit system privileges. O.PROTCT provides for TOE self-protection.

T.IMPCON

The TOE may be susceptible to improper configuration by an authorised or unauthorised user, causing potential intrusions to go undetected.

O.INSTAL provides for proper configuration of the TOE by authorised administrators. O.EADMIN ensures the TOE has all the administrator functions to manage the appliance. O.IDAUTH provides for the authentication of users before access to TOE functions. O.RBAC builds on this by only permitting users with authorised roles to access TOE functions. O.AUDITS provides for accountability on the part of users who improperly configure the TOE.

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

O.OFLOWS requires the TOE to handle data storage overflows.

T.FACCNT
Unauthorised attempts to access TOE data or security functions by unauthorised users may go undetected.

O.AUDITS requires the TOE to collect audit data on use and configuration of the TOE.

T.MISUSE
An unauthorised user may gain access or cause activity indicative of misuse on an IT System the TOE monitors which goes undetected.

O.AUDITS and O.IDSENS require the TOE to collect audit and system data to address this threat.

T.INADVE
An authorised or unauthorised user may cause inadvertent activity or access on an IT System the TOE monitors which goes undetected.

O.AUDITS and O.IDSENS require the TOE to collect audit and system data to address this threat.

T.MISACT
An authorised or unauthorised user may produce malicious activity, such as the introduction of Trojan horses, viruses, worms, and other malware on an IT System the TOE monitors which goes undetected.

O.AUDITS and O.IDSENS require the TOE to collect audit and system data to address this threat.

T.FALACT
The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity on the IT Systems the TOE monitors.

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

T.FALREC
The TOE may fail to recognise vulnerabilities or inappropriate activity based on the data it has collected on the IT Systems the TOE monitors.

O.IDANLZ provides for the TOE to recognize vulnerabilities or inappropriate activity based on conclusions drawn from analysis of captured data.

T.EXPORT
An authorised user of the TOE may export information from the TOE to an IT System where it can be accessed by unauthorised users.

O.AUDITS requires the TOE to collect audit data. O.EXPORT guarantees the confidentiality of data as it is transferred. O.INSTAL requires that the TOE be operated in a manner consistent with IT security and guidance.

P.DETECT
All network events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious attack of IT System assets must be collected.

O.AUDITS and O.IDSENS require the TOE to collect audit and system data to address this policy.

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

> O.IDANLZ requires analytical processes to be applied to collected data. O.RESPON provides for appropriate response to analytical conclusions.

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

> O.AUDITS requires the auditing of all data accesses and use of TOE functions. O.IDAUTH supports this by ensuring each user is uniquely identified and authenticated before given access to TOE data and functions. O.RBAC further supports this by ensuring users are assigned to roles which define the scope of actions they may take.

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

> O.PERSON ensures competent administrators will manage the TOE and O.EADMIN ensures there is a sufficient set of functions to use. O.INSTAL supports this further by ensuring proper installation, management, and operation of the TOE. O.IDAUTH provides for authentication before access. O.RBAC builds on this by only permitting users with authorised roles to access TOE functions.

P.ACCESS
All data collected, analyzed, generated, and produced by the TOE shall only by used for authorised purposes.

> O.IDAUTH provides for the authentication of users before access to TOE functions. O.RBAC builds on this by only permitting users with authorised roles to access TOE functions. O.AUDITS provides for accountability on the part of users who attempt to halt TOE functions. O.PROTCT provides for TOE self-protection.

P.INTGTY
Data collected, analyzed, generated, and produced by the TOE shall be protected from unauthorised modification.

> O.INTEGR ensures the protection of data from unauthorised modification.

P.PROTCT
The TOE shall be protected from unauthorised accesses and disruptions of the following: analysis and response activities, collection activities, and TOE data and functions.

> O.OFLOWS supports this policy by requiring the TOE to handle disruptions due to storage exhaustion. O.PHYCAL ensures the TOE is protected from unauthorised physical access.

8.1.2 Environment Security Objectives Rationale

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

The environmental security objectives are O.INSTAL, O.PHYCAL, O.PERSON, O.CREDEN, and O.INTROP. These objectives are satisfied by procedural and administrative measures and need only be mapped to assurance measures. The guidance documentation (AGD_ADM, AGD_USR) addresses these objectives.

8.2 Security Requirements Rationale

This section provides the rationale for the SFRs and SARs.

8.2.1 Security Functional Requirements Rationale

This section will demonstrate that each SFR addresses at least one security objective, and each security objective is addressed by at least one SFR. Table 7 – Mapping of SFRs to Objectives shows this mapping explicitly and is followed by a discussion of each objective's coverage in more detail.

Table 7 – Mapping of SFRs to Objectives

	O.IDSENS	O.IDANLZ	O.AUDITS	O.EXPORT	O.IDAUTH	O.RESPON	O.INTEGR	O.EADMIN	O.OFLOWS	O.PROTCT	O.RBAC
FAU_ADG.1			X								
FAU_GEN.2			X								
FAU_SAR.1(1)								X			
FAU_SAR.1(2)								X			
FAU_SAR.2											X
FAU_STG.2							X		X	X	X
FAU_STG.4									X		
FIA_ATD.1					X						
FIA_SOS.1(1)					X						
FIA_SOS.1(2)					X						
FIA_UAU.1					X						X
FIA_UAU.2					X						X
FIA_UAU.7(1)					X						
FIA_UAU.7(2)					X						
FIA_UID.1					X						X
FIA_UID.2					X						X

	O.IDSENS	O.IDANLZ	O.AUDITS	O.EXPORT	O.IDAUTH	O.RESPON	O.INTEGR	O.EADMIN	O.OFLOWS	O.PROTCT	O.RBAC
FMT_MOF.1(1)										X	X
FMT_MOF.1(2)										X	X
FMT_MTD.1(1)							X			X	X
FMT_MTD.1(2)							X			X	X
FMT_SMF.1					X						X
FMT_SMR.1					X						X
FPT_ITC.1				X							
FPT_RVM.1			X		X		X	X		X	
FPT_SEP.1			X				X	X		X	
FPT_STM.1			X								
NK-IDS_SDC.1	X										
NK-IDS_ANL.1		X									
NK-IDS_RCT.1						X					
NK-IDS_RDR.1								X			X
NK-IDS_STG.1(1)							X		X	X	X
NK-IDS_STG.1(2)							X		X	X	X

The following discussion provides more detail on the coverage of each security objective.

O.IDSENS
The TOE must collect and store network events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious attack within the IT environment.

> The TOE is required to collect and store network events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious attack within the IT environment. These events must be defined in the ST [NK-IDS_SDC.1].

O.IDANLZ
The TOE must apply analytical processes and information to collected data to derive conclusions about intrusions (past, present, future).

> The TOE is required to perform intrusion and other analytics and generate conclusions [NK-IDS_ANL.1].

O.AUDITS
The TOE must record audit records for configuration changes and use of the TOE functions.

Security relevant events must be defined and auditable for the TOE [FAU_ADG.1]. Furthermore, user identity association in auditable events should provide for accountability [FAU_GEN.2]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1]. Reliable time stamps must be available for use in the audit records [FPT_STM.1].

O.EXPORT
The TOE will ensure the confidentiality of its data when it is transferred across a network.

The TOE must protect its data from disclosure as it is transferred to external systems [FPT_ITC.1].

O.IDAUTH
The TOE must uniquely identify all users, and will authenticate the claimed identity before granting access to the TOE facilities.

Security attributes of subjects used for TOE authentication must be defined [FIA_ATD.1]. Passwords must be specified to meet certain minimum strength metrics [FIA_SOS.1(1), FIA_SOS.1(2)]. Users authorised to access the TOE are defined using an identification and authorisation process [FIA_UAU.1, FIA_UAU.2, FIA_UID.1, FIA_UID.2, FMT_SMF.1]. Feedback during authentication is protected from disclosing too much information about credentials [FIA_UAU.7(1), FIA_UAU.7(2)]. The TOE must appropriately handle the different administrative and user roles [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1].

O.RESPON
The TOE must respond appropriately to analytical conclusions based on the collected data.

The TOE is required to respond accordingly when an intrusion or anomaly is detected [NK-IDS_RCT.1].

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

The TOE is required to protect the audit data from unauthorised deletions and modifications as well as guarantee the availability of the audit data in the event of storage exhaustion [FAU_STG.2]. The same requirements apply to system data [NK-IDS_STG.1(1), NK-IDS_STG.1(2)]. Only authorised administrators and users may access and manage TSF data [FMT_MTD.1(1), FMT_MTD.1(2)]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

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

The TOE must provide the ability to review the audit trails [FAU_SAR.1(1), FAU_SAR.1(2)]. The TOE must provide the ability for authorised administrators and users to view system data and analysis results [NK-IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

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

The TOE is required to protect both audit and system data from unauthorised deletion and modification, and guarantee its availability in the event of storage exhaustion [FAU_STG.2, NK-IDS_STG.1(1), NK-IDS_STG.1(2)]. Furthermore, the TOE must prevent the loss of audit data in the event the audit trail is full [FAU_STG.4].

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

The TOE is required to protect both audit and system data from unauthorised deletion and modification, and guarantee its availability in the event of storage exhaustion [FAU_STG.2, NK-IDS_STG.1(1), NK-IDS_STG.1(2)]. The TOE is required to restrict managing the behavior of TOE functions to authorised users [FMT_MOF.1(1), FMT_MOF.1(2)]. Only authorised administrators and users may access and manage TSF data [FMT_MTD.1(1), FMT_MTD.1(2)]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

O.RBAC

The TOE must prevent users from gaining access to and performing operations on the resources for which their role is not explicitly authorised. The TOE must restrict the review of audit data to those with explicit read-access [FAU_SAR.2]. The TOE is required to protect the stored audit records from unauthorised deletions and modifications and guarantee availability of records after storage exhaustion [FAU_STG.2]. Users authorised to access the TOE are defined using an identification and authorisation process [FIA_UAU.1, FIA_UAU.2, FIA_UID.1, FIA_UID.2, FMT_SMF.1]. The TOE will only allow authorised users to manage the behaviour of TOE functions [FMT_MOF.1(1), FMT_MOF.1(2)]. Only authorised users can query, delete, and manipulate system data [FMT_MTD.1(1), FMT_MTD.1(2)]. The TOE must appropriately handle the different administrative and user roles [FMT_SMR.1]. The TOE must restrict the review of collected system data and results to those with explicit access [NK-IDS_RDR.1]. The TOE must protect system data from unauthorised deletion and modification, and guarantee its availability in the event of storage exhaustion [NK-IDS_STG.1(1), NK-IDS_STG.1(2)].

8.2.2 Rationale for Satisfying Functional Requirement Dependencies

Table 8 – Functional Requirement Dependency Coverage shows that all SFR dependencies from CC (and explicitly stated dependencies) have been met by this ST with explanation.

Table 8 – Functional Requirement Dependency Coverage

Functional Requirement	Dependencies	Satisfied?
FAU_ADG.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1	*FAU_ADG.1
	FIA_UID.1	Yes
FAU_SAR.1	FAU_GEN.1	*FAU_ADG.1
FAU_SAR.2	FAU_SAR.1	Yes
FAU_STG.2	FAU_GEN.1	*FAU_ADG.1
FAU_STG.4	FAU_STG.1	Yes, via hierarchical FAU_STG.2

FIA_UAU.1	FIA_UID.1	Yes
FIA_UAU.7	FIA_UAU.1	Yes
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes
FMT_SMR.1	FIA_UID.1	Yes
NK-IDS_SDC.1	FPT_STM.1[6]	Yes
NK-IDS_ANL.1	NK-IDS_SDC.1	Yes
NK-IDS_RCT.1	NK-IDS_ANL.1	Yes
NK-IDS_RDR.1	NK-IDS_SDC.1 NK-IDS_ANL.1	Yes
NK-IDS_STG.1(1)	NK-IDS_SDC.1	Yes
NK-IDS_STG.1(2)	NK-IDS_ANL.1	Yes

*Dependencies on FAU_GEN.1 are due to SFRs that require audit data to be generated. The extended requirement FAU_ADG.1 is a modified form of FAU_GEN.1 that provides for the generation of audit data. Hence, dependencies on FAU_GEN.1 are satisfied by the requirement FAU_ADG.1.

8.2.3 TOE Security Assurance Requirements Rationale

EAL 2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. At this level, minimal additional tasks are placed upon the vendor that follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the NIKSUN appliance may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment (eg, firewalls, VPN, key card access to physical facilities). At EAL2, the appliance will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.2.4 Rationale for Satisfying Assurance Requirement Dependencies

The EAL 2 assurance package is self-contained with all dependencies satisfied. The explicit dependencies are show in Table 9 – Assurance Requirements Dependency Coverage.

[6] Due to the timestamping of packets, a dependency of NK-IDS_SDC.1 on FPT_STM.1 has been added.

Table 9 – Assurance Requirements Dependency Coverage

Assurance Requirement	Dependencies	Satisfied?
ADO_IGS.1	AGD_ADM.1	Yes
ADV_FSP.1	ADV_RCR.1	Yes
ADV_HLD.1	ADV_FSP.1 ADV_RCR.1	Yes
AGD_ADM.1	ADV_FSP.1	Yes
AGD_USR.1	ADV_FSP.1	Yes
ATE_COV.1	ADV_FSP.1 ATE_FUN.1	Yes
ATE_IND.2	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	Yes
AVA_SOF.1	ADV_FSP.1 ADV_HLD.1	Yes
AVA_VLA.1	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1	Yes

8.3 TOE Summary Specification Rationale

This section provides the rationale for the TOE Summary Specification of security functions and assurance measures.

8.3.1 TOE Security Functions Rationale

This section demonstrates that the TOE security functions are suitable to meet the SFRs included in this ST.

Table 10 – Mapping of SFRs to TOE Security Functions

Functional Requirement	TOE Security Function	Rationale
FAU_ADG.1	NK_FAU	Auditable events tracked in the Activities Log and Export Log satisfy this requirement.
FAU_GEN.2	NK_FAU	Met by user identity being associated with all audit events that result from user activity.
FAU_SAR.1(1)	NK_FAU	Administrators can access audit records throught the GUI.
FAU_SAR.1(2)	NK_FAU	Users can access audit logs through the CLI.
FAU_SAR.2	NK_FAU	Satisfied by fact that Administrators must grant explicit read access to audit records through the GUI.
FAU_STG.2	NK_FAU	Audit log protected through the GUI (no write/delete). Audit log rotation guarantees availability.
FAU_STG.4	NK_FAU	Audit log rotation prevents data loss.
FIA_ATD.1	NK_FIA	GUI and CLI require security attributes for users.
FIA_SOS.1(1)	NK_FIA NK_FMT NK_FPT	GUI account passwords, when initially specified, must meet certain minimum strength metrics. Passwords are verified during authentication. This contributes to TSF protection.
FIA_SOS.1(2)	NK_FIA NK_FMT NK_FPT	CLI account passwords, when initially specified, must meet certain minimum strength metrics. Passwords are verified during authentication. This contributes to TSF protection.
FIA_UAU.1	NK_FIA	Only HTTPS session establishment allowed before GUI authentication.
FIA_UAU.2	NK_FIA	Only login attempt allowed before CLI authentication.
FIA_UAU.7(1)	NK_FIA	Masked password during GUI authentication.
FIA_UAU.7(2)	NK_FIA	No password echo during CLI authentication.
FIA_UID.1	NK_FIA	Only HTTPS session establishment allowed before GUI identification.
FIA_UID.2	NK_FIA	Only login attempt allowed before CLI identification.
FMT_MOF.1(1)	NK_FMT	GUI Administrator can control data collection, review, analysis and reaction.
FMT_MOF.1(2)	NK_FMT	Authorised CLI users can start/stop data collection.
FMT_MTD.1(1)	NK_FMT	Only GUI Admin can query, delete, and manipulate TOE data.

Functional Requirement	TOE Security Function	Rationale
FMT_MTD.1(2)	NK_FMT	Authorised CLI users can query and delete TOE data.
FMT_SMF.1	NK_FMT	Authentication, authorisation, and configuration of functionality is allowed.
FMT_SMR.1	NK_FMT	Administrator, Advanced User, User, and Administrator-defined roles maintained by GUI. Superuser and Appliance User roles in the CLI.
FPT_ITC.1	NK_FMT NK_FPT	HTTPS sessions enforced through GUI and on import/export.
FPT_RVM.1	NK_FPT NK_FIA	Identification and authentication cannot be bypassed. Features not rendered or disabled for unauthorised users.
FPT_SEP.1	NK_FPT	Self-contained appliance. Three separate interfaces into the appliance. Separation of TSF data, system data, and execution.
FPT_STM.1	NK_FPT	Reliable system time provided by OS.
NK-IDS_SDC.1	NK_SDC	Continuous recording of network traffic meets requirement.
NK-IDS_ANL.1	NK_ANL	Statistical metadata, Anomaly, Signature, QoS, RTX, Reconstruction meet requirement.
NK-IDS_RCT.1	NK_ANL	Event viewer, email, SNMP traps, and syslog alerts meet requirement.
NK-IDS_RDR.1	NK_SDC NK_ANL	Raw packet data and reconstructed sessions are restricted to Administrators, Advanced Users, and authorised CLI users. Analysis and event results accessible by all with explicit read access.
NK-IDS_STG.1(1)	NK_SDC NK_ANL	Packet and statistics streams are protected from unauthorised deletion, cannot be modified, and subject to space management and archiving.
NK-IDS_STG.1(2)	NK_ANL	Event data is protected from unauthorised deletion and modification, and keeps last 100,000 alerts.

8.3.2 TOE Assurance Measures Rationale

The documents identified and described in Table 5 – Assurance Measures Mapped to Security Assurance

Requirements provide sufficient evidence in support of EAL2.

8.3.3 Strength of Function Rationale

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information.

The TOE requires passwords to be a minimum of 6 alphanumeric characters. This equates to a password space of approximately $7 \times 10^{+11}$, where on average a brute force attack would have to try half of these values. The probability of guessing a password is low enough to be considered consistent with the SOF-basic rating, which in turn is consistent with the security objectives contained herein.

8.4 PP Claims Rationale

The NIKSUN NetDetector/NetVCR 2005 TOE does not claim conformance to any registered PP.

9 Acronyms

CC	Common Criteria
CLI	Command line interface
DCE	Data Capture Engine
GUI	Graphical User Interface
HTTPS	Secure Hypertext Transfer Protocol
LAN	Local Area Network
NIC	Network interface card
OS	Operating System
PDU	Protocol Data Unit
PP	Protection Profile
QoS	Quality of Service
RTX	Real Time Experts
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation

TSF	TOE Security Function
TSP	TOE Security Policy
UIE	User Interface Engine