SECURITY TARGET FOR THE INTELLITACTICS™ INCORPORATED NETWORK SECURITY MANAGER™ (NSM™)

VERSION 4.1

EWA-Canada Document No. 1447-011-D001
Version 1.13, 18 November 2004

Prepared for:

Intellitactics™ Incorporated
305 King Street W., Suite 800
Kitchener, Ontario
Canada
N2G 1B9

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
55 Metcalfe St., Suite 1600
Ottawa, Ontario
K1P 6L5

SECURITY TARGET FOR THE INTELLITACTICS™ INCORPORATED NETWORK SECURITY MANAGER™ (NSM™) VERSION 4.1

Document No. 1447-011-D001
Version 1.13, 18 November 2004

Original approved by:

Project Engineer:	C. Cantlon	18 November 2004
Project Manager:	E. Connor	18 November 2004
	(Signature)	(Date)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 IDENTIFICATION

This document details the Security Target (ST) for the Intellitactics™ Incorporated Network Security Manager™ (NSM™). This ST has been prepared[1] in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 2.2, Revision 256, January 2004.

1.2 OVERVIEW

This ST specifies the IT security requirements on NSM™ and identifies the functional and assurance security measures provided by it to meet the requirements. The Target of Evaluation Description section describes the NSM™ and identifies the scope and boundaries of the evaluation. The TOE Security Environment section specifies assumptions for the intended environment and usage of NSM™, describes threats that are countered by NSM™ and its environment, and describes organisational policies to which NSM™ conforms.

Section Security Objectives describes the objectives for NSM™ and its supporting environment. Section IT Security Requirements details the security functional and assurance requirements met by NSM™ and the security functional requirements to be met by its operating environment. The TOE Summary Specification describes the security functions of NSM™ and the assurance measures applied to it that meet the IT security requirements for the TOE. Section Protection Profile Claims specifies any Protection Profiles to which NSM™ conforms. Section Rationale, provides evidence as to how the stated assumptions are met, the stated threats are countered, and the stated organisational policies realised by the stated objectives. Evidence is also provided in this section on how the stated objectives are met by the identified IT security requirements and how the security functionality of NSM™, and the assurance measures applied to it, meet the IT security requirements for the TOE.

The NSM™ is a threat management tool that provides a graphic visualisation of security events as they are reported by devices, such as firewalls, routers, and Intrusion Detection System (IDS) sensors, within the monitored network(s). Security events are IT activities that compromise the confidentiality, integrity, availability, or accountability of a IT network.

IT activities for which monitoring devices provide a report and which may or may not indicate an intrusion into the network and an attack on the assets handled by the network. As security events are reported, the NSM™ enforces rules that allow for customised prioritisation, handling, and response of each event.

[1] The ST authors were D. MacFarlane and C. Cantlon of EWA-Canada.

Appropriate physical security measures are expected to exist for the network on which the NSM™ is deployed. The Target of Evaluation (TOE) consists of the following NSM™ components: NSM™ Remote Console, NSM™ Central Server, NSM™ Event Consolidator, NSM™ Reporting System Server, and NSM™ Database.

1.3 CC CONFORMANCE

NSM™ 4.1 is CC Part 2 conformant and CC Part 3 conformant with a claimed Evaluation Assurance Level of EAL2.

1.4 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations are identified in this ST in the following manner:

- **Selection:** Indicated by enclosing brackets and italicised text, e.g., [*selected item*].
- **Assignment:** Indicated by enclosing brackets and regular text, e.g., [assigned item].
- **Refinement:** Indicated by underlined text, e.g., refined item.
- **Iteration:** Indicated by assigning a number at the functional component level, e.g., "FDP_ACC.1, Subset access control (1)" and "FDP_ACC.1, Subset access control (2)".

1.5 TERMINOLOGY

The following terminology is used throughout this document:

Administrators – A subset of *authorised users* that manage and administer the *TOE*.

Attacker – A person whose interactions with the *TOE* are intended to violate the *TSP*.

Audit data – Data generated by the audit mechanism of the *TOE*.

Authentication data – Data used to verify the claimed identity of a *user*.

Authorised user – A *user* who may, in accordance with the *TSP*, perform an operation.

Configuration data – Data used to modify the behaviour of the *TOE*.

Event data – Data regarding a security event that is sent to the *TOE* by a third party security device.

External IT entity – Any IT product or system, untrusted or trusted, outside of the *TOE* that interacts with the *TOE*.

Human user – Any person who interacts with the *TOE*.

Target of Evaluation (TOE) – An IT product or system and its associated *administrator* and *user* guidance documentation that is the subject of an evaluation.

TOE Boundary – A continuous perimeter that defines the bounds of the TOE and thus what is to be evaluated, what are the interfaces to the defined TOE which provide paths for input to, and allow output from, the TOE; and what communications between independent entities are intra-TOE communications.

TOE Security Functions (TSF) – A set consisting of all hardware, software, and firmware of the *TOE* that must be relied upon for the correct enforcement of the *TSP*.

TOE Security Policy (TSP) – A set of rules that regulate how assets are managed, protected, and distributed within a *TOE*.

TSF data – Data created by and for the *TOE* that might affect the operation of the *TOE*, such as *authentication data* and *configuration data*.

TSF Scope of Control (TSC) – The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

Unauthorised user – A *user* who may not, in accordance with the *TSP*, perform an operation.

User – Any entity (*human user* or *external IT entity*) outside the *TOE* that interacts with the *TOE*.

User data – Data created by and for the *user* that does not affect the operation of the *TSF*, such as *event data*.

2 TARGET OF EVALUATION DESCRIPTION

The NSM™ is a threat management tool that provides a graphic visualisation of security events as they are reported by devices within the monitored network(s). The NSM™ enforces rules that allow for customised prioritisation, handling, and response of each security event and is comprised of the following components: NSM™ Remote Console, NSM™ Central Server, NSM™ Event Consolidator, NSM™ Reporting System Server, and NSM™ Database.

2.1 NSM™ COMPONENTS

A typical NSM™ installation is shown in Figure 1.

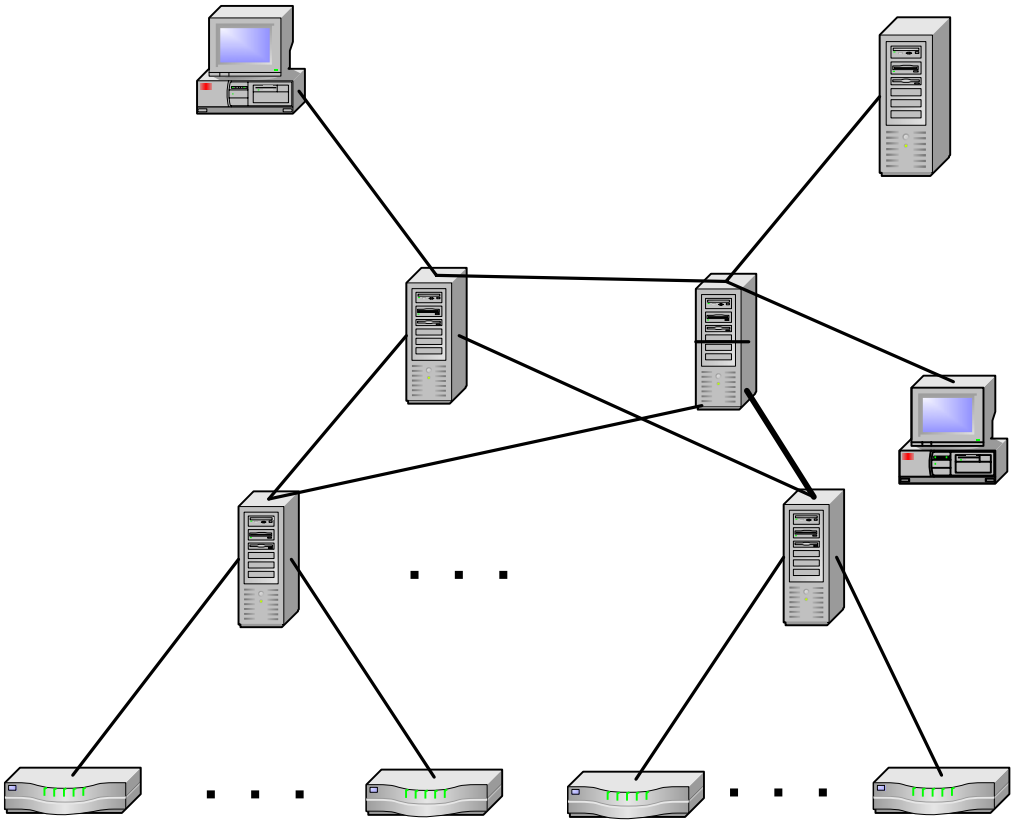


Figure 1. Typical NSM™ Installation

The communications channels shown in Figure 1 occur over an Ethernet network and the following inter-component communication is protected by version 3.0 of the Secure Sockets Layer (SSL) protocol: between the NSM™ Remote Console and the NSM™ Central Server and between NSM™ Central Server and the NSM™ Event Consolidator.

The NSM™ Database stores audit data and the event data received from the security devices. NSM™ supports the use of the following database as the NSM™ Database: MS SQL Server 2000. Figure 1 illustrates a typical installation wherein only a single instance of the database is used. Separate database instances can be used to store event data. These would be installed on the NSM™ Event Consolidator platforms or on platforms directly connected to each NSM™ Event Consolidator.

Audit data may be reviewed using either the NSM™ Remote Console or a web browser launched by the NSM™ Reporting System Server. The NSM™ Remote Console displays the last one hundred audit records and allows access to the records to users in the Audit-review role. The web browser, through the use of the NSM™ Reporting System Server, displays and allows searching of all audit records stored in the NSM™ Database, but only allows access to the records to the Audit-review role.

The NSM™ Remote Console is the Graphical User Interface (GUI) that allows interaction between the NSM™ and the user. Through the NSM™ Remote Console users can view, create, modify, and delete rules on the NSM™ Central Server and any of the NSM™ Event Consolidators, as allowed by their privileges. The NSM™ Remote Console also allows users to view a visual representation of event data to help understand the activity in the monitored network.

The NSM™ Central Server is the centre of the NSM™. It primarily processes messages received from NSM™ Event Consolidators, but also has the ability to process messages received from other NSM™ Central Servers and directly from third-party security devices. The NSM™ Central Server performs user authentication, enforces any rules it contains, and generates audit data for all user-initiated actions performed on the server.

The NSM™ Event Consolidator primarily processes messages from third-party security devices but also has the ability to process messages received from other NSM™ Event Consolidators and the NSM™ Central Server. The NSM™ Event Consolidator enforces any rules it contains; thus it can be used to actively reduce resource utilisation on the NSM™ Central Server. The NSM™ Event Consolidator also generates audit data for all user-initiated actions performed on it.

The NSM™ Reporting System Server is a World Wide Web (WWW) server that allows users to review, search, sort, and generate reports on audit data and stored event data.

All of the NSM™ components proprietary to Intellitactics™ Incorporated (i.e., all of the listed NSM™ components except the NSM™ Database) are developed in the Java® programming language and require a Java® Virtual Machine (JVM) to be installed on the corresponding host Personal Computer (PC).

2.2 EVALUATED CONFIGURATION

The TOE consists of the NSM™ Central Server, the NSM™ Event Consolidator, the NSM™ Reporting System Server, the NSM™ Remote Console, and the NSM™ Database. It shall be referred to collectively as the NSM™ throughout this document.

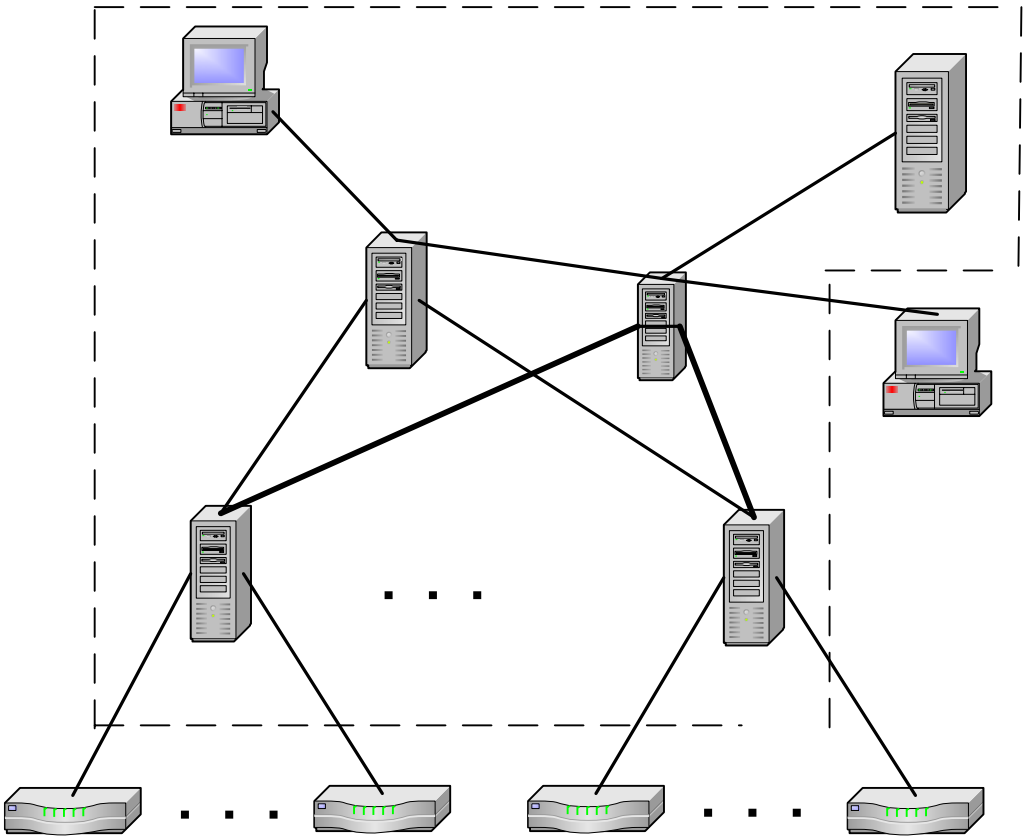
The configuration of each individual NSM™ component in the evaluated configuration is given in Table 1. Figure 2 illustrates where the TOE Boundary is and what platforms are within it. Internet Explorer® is used on the Remote Console for accessing the NSM™ Reporting System Server.

Table 1. Evaluated Configuration

NSM™ Component	Quantity	Configuration
Remote Console	1	Windows® 2000 Server SP4 / Intel®, Internet Explorer® 6 SP1
Central Server	1	Windows® 2000 Server SP4 / Intel®, Internet Explorer® 6 SP1 Stunnel 4.05
Event Consolidator	1	Windows® 2000 Server SP4 / Intel®, Internet Explorer® 6 SP1 Stunnel 4.05
Reporting System Server	1	Windows® 2000 Server SP4 / Intel®, Internet Explorer® 6 SP1 Stunnel 4.05
Database	1	Windows® 2000 Server SP4 / Intel®, Internet Explorer® 6 SP1, Microsoft SQL Server 2000 Stunnel 4.05

Stunnel 4.05 is a third party executable that provides SSL encryption for the transmission of event data from the NSM™ Central Server to the NSM™ Database, from the NSM™ Event Consolidator to the NSM™ Database, and from the NSM™ Database to the NSM™ Reporting System Server. Stunnel does not support the meeting of any security functional claims made for the TOE.

The hardware requirements for each of the NSM™ components and the installation instructions for a secure configuration are specified in the NSM™ Installation Guide.



NSM™ Remo
Console

Figure 2. TOE Boundary Diagram

3 TOE SECURITY ENVIRONMENT

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 resources necessary to perform its functions.

3.1.2 Physical Assumptions

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

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

3.1.3 Personnel Assumptions

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

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

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

3.2 ORGANISATIONAL POLICIES

This section identifies one organisational policy for the TOE.

P.WRNING The TOE must warn potential users that they are not to use the TOE in an unauthorised manner.

3.3 THREATS

This section identifies threats for the TOE and its IT environment. The threat agents are attackers, as defined in Section 1.5, or failures and the assets subject to attack are the data and information that are processed and stored by the TOE.

3.3.1 TOE Threats

The TOE and its IT environment must counter the following threats:

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

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

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

T.NOHALT An unauthorised user may attempt to compromise the continuity of the TOE's analysis functionality by halting execution of the TOE.

T.PRIVIL An unauthorised user may circumvent physical or logical protection for the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON An administrator may inadvertently configure the TOE incorrectly resulting in security events going undetected.

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

T.REPLAY An unauthorised user may use previously captured or falsified data to authenticate to the TOE or alter its configuration.

T.NOCOM Internal TOE communications may be interrupted due to failure in the communication hardware resulting in event data and audit data not being recorded in the database.

T.REACT Hostile agents or unauthorised users may attempt to gain access to a protected network and the user data on it without the knowledge of the protected network's system administrator.

T.AUDEXH An attacker may attempt to hide their malicious actions by flooding the audit logs with legitimate activity to exhaust the audit storage so records of their malicious actions are either overwritten or not collected.

T.IMPERSN An unauthorised user may acquire an authorised user's password and use it to gain access to the TSF and event data without the knowledge of the authorised user or try to gain access to the TSF and event data by guessing the password for a user's account.

3.3.2 IT Environment Threats

Procedural and/or administrative measures must counter the following IT environment threats:

T.USAGE The TOE may unwittingly be operated in an insecure manner by an authorised user exposing event data and graphs to unauthorised modification or allowing for denial of service attacks on the TOE.

T.MANAGE The TOE may unwittingly be managed and administered in an insecure manner by an administrator exposing valid user account information to attackers or preventing the collection of security event data to detect intrusions or the collection of audit data to hold authorised users accountable for their actions.

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 IT SECURITY OBJECTIVES FOR THE TOE

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

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

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

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

O.AUHIST The TOE must provide information so that an authorised user can determine when their account has been breached by an unauthorised user through the presentation of valid authentication data or when an unauthorised user has attempted unsuccessfully to access their account.

O.WARN The TOE must warn potential users that they are not to use the TOE in an unauthorised manner.

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

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

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

O.REPLAY The TOE must be able to protect itself from replay attacks.

O.ACTION The TOE must accept event data from external security devices and then apply analytical process and information to derive conclusions about the reported events.

O.COMM The TOE must provide a mechanism to handle internal communication failures.

4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT OF THE TOE

The IT environment of the TOE must satisfy the following objective.

O.PERFORM The TOE must be protected from interference that would prevent it from performing its functions.

4.3 NON-IT ENVIRONMENT SECURITY OBJECTIVES

The non-IT environment of the TOE must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

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

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

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

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

O.INTROP The TOE is interoperable with the IT system it monitors and the resources of the IT system are accessible to the TOE.

5 IT SECURITY REQUIREMENTS

This section defines the functional and assurance requirements for the TOE and the functional requirements for the IT environment of the TOE. The functional requirements consist of functional components drawn from Part 2 of the CC, and the assurance requirements consist of an Evaluation Assurance Level (EAL) containing assurance components drawn from Part 3 of the CC.

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The functional security requirements for the TOE consist of the components drawn from Part 2 of the CC summarised in Table 2 and two explicitly-stated security functional requirements.

Table 2. Summary of Security Functional Requirements

Functional Components	
Identifier	**Name**
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FAU_SAR.1 (1)	Audit review
FAU_SAR.1 (2)	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3 (1)	Selectable audit review
FAU_SAR.3 (2)	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.2	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
FDP_ACC.1 (1)	Subset access control
FDP_ACC.1 (2)	Subset access control
FDP_ACF.1 (1)	Security attribute based access control
FDP_ACF.1 (2)	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ROL.1	Basic rollback
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_SOS.2	TSF generation of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding

Functional Components	
Identifier	**Name**
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1 (1)	Management of security attributes
FMT_MSA.1 (2)	Management of security attributes
FMT_MTD.1	Management of TSF data
FMT_REV.1	Revocation
FMT_SAE.1	Time-limited authorisation
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPR_UNO.4	Authorised user observability
FPT_FLS.1	Failure with preservation of secure state
FPT_RVM.1	Non-bypassability of the TSP
FPT_STM.1	Reliable time stamps
FRU_FLT.1	Degraded fault tolerance
FTA_TAB.1	Default TOE access banners
FTA_TAH.1	TOE access history
FTA_TSE.1	TOE session establishment
GRP_IFC.2	Complete information flow control to graphs
GRP_IFF.1	Simple attributes for graph creation

FAU_ARP.1 Security Alarms

FAU_ARP.1.1 – The TSF shall take [one or more of the following actions: visual alert, e-mail, SNMP trap] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

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

a. Startup and shutdown of the audit function; (has been removed)
b. All auditable events for the [*minimum*] level of audit; and
c. [all user-initiated events; and
start-up and shutdown of the NSM™ Central Server and the NSM™ Event Consolidator].

Application Note: Auditable events for the default level of audit include all minimum requirements and are identified in Table 3

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

a. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST:
[
- URL – the URL of the graph;
- item_info – item affected;
- NSM™ domain;
- server – the type of NSM™ software component (e.g., Central Server, Event Consolidator);
- IP address – the IP address of the NSM™ Remote Console;
- communication port – the TCP port number of the NSM™ Remote Console; and
- version of the particular NSM™ component].

Table 3. Additional Auditable Events from CC Functional Components

Functional Component	Audit Level	Auditable Event
FAU_ARP.1	Minimal	Actions taken due to imminent security violations.
FAU_SAA.1	Minimal	Enabling and disabling of any of the analysis mechanisms.
	Minimal	Automated responses performed by the tool.
FAU_SEL.1	Minimal	All modifications to the audit configuration that occur while the audit collection functions are operating.
FDP_ACF.1	Minimal	Successful requests to perform an operation on an object covered by the SFP.
FDP_IFF.1	Minimal	Decisions to permit requested information flows.
FDP_ROL.1	Minimal	All successful rollback operations.
FIA_AFL.1	Minimal	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_SOS.1 FIA_SOS.2	Minimal	Rejection by the TSF of any tested secret.
FIA_UAU.1	Minimal	Unsuccessful use of the authentication mechanism.
FIA_UID.1	Minimal	Unsuccessful use of the user identification mechanism, including the user identity provided.
FIA_USB.1	Minimal	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).
FMT_REV.1	Minimal	Unsuccessful revocation of security attributes.
FMT_SMF.1	Minimal	Use of the management functions.
FMT_SMR.1	Minimal	Modifications to the group of users that are part of a role
FPR_UNO.4	Minimal	The observation of the use of a resource or service by a user or subject.
FPT_STM.1	Minimal	Changes to the time.
FRU_FLT.1	Minimal	Any failure detected by the TSF.
FTA_TSE.1	Minimal	Denial of a session establishment due to the session establishment mechanism.

FAU_GEN.2 User identity association

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

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 – The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 – The TSF shall enforce the following rules for monitoring audited events:

a. accumulation of [login failures timed to avoid lockout] known to indicate a potential security violation; and
b. [none].

FAU_SAR.1 Audit review (1)

FAU_SAR.1.1 – The TSF shall provide [the Audit-review role] with the capability to read [all audit data] from the last one hundred audit records via the NSM™ Remote Console.

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

FAU_SAR.1 Audit review (2)

FAU_SAR.1.1 – The TSF shall provide [the Audit-review role] with the capability to read [all audit data] from the audit records via the NSM™ Reporting System Server.

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

FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 – The TSF shall prohibit all users read-access to the audit records via the NSM™ Reporting System Server and via the NSM™ Remote Console, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review (1)

FAU_SAR.3.1 – The TSF shall provide the ability to perform [*ordering*] of audit data based on [date and time, user name, event type, and the graph URL].

FAU_SAR.3 Selectable audit review (2)

FAU_SAR.3.1 – The TSF shall provide the ability to perform [*searches*, *sorting*] of audit data based on [event type, item info, NSM™ domain, server, IP address of NSM™ Remote Console, communication port of NSM™ Remote Console, user name, and graph URL].

FAU_SEL.1 Selective audit

FAU_SEL.1.1 – The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a. [*event type*];
[
b. item info;
c. NSM™ domain;
d. server;
e. IP address of NSM™ Remote Console, if applicable;
f. communication port of NSM™ Remote Console, if applicable; and
g. version of the particular NSM™ component].

FAU_STG.2 Guarantees of audit data availability

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

FAU_STG.2.2 – The TSF shall be able to [*prevent*] modifications to the audit records.

FAU_STG.2.3 – The TSF shall ensure that [the most recent] audit records will be maintained when the following conditions occur: [*audit storage exhaustion*].

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 – The TSF shall [*overwrite the oldest stored audit records*] and [send an alarm via one or more of the following actions: visual alert, SNMP trap, e-mail] if the audit trail is full.

FDP_ACC.1 Subset access control (1)

FDP_ACC.1.1 – The TSF shall enforce the [LOGIN_SFP] on [users authenticating to the TOE].

FDP_ACC.1 Subset access control (2)

FDP_ACC.1.1 – The TSF shall enforce the [ACCESS_SFP] on [authenticated users using the TSF].

FDP_ACF.1 Security attribute based access control (1)

FDP_ACF.1.1 – The TSF shall enforce the [LOGIN_SFP] to objects based on [user name, password, and NSM™ domain].

FDP_ACF.1.2 – The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
a. a user account for 'user name' exists in the selected NSM™ domain; and
b. 'password' matches the password for the identified user account].

FDP_ACF.1.3 – The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 – The TSF shall explicitly deny access of subjects to objects based on the [none].

FDP_ACF.1 Security attribute based access control (2)

FDP_ACF.1.1 – The TSF shall enforce the [ACCESS_SFP] to objects based on [user name, user role, graph permissions, and graph status].

FDP_ACF.1.2 – The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[

a. an authenticated user may only view a graph if the graph permissions grant the View permission to the user role or specific user account;
b. an authenticated user may only make additions (e.g., operators and edges) to a graph if the graph permissions grant the Add permission to the user role or specific user account;
c. an authenticated user may only delete an existing graph if the graph permissions grant the Delete permission to the user role or specific user account;
d. an authenticated user may only make modifications to an existing graph if the graph permissions grant the Modify permission to the user role or specific user account;
e. an authenticated user may only modify the permissions of a graph if the graph permissions grant the Permissions permission to the user role or specific user account;
f. the graph permissions are comprised of an aggregate of the permissions for the user role and user name;
g. the graph status must be set to "locked" before Add, Delete, Modify, or Permissions permission-related operations may be performed on it;
h. only one authenticated user may lock a graph at any given time;
i. the Administrator role can override a lock put on a graph by other user roles;
j. a user may change their own password if the Administrator allows it when creating the account for the user; and
k. the only user role that can manage all aspects of user accounts, including passwords, is the Administrator role].

FDP_ACF.1.3 – The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 – The TSF shall explicitly deny access of subjects to objects based on [none].

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 – The TSF shall enforce the [SSL_SFP] on
a. [subjects: the NSM™ Remote Console, NSM™ Central Server, and NSM™ Event Consolidator components of the TOE;
b. information: event data; and
c. operations: transmission between listed subjects].

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 – The TSF shall enforce the [SSL_SFP] based on the following types of subject and information security attributes:
a. [subject security attributes: CipherSuite; and
b. information security attributes: none].

FDP_IFF.1.2 – The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
a. [the value of CipherSuite on both the transmitting and receiving subject is the same].

FDP_IFF.1.3 – The TSF shall enforce [no additional information flow control rules].

FDP_IFF.1.4 – The TSF shall provide the following [none].

FDP_IFF.1.5 – The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.6 – The TSF shall explicitly deny an information flow based on the following rules: [none].

FDP_ROL.1 Basic rollback

FDP_ROL.1.1 – The TSF shall enforce [ACCESS_SFP] to permit the rollback of the [Add, Delete, and Modify permissions-related operations] on the [graphs].

FDP_ROL.1.2 – The TSF shall permit operations to be rolled back within the [period of time that the following conditions hold: the graph is locked by a user, and another user with the same or higher permissions has not attempted to lock the same graph].

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 – The TSF shall detect when [three] unsuccessful authentication attempts occur related to [consecutive attempts to login to a user account within a settable period of time (default is five minutes)].

FIA_AFL.1.2 – When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lock the user account for a settable period of time (default is ten minutes) and generate one or more of the following notifications: visual alert, e-mail, SNMP trap].

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 – The TSF shall maintain the following list of security attributes belonging to individual users: [user name, password, user role(s), and user account status].

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 – The TSF shall provide a mechanism to verify that secrets meet [the following criteria for user passwords: a minimum length of six characters with at least one change of case, one digit, and one special character].

FIA_SOS.2 TSF generation of secrets

FIA_SOS.2.1 – The TSF shall provide a mechanism to generate secrets that meet [the criteria specified in FIA_SOS.1.1 for user passwords].

FIA_SOS.2.2 – The TSF shall be able to enforce the use of the TSF generated secrets for [user authentication].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 – The TSF shall allow [NSM™ domains to be added or removed] on behalf of the user 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.

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 – The TSF shall provide only [the user name in plain text and each character of the password as a masked character] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

FIA_UID.1.1 – The TSF shall allow [NSM™ domains to be added or removed] on behalf of the user 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.

FIA_USB.1 User-subject binding

FIA_USB.1.1 – The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 – The TSF restrict the ability to [*determine the behaviour of*, *modify the behaviour of*] the function of [audit mechanism] to [users and roles with the appropriate permissions to the /system/audit_rules/ graph].

FMT_MSA.1 Management of security attributes (1)

FMT_MSA.1.1 – The TSF shall enforce the [ACCESS_SFP] to restrict the ability to

a. [*delete* [create]] the security attributes [user name, user role]
b. [*modify* [none]] the security attributes [password, user account status] to [the Administrator role].

Application Note: Deleting and creating the security attributes ‘user name’ and ‘user role’ is analogous to deleting and creating a user account and user role, respectively.

FMT_MSA.1 Management of security attributes (2)

FMT_MSA.1.1 – The TSF shall enforce the [ACCESS_SFP] to restrict the ability to [*modify* [none]] the security attributes [password] to [the Everyone role].

Application Note: As specified in FDP_ACF.1 (2), each user may change their own password but only the Administrator role may change the password of other users.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 – The TSF shall restrict the ability to [*change_default*, *query*, *modify* [none]] the [TSF configuration data] to [all users and roles with corresponding permissions of a graph].

FMT_REV.1 Revocation

FMT_REV.1.1 – The TSF shall restrict the ability to revoke security attributes associated with the [*users*] within the TSC to [the Administrator role].

FMT_REV.1.2 – The TSF shall enforce the rule [of that if a user account has been disabled then the user is denied access to the TSF].

FMT_SAE.1 Time-limited authorisation

FMT_SAE.1.1 – The TSF shall restrict the capability to specify an expiration time for [a user account] to [the Administrator role].

FMT_SAE.1.2 – For each of these security attributes, the TSF shall be able to [disable the user account] after the expiration time for the indicated security attribute has passed.

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 – The TSF shall be capable of performing the following management functions:
a. [create and delete a user account;
b. create and delete user roles;
c. enable and disable a user account;
d. modify a user's password;
e. disallow the ability of a user to change their password for an account;
f. specify an expiration time for a user account; and
g. override default values for information].

FMT_SMR.1 Security roles

FMT_SMR.1.1 – The TSF shall maintain the roles [Administrator, Audit-review, Everyone, View-only, and View-viz-only].

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

FPR_UNO.4 Authorised user observability

FPR_UNO.4.1 – The TSF shall provide [all users and roles with View permission of a graph] with the capability to observe the [editing of the graph (i.e., performing Add, Delete, or Modify permission-related operations)].

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 – The TSF shall preserve a secure state when the following types of failures occur: [loss of the communication path between the NSM™ Central Server and the NSM™ Database, loss of the communication path between the NSM™ Central Server and the NSM™ Event Consolidator, loss of the communication path between the NSM™ Central Server and the NSM™ Remote Console, loss of the communication path between the NSM™ Event Consolidator and the NSM™ Database, loss of the communication path between the NSM™ Event Consolidator and the NSM™ Remote Console, loss of the communication path between the NSM™ Reporting System Server and the NSM™ Central Server, and loss of the communication path between the NSM™ Reporting System Server and the NSM™ Database].

FPT_RVM.1 Non-bypassability of the TSP

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

FPT_STM.1 Reliable time stamps

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

Application Note: In this context, “reliable” means that the chronological order of auditable events is preserved.

FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 – The TSF shall ensure the operation of [event data collection] when the following failures occur: [inter-NSM™ component communication failure].

FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 – Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

FTA_TAH.1 TOE access history

FTA_TAH.1.1 – Upon successful session establishment, the TSF shall display the [*date*, *time*] of the last successful session establishment to the user.

FTA_TAH.1.2 – Upon successful session establishment, the TSF shall display the [*date*, *time*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 – The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 – The TSF shall be able to deny session establishment based on [user account status].

5.2 EXPLICITLY-STATED TOE SECURITY FUNCTIONAL REQUIREMENTS

GRP_IFC.2 Complete information flow control to graphs

GRP_IFC.2.1 – The TSF shall enforce the [GRAPH_SFP] on
a. [subjects: graphs;
b. Information: event data]
and all operations that cause that information to flow to and from subjects covered by the policy.

GRP_IFC.2.2 – The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control policy.

Dependencies: GRP_IFF.1 Simple attributes for graph creation

GRP_IFF.1 Simple attributes for graph creation

GRP_IFF.1.1 – The TSF shall enforce the [GRAPH_SFP] based on the following types of subject and graph decision attributes:
a. [subject attributes: none; and
b. graph decision attributes: facility, facility_ip, facility_zone, priority, s_ip, s_zone, service, t_ip, t_port, t_zone, type, user_id].

GRP_IFF.1.2 – The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
a. [the flow of event data through graphs is controlled by the graphs themselves; and
b. decision points in graphs are based on the selected attribute values].

GRP_IFF.1.3 – The TSF shall enforce [no additional information flow control rules].

GRP_IFF.1.4 – The TSF shall provide the following [none].

GRP_IFF.1.5 – The TSF shall explicitly authorise an information flow based on the following rules:
a. [the initial flow of event data is to the input graph; and
b. the flow of event data to the input graph is always permitted].

GRP_IFF.1.6 – The TSF shall explicitly deny an information flow based on the following rules: [none].

Dependencies: GRP_IFC.1 Subset information flow control to graphs

5.3 SECURITY FUNCTIONAL REQUIREMENTS FOR THE IT ENVIRONMENT

The functional security requirements for the IT environment of the TOE consist of a component from Part 2 of the CC.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 – The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 – The TSF shall enforce separation between the security domains of subjects in the TSC.

5.3 TOE SECURITY ASSURANCE REQUIREMENTS

The security assurance requirements for EAL 2, as specified in Part 3 of the CC, are given in Table 4. A.

Table 4. Assurance Requirements for NSM™

Assurance Class	Assurance Components	
	Identifier	**Name**
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 specification
	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

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

A typical attacker in the intended environment for the NSM™ is deemed to possess only limited knowledge of the system and lack the skills and resources required to manipulate its interfaces. Thus, the attack potential to meet or exceed for AVA_SOF.1 calculations is LOW, and the strength of function claim is SOF-basic. The strength of function claim applies to the combination of security function F.PASS, which enforces minimum password requirements, and F.AUTH, which disables an account for a set period of time when a set number of unsuccessful authentication attempts have been made.

6.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

F.SSL — The TSF implements version 3.0 of the SSL protocol for data communication between the NSM™ Central Server and the NSM™ Remote Console, between the NSM™ Event Consolidator(s) and the NSM™ Remote Console, and between the NSM™ Event Consolidator(s) and the NSM™ Central Server.

F.LOCK — The TOE provides locking of graphs to prevent multiple users from editing the same graph. Multiple users are able to view but not edit the same graph.

F.AUDEVT — The TSF generates an audit record of the following events, and associates each event with the user that caused the event:

a. all user-initiated events (e.g., viewing, modifying, or deleting a graph);
b. start-up and shutdown of the NSM™ Central Server and the NSM™ Event Consolidator;
c. failed and successful user logins; and
d. all other remaining auditable events for the *minimal* level of audit identified in Table 3.

F.AUDINF — The TSF records the following information for each audit event, where applicable:

a. date and time;
b. user name;
c. type of event;
d. outcome of the event (success or failure);
e. URL of the graph;
f. item_info;
g. NSM™ domain;
h. server;

i. IP address of the NSM™ Remote Console,
j. communication port of the NSM™ Remote Console; and
k. version of the NSM™ component where the event originated.

F.AUDSEL The TSF is able to include or exclude auditable events from the set of audited events based on the following attributes:

- event type;
- item info;
- NSM™ domain;
- server;
- IP address of NSM™ Remote Console, if applicable;
- communication port of NSM™ Remote Console, if applicable; and
- version of the particular NSM™ component.

F.ROLE The TSF supports the roles of Administrator, Audit-review, Everyone, View-only, and View-viz-only.

F.TIME The TSF provides a reliable date and time for creating timestamps.

F.ALARM The TSF provides the ability to send an alert by performing a combination of the following actions: displaying a visual alert; sending a e-mail, or causing a SNMP trap. Alarms are sent when the following events occur:

a. audit storage is exhausted;
b. user account is locked out;
c. attempts to authenticate to a user account that is locked out;
d. user name and/or password not provided during an authentication attempt;
e. unsuccessful attempts to authenticate a user, i.e. incorrect password;
f. account is disabled;
g. account has expired;
h. user account for the specified user name is not found; and
i. accumulation of login failures timed to avoid lockout which is a potential security policy violation.

F.AUDRVW The TOE provides the ability to view audit records using the NSM™ Remote Console and a web browser with the NSM™ Reporting System Server. Through the NSM™ Remote Console, the Audit-review role may review the most recent one hundred audit records. The NSM™ Reporting System Server allows the Audit-review role to review all audit data stored in the NSM™ Database. In both cases, the audit data may be ordered based on the following attributes:

a. date and time;
b. user name;
c. event type; and
d. URL of the graph.

F.AUDRPT The TOE provides the Audit-review role with the ability to generate reports of audit data through the NSM™ Reporting System Server by searching and sorting the data based on the following attributes:

a. event type;
b. item info;
c. NSM™ domain;
d. server;
e. IP address of NSM™ Remote Console;
f. communication port of NSM™ Remote Console;
g. user name; and
h. graph URL.

F.AUDSTO The TSF protects audit records from unauthorised modification and deletion and ensures that the most recent audit records are maintained in the case of audit storage exhaustion by overwriting the oldest stored audit records.

F.AUTH Other than adding or removing potential NSM™ domains, access to the TSF is restricted to users who authenticate to an existing NSM™ domain with a valid user name and password. Prior to authentication, a warning is displayed to the user regarding unauthorised use of the TSF. During authentication, the user's password is not displayed to the user but is displayed as a series of masked characters. If a user account has been disabled then all authentication attempts are denied. If a user makes three consecutive unsuccessful attempts to authenticate to a user account within a settable period of time (default is five minutes), then an alarm is generated and the account is locked out for a settable period of time (default is ten minutes).

F.HIST Upon successful authentication, the date and time of the previous successful authentication is displayed to the user. The date and time of the most recent unsuccessful authentication attempt and the total number of unsuccessful authentication attempts since the last successful authentication is also displayed. The authentication history cannot be erased without review by the user.

F.PASS The TSF provides a mechanism to verify that user passwords meet a minimum length of six characters with at least one change of case, one digit, and one special character. The same mechanism can generate passwords that meet these criteria and enforce their use.

F.USER The graph permissions granted to a user role and explicitly to a user determine which tasks the user may perform. The graph permissions are comprised of an aggregate of the permissions for the user role and the user name if the permissions granted to the user and to the user role the user is assigned are not the same. User roles are implemented through groups. The TSF provides a limited ability for the user to rollback operations performed on graphs. The TSF provides each user with the ability to change their password. Subjects that act on behalf of the user inherit the roles and graph permissions associated with that user.

F.ADMIN The TSF provides the Administrator role with the following capabilities:

a. create and delete a user account;
b. create and delete user roles;
c. enable and disable a user account;
d. modify a user's password;
e. disallow the ability of a user to change their password for an account;
f. specify an expiration time for a user account; and
g. override default values for information.

F.ACTION The TSF applies analytical processes and information to all received security event data by passing the data through the graphs, beginning with the input graph. The TSF performs the actions specified in the graphs as a result of these processes. Where graphs are sent – to a database, to other servers in the system via LMP messages, or to an e-mail address – depends on operators which make a decision based upon the graph decision attributes for the graph.

F.FAILSAFE The TSF shall maintain a secure state when the following failures occur:

a. loss of the communication path between the NSM™ Central Server and the NSM™ Database,
b. loss of the communication path between the NSM™ Central Server and the NSM™ Event Consolidator,
c. loss of the communication path between the NSM™ Central Server and the NSM™ Remote Console,
d. loss of the communication path between the NSM™ Event Consolidator and the NSM™ Database,
e. loss of the communication path between the NSM™ Event Consolidator and the NSM™ Remote Console,
f. loss of the communication path between the NSM™ Reporting System Server and NSM™ Central Server, and
g. loss of the communication path between the NSM™ Reporting System Server and the NSM™ Database.

In addition, the TSF shall ensure the operation of the following functions in the case of each failure:

a. collection of event data to be resent to the intended NSM™ component.

F.STARTUP The TOE ensures that all its components are started before it becomes responsive to its Remote Consoles and its listeners (SNMP, Syslog, LMP, SMTP). The message listeners are not enabled until all other components of the TOE have completed their startup and the TOE does not listen to requests from its Remote Consoles until its graphs have been loaded.

6.2 SECURITY FUNCTIONAL POLICIES

6.2.1 Security Functional Policy for Authenticating (Logging In) to NSM™ (LOGIN_SFP)

Users must authenticate to NSM™ to be able to access its security functions and the objects under its control. User accounts are created to authorize the access of users and require the specification of a user name, password, and NSM™ domain.

Passwords must have a minimum length of six characters with at least one digit, one special character, and one change of case, i.e. at least one upper case alpha character if the rest of the alpha characters are in lower case or at least one lower case alpha character if the rest of the alpha characters are in upper case. NSM™ verifies that passwords meet these criteria when they are created and has the capability to generate user passwords that meet the required criteria. NSM™ can enforce the use of generated passwords for a user account.

A user requesting access to NSM™ must provide the user name and the corresponding password for an existing user account. When entered the user name is displayed in plain text and each character of the password is masked. The only action allowed before a user is successfully authenticated to NSM™ is the addition or removal of an NSM™ domain.

6.2.2 Security Functional Policy for Access Control to NSM™ Controlled Objects (ACCESS_SFP)

NSM™ enforces the ACCESS_SFP on all authenticated users to NSM™. Access to controlled objects is allowed based upon the user name of the account to which the user has authenticated, the user role in which the user is acting, the graph permissions set for the user name or the user role, and the status of the graph.

An authenticated user acting in a user role and authenticated to a user account may only:

- View a graph if either the user role or the user account has the View permission to the graph;
- Make additions (e.g., operators and edges) to a graph if either the user role or the user account has the Add permission for the graph;
- Delete an existing graph if either the user role or the user account has the Delete permission for the graph;
- Make modifications to a graph if either the user role or the user account has the Modify permission for the graph; or
- Modify the permissions for a graph if either the user role or the user account has the Permissions permission for the graph.

The graph status can have one of two values: locked or unlocked. The graph status for the graph must be set to "locked" before a user can make additions to the graph, delete the graph, make modifications to the graph, or modify the permissions for the graph. Only one authenticated user may lock a graph at one time, but users acting in the Administrator role may override a lock put on a graph by a user acting in any other type of role.

NSM™ allows the rollback of the add, delete, and modify operations on graphs during the time the graph is locked by the user and another user with the same or higher permissions has not attempted to lock the particular graph. Once the graph is unlocked, the add, delete, and modify operations cannot be rolled back.

User accounts must be created by administrators acting in the Administrator role. The Administrator role is the only role that can manage all aspects of a user account. NSM™ has a default administrator account so that initial access to NSM™ is controlled. An administrator acting in an Administrator role must set the initial password for a user account. The account owner, however, can change the password for their account if the Administrator allows it when creating the account.

Only administrators acting in the Administrator role can create or delete the role for a user account.

6.2.3 Security Functional Policy for the Protection of Event Data Transmitted Between Physically-Separate Components of NSM™ (SSL_SFP)

Event data communicated between the physically-separated components of the NSM™ Central Server and the NSM™ Remote Console, between the physically-separated components of the NSM™ Event Consolidator(s) and the NSM™ Remote Console, and between the physically-separated NSM™ Event Consolidator(s) and the NSM™ Central Server must be protected by the use of the Secure Sockets Layer (SSL) protocol (version 3.0). The flow of event data between the transmitting and the receiving subject is only allowed if the subjects have the same value of CipherSuite set.

6.2.4 Security Functional Policy for the Flow of Event Data to NSM™ Graphs (GRAPH_SFP)

NSM™ enforces the GRAPH_SFP on the flow of event data to graphs. This security functional policy is enforced based upon the graph decision attributes of facility, facility_ip, facility_zone, priority, s_ip, s_zone, service, t_ip, t_port, t_zone, type, and user_id.

The flow of event data through the graphs is controlled by the graphs themselves and the decision points in the graphs are based on the graph decision attribute values. The initial flow of event data is to the input graph. The flow of event data to the input graph is always permitted. Where graphs are sent – to a database, to other servers in the system via LMP messages, or to an e-mail address – depends on the operator which makes a decision based upon the graph decision attributes for the graph.

6.3 ASSURANCE MEASURES

A description of each of the TOE assurance measures follows.

M.ID The TOE incorporates a unique version identifier that can be displayed to the user.

M.SYSTEM The TOE is developed and maintained using a system to ensure only authorised changes are implemented in the evaluated version of the TOE. This system is documented.

A list of all TOE documentation and all configuration items required to create the TOE is maintained.

M.GETTOE The developer has a controlled process and procedures whereby the developer ships a copy of the TOE to a customer on CD-ROM, secured in its package with a tamper-proof seal. The process and procedures are documented.

M.SETUP The TOE includes an automated installation and set-up program compatible with the TOE operating system. The installation process is self-explanatory, and there are additional instructions to clearly document the installation process in the *NSM Installation and Configuration Guide*. The default installation results in the secure installation and start-up of the TOE.

M.SPEC A high-level design and functional specification of the TOE have been provided by the developer for the evaluation. The documents describe the TOE security functionality, subsystems, and interfaces.

M.TRACE Correspondence mappings are provided by the developer such that the security functionality detailed in the TOE functional specification is upwards traceable to this ST and downwards traceable to the high-level design.

M.DOCS Sufficient user and administrator guidance documentation is provided. The user guidance is provided in the document *NSM Basics Guide* and administrator guidance is provided in the document *NSM Administrator's Guide*.

M.TEST A suitably configured TOE is tested in a controlled environment to confirm that TOE functionality operates as specified, and that the TOE is protected from a representative set of well-known attacks. These tests are described in terms of setup, procedure, expected results, and actual results.

A mapping between developer test cases and TOE functionality has been documented by the developer. The assurance requirements also ensure the TOE functionality is tested in a real-world environment.

M.PROVIDE The developer has provided a suitable TOE for testing.

M.SECASS The developer examines the TOE design to ensure the security functions adequately address perceived threats in the security environment. The results of the examination are documented. Threats include deliberate attempts to disable, bypass, and brute-force attack the TSF.

The strength of passwords that can be set and accepted as valid authentication data by the NSM™ is also analysed and documented.

7 PROTECTION PROFILE CLAIMS

This ST does not claim conformance to a Protection Profile.

8 RATIONALE

This section contains the Rationale arguments and proof.

8.1 SECURITY OBJECTIVES RATIONALE

8.1.1 IT Security Objectives Rationale

This section provides rationale for how each TOE organisational policy and threat is addressed by the IT security objectives for both the TOE and the TOE's IT environment (O.PERFORM). Table 5 summarises the mapping of objectives to threats.

Table 5. Threats vs. IT Security Objectives

	O.WARN	O.PROTCT	O.EADMIN	O.ACCESS	O.IDAUTH	O.AUHIST	O.OFLOWS	O.AUDITS	O.INTEGR	O.REPLAY	O.ACTION	O.COMM	O.PERFORM
P.WRNING	X												
T.COMINT		X		X	X				X				X
T.COMDIS		X		X	X								X
T.LOSSOF		X		X	X				X				X
T.NOHALT				X	X								X
T.PRIVIL		X		X	X								X
T.IMPCON			X	X	X			X					
T.INFLUX							X						
T.REPLAY										X			
T.NOCOM												X	
T.REACT											X		
T.AUDEXH T.IMPERSN						X	X						

P.WRNING *The TOE must warn potential users that they are not to use the TOE in an unauthorised manner.*

O.WARN ensures that the TOE warns potential users that they are not to use the TOE in an unauthorised manner.

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

O.PROTCT provides protection from unauthorised modifications to TOE data. O.IDAUTH requires that users authenticate to the TOE prior to accessing any TOE data, while O.ACCESS only allows users to access TOE data that is appropriate for that user. O.INTEGR ensures that TOE data will not be modified. O.PERFORM ensures that the TOE will be protected from interference in the performance of its functions.

T.COMDIS *An unauthorised user may attempt to disclose the data analysed and produced by the TOE by bypassing a security mechanism.*

O.PROTCT provides protection from unauthorised access to TOE data. O.IDAUTH requires that users authenticate to the TOE prior to accessing any TOE data, while O.ACCESS only allows users to access TOE data that is appropriate for that user. O.PERFORM ensures that the TOE will be protected from interference in the performance of its functions.

T.LOSSOF *An unauthorised user may attempt to remove or destroy data analysed and produced by the TOE.*

O.PROTCT provides protection from unauthorised modifications to TOE data. O.IDAUTH requires that users authenticate to the TOE prior to accessing any TOE data, while O.ACCESS only allows users to access TOE data that is appropriate for that user. O.INTEGR ensures that TOE data will not be deleted. O.PERFORM ensures that the TOE will be protected from interference in the performance of its functions.

T.NOHALT *An unauthorised user may attempt to compromise the continuity of the TOE's analysis functionality by halting execution of the TOE.*

O.IDAUTH requires that users authenticate to the TOE prior to accessing any TOE functions, while O.ACCESS only allows users to access TOE functions that are appropriate for that user. O.PERFORM ensures that the TOE will be protected from interference in the performance of its functions.

T.PRIVIL *An unauthorised user may circumvent physical or logical protection for the TOE and exploit system privileges to gain access to TOE security functions and data.*

O.PROTCT provides protection from unauthorised access to TOE functions and data. O.IDAUTH requires that users authenticate to the TOE prior to accessing any TOE functions and data, while O.ACCESS only allows users to access TOE functions and data that are appropriate for that user. O.PERFORM ensures that the TOE will be protected from interference in the performance of its functions.

T.IMPCON *An administrator may inadvertently configure the TOE incorrectly resulting in security events going undetected.*

O.EADMIN ensures that the TOE has all of the necessary administrator functions to manage the TOE. O.IDAUTH requires that users authenticate to the TOE prior to accessing any TOE functions and O.AUDITS ensures that all access to TOE functions and data are audited when the TOE is improperly configured it can be determined who did it and when. O.ACCESS only allows users to access TOE functions that are appropriate for that user.

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

O.OFLOWS ensures that the TOE is able to handle data storage overflows.

T.REPLAY *An unauthorised user may use previously captured data to alter its configuration.*

O.REPLAY ensures that the TOE is protected from replay attacks.

T.NOCOM *Internal TOE communications may be interrupted due to failure in the communication hardware resulting in event data and audit data not being recorded in the database.*

O.COMM ensures that the TOE has a mechanism to handle TOE internal communication failures.

T.REACT *Hostile agents or unauthorised users may attempt to gain access to a protected network and the user data on it without the knowledge of the protected network's system administrator.*

O.ACTION ensures that the TOE reacts accordingly to inappropriate activity reported by the security devices so that the administrator of the protected network is made aware of the activity.

T.AUDEXH *An attacker may attempt to hide their malicious actions by flooding the audit logs with legitimate activity to exhaust the audit storage so records of their malicious actions are either overwritten or not collected.*

O.OFLOWS ensures that the TOE can appropriately handle potential audit storage overflows.

T.IMPERSN *An unauthorised user may acquire an authorised user's password and use it to gain access to the TSF and event data without the knowledge of the authorised user or try to gain access to the TSF and event data by guessing the password for a user's account.*

O.AUHIST ensures that the TOE provides information so that an authorised user can determine when their account has been breached by an unauthorised user through the presentation of valid authentication data or when an unauthorised user has attempted unsuccessfully to access their account.

8.1.2 Environment Security Objectives Rationale

This section provides rationale for how each assumption and IT environment threat is addressed by the environment security objectives. Table 6 summarises the mapping of objectives to assumptions and IT environment threats.

Table 6. Assumptions and Threats vs. Environment Security Objectives

	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP
A.ACCESS					X
A.PROTCT		X			
A.LOCATE		X			
A.MANAGE				X	
A.NOEVIL	X	X		X	
A.NOTRST		X	X		
T.USAGE				X	
T.MANAGE				X	

A.ACCESS *The TOE has access to all the IT system resources necessary to perform its functions.*

O.INTROP ensures that the TOE has access to the required IT system resources.

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

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

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

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

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

O.PERSON ensures that all administrators are qualified and trained to manage the TOE.

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

O.INSTAL ensures that the TOE is properly installed and configured. O.PHYCAL provides for the physical protection of the TOE. O.PERSON ensures that users and administrators are properly trained.

A.NOTRST *The TOE can only be accessed by authorised users.*

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

T.USAGE *The TOE may unwittingly be operated in an insecure manner by an authorised user exposing event data and graphs to unauthorised modification or allowing for denial of service attacks on the TOE.*

O.PERSON ensures that all authorised users are qualified and trained to operate the TOE.

T.MANAGE *The TOE may unwittingly be managed and administered in an insecure manner by an administrator exposing valid user account information to attackers or preventing the collection of security event data to detect intrusions or the collection of audit data to hold authorised users accountable for their actions.*

O.PERSON ensures that all administrators are qualified and trained to manage and administer the TOE.

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 Security Functional Requirements Rationale

This section provides rationale describing how IT security objectives for the TOE are addressed by the TOE security functional requirements. Table 7 summarises the mapping of TOE security functional requirements to IT security objectives.

Table 7. Security Functional Requirements vs. IT Security Objectives

	O.PROTCT	O.EADMIN	O.ACCESS	O.IDAUTH	O.AUHIST	O.WARN	O.OFLOWS	O.AUDITS	O.INTEGR	O.REPLAY	O.ACTION	O.COMM
FAU_ARP.1	X											
FAU_GEN.1								X				
FAU_GEN.2								X				
FAU_SAA.1	X											
FAU_SAR.1 (1)		X										
FAU_SAR.1 (2)		X										
FAU_SAR.2			X									
FAU_SAR.3 (1)		X										
FAU_SAR.3 (2)		X										
FAU_SEL.1		X						X				
FAU_STG.2	X		X				X		X			
FAU_STG.4							X					
FDP_ACC.1 (1)			X	X								
FDP_ACC.1 (2)			X									
FDP_ACF.1 (1)			X	X								
FDP_ACF.1 (2)			X									
FDP_IFC.1										X		
FDP_IFF.1										X		
FDP_ROL.1		X										
FIA_AFL.1		X		X								
FIA_ATD.1			X	X								
FIA_SOS.1				X								
FIA_SOS.2				X								
FIA_UAU.1			X	X								
FIA_UAU.7				X								
FIA_UID.1			X	X								
FIA_USB.1			X									
FMT_MOF.1	X	X	X									
FMT_MSA.1 (1)	X	X	X									
FMT_MSA.1 (2)	X	X	X									
FMT_MTD.1	X	X	X									
FMT_REV.1	X	X	X									
FMT_SAE.1	X	X	X									
FMT_SMF.1	X	X	X									
FMT_SMR.1	X	X	X									
FPR_UNO.4		X										
FPT_FLS.1	X											X

	O.PROTCT	O.EADMIN	O.ACCESS	O.IDAUTH	O.AUHIST	O.WARN	O.OFLOWS	O.AUDITS	O.INTEGR	O.REPLAY	O.ACTION	O.COMM
FPT_RVM.1	X	X		X				X	X			
FPT_STM.1								X				
FRU_FLT.1	X											X
FTA_TAB.1						X						
FTA_TAH.1					X							
FTA_TSE.1				X								
GRP_IFC.2											X	
GRP_IFF.1											X	

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

The TOE is required to automatically respond to a potential security violation [FAU_ARP.1]. The TOE is required to monitor the audited events for a potential security violation [FAU_SAA.1]. The TOE is required to protect the audit data from unauthorised deletion as well as guarantee its availability in the event of audit storage exhaustion [FAU_STG.2]. The TOE must ensure that only authorised users have the ability to manage the behaviour of the TOE security functions security attributes, their default values and expiration, and the behaviour of TOE functions [FMT_MOF.1, FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_SAE.1, FMT_SMF.1, FMT_SMR.1]. The TOE must ensure that only authorised users have the ability to manage TSF data [FMT_MTD.1, FMT_SMF.1]. The TOE must ensure that only administrators have the ability to revoke security attributes [FMT_REV.1, FMT_SMR.1]. The TOE must preserve a secure state and ensure operation of identified functions when a failure occurs [FPT_FLS.1, FPT_FLT.1]. The TOE must ensure that functions enforcing the TSP run successfully, so that data and TSF are protected, before other functions within the TSC are allowed to proceed [FPT_RVM.1].

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

The TOE must provide the ability to review and manage the audit trail [FAU_SAR.1 (1), FAU_SAR.1 (2), FAU_SAR.3 (1), FAU_SAR.3 (2), FAU_SEL.1]. The TOE must provide the ability to undo operations performed while creating and editing graphs [FDP_ROL.1]. The TOE must alert the administrator when too many failed authentication attempts occur [FIA_AFL.1]. The TOE must provide the ability to manage security attributes, their default values and expiration, and the behaviour of TOE functions to authorised users only [FMT_MOF.1, FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_SAE.1, FMT_SMF.1, FMT_SMR.1]. The TOE must provide the ability to manage TSF data to authorised users only [FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The TOE must provide the ability to revoke security attributes to administrators only [FMT_REV.1, FMT_SMR.1]. The TOE must provide the ability for authorised users to observe the usage of services [FPR_UNO.4]. The TOE must ensure that functions enforcing the TSP run successfully, so that data and TSF are protected, before other functions within the TSC are allowed to proceed [FPT_RVM.1].

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

The TOE is required to restrict the review of audit data via the NSM™ Reporting System Server or via the NSM™ Remote Console to those granted explicit read-access [FAU_SAR.2]. The TOE is required to protect the audit data from unauthorised deletion [FAU_STG.2]. The TOE is required to restrict access to the TSF to users with a valid user name and password [FDP_ACC.1 (1), FDP_ACF.1 (1)]. The TOE is required to regulate interaction with the TSF based on permissions [FDP_ACC.1 (2), FDP_ACF.1 (2)]. The TOE must maintain user roles, through groups, and their associated graph permissions [FIA_ATD.1]. Users authorised to access the TOE functions and data are defined using an identification and authentication process [FIA_UAU.1, FIA_UID.1]. The TOE must ensure that subjects acting on behalf of the user have the same level of access to TOE functions and data [FIA_USB.1]. The TOE must ensure that only authorised users have the ability to manage security attributes, their default values and expiration, and the behaviour of TOE functions [FMT_MOF.1, FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_SAE.1, FMT_SMF.1, FMT_SMR.1]. The TOE must ensure that only authorised users have the ability to manage TSF data [FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The TOE must ensure that only administrators have the ability to revoke security attributes [FMT_REV.1].

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

The TOE is required to enforce an access control policy on users authenticating to the TOE [FDP_ACC.1 (1), FDP_ACF.1 (1)]. The TOE must respond accordingly when a user fails too many authentication attempts by locking out the user account so an attacker cannot gain access and by notifying the administrator of the possible attack [FIA_AFL.1]. The TOE must maintain the user name and password of all users [FIA_ATD.1]. The TOE must ensure that user passwords are non-trivial such that an attacker cannot guess the password and gain unauthorised access to TOE functions and data [FIA_SOS.1]. The TOE must provide the capability to auto-generate user passwords and enforce their use [FIA_SOS.2]. Users authorised to access the TOE functions and data are defined using an identification and authentication process [FIA_UAU.1, FIA_UID.1]. The TOE must only provide limited feedback during authentication so an attacker does not have information that can be used to guess the password [FIA_UAU.7]. The TOE must be able to deny authentication attempts if a user account has been disabled [FTA_TSE.1]. The TOE must ensure that functions enforcing the TSP run successfully, so that data and TSF are protected, before other functions within the TSC are allowed to proceed [FPT_RVM.1].

O.AUHIST *The TOE must provide information so that an authorised user can determine when their account has been breached by an unauthorised user through the presentation of valid authentication data or when an unauthorised user has attempted unsuccessfully to access their account.*

The TOE is required to provide an access history to an authenticated user showing the date and time of the last authenticated access to the account so that the authorised user can determine if the account has been breached by presentation of valid authentication information or so that the authorised user can determine how many unsuccessful attempts have been made to access their account [FTA_TAH.1].

O.WARN *The TOE must warn potential users that they are not to use the TOE in an unauthorised manner.*

The TOE is required to display a warning message that the TOE is not to be used in an unauthorised manner to potential users [FTA_TAB.1].

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

The TOE is required to guarantee the availability of audit data in the event of audit storage exhaustion [FAU_STG.2]. The TOE is required to prevent the loss of audit data in the event the audit trail is full [FAU_STG.4].

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

Security relevant events must be defined and auditable for the TOE [FAU_GEN.1]. All auditable events must be associated with the user that caused the event [FAU_GEN.2]. The TOE must provide the capability to select, which security-relevant events are, audited [FAU_SEL.1]. The TOE must provide a reliable timestamp for inclusion in audit records [FPT_STM.1]. The TOE must ensure that functions enforcing the TSP run successfully, so that data and TSF are protected, before other functions within the TSC are allowed to proceed [FPT_RVM.1].

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

The TOE is required to protect the audit data from unauthorised deletion as well as guarantee its availability in the event of audit storage exhaustion [FAU_STG.2]. The TOE must ensure that functions enforcing the TSP run successfully, so that data and TSF are protected, before other functions within the TSC are allowed to proceed [FPT_RVM.1].

O.REPLAY *The TOE must be able to protect itself from replay attacks.*

The TOE must use the SSL protocol when transmitting configuration data between distributed components to protect against insertion and replay attacks [FDP_IFC.1, FDP_IFF.1].

O.ACTION *The TOE must accept event data from external security devices and then apply analytical process and information to derive conclusions about the reported events.*

The TOE passes all event data through the defined graphs [GRP_IFC.2, GRP_IFF.1].

O.COMM *The TOE must provide a mechanism to handle internal communication failures.*

The TOE must maintain a secure state [FPT_FLS.1] and continue to collect event data for future storage in the case of communication failures [FRU_FLT.1].

8.2.2 Rationale for Security Functional Requirements for the IT Environment of the TOE

This section provides rationale describing how the security objective, O.PERFORM, for the IT environment of the TOE is addressed by the security functional requirement for the IT environment, FPT_SEP.1.

O.PERFORM *The TOE must be protected from interference that would prevent it from performing its functions.*

The operating system on which the TOE runs must provide and maintain a security domain for the execution of the TOE that protects it from interference and tampering by untrusted subjects and must enforce separation of the security domains of TSF subjects [FPT_SEP.1].

8.2.3 Assurance Requirements Rationale

The NSM™ is designed to consolidate and manage event data received from security devices in the deployed network and is intended for use by an average PC user. An assurance level of EAL 2, structurally tested, was selected as the threat to security is considered to be unsophisticated attackers and the resources to be protected consist mainly of system resources and event data. It is felt that an evaluation at this level provides evidence that the TOE functions in a manner consistent with its documentation and that it provides useful protection against the identified threats.

8.2.4 Rationale for Satisfying Security Functional Component Dependencies for the TOE

Table 8 identifies the Security Functional Requirements for the TOE and their associated dependencies, and also indicates whether the ST explicitly addresses each dependency.

Table 8. Security Functional Component Dependencies

Functional Component	Dependencies	Dependency Satisfied?
FAU_ARP.1	FAU_SAA.1	Yes
FAU_ GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1	Yes
	FIA_UID.1	Yes
FAU_SAA.1	FAU_GEN.1	Yes
FAU_ SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_ SAR.1	Yes
FAU_ SEL.1	FAU_GEN.1	Yes
	FMT_MTD.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes (FAU_STG.2 is hierarchical to FAU_STG.1)

Functional Component	Dependencies	Dependency Satisfied?
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_ MSA.3	No
FDP_IFC.1	FDP_IFF.1	Yes
FDP_ IFF.1	FDP_IFC.1	Yes
	FMT_MSA.3	No
FDP_ROL.1	FDP_ACC.1 or FDP_IFC.1	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	–	–
FIA_SOS.1	–	–
FIA_SOS.2	–	–
FIA_UAU.1	FIA_UID.1	Yes
FIA_UAU.7	FIA_UAU.1	Yes
FIA_UID.1	–	–
FIA_USB.1	FIA_ATD.1	Yes
FMT_ MOF.1	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Yes
	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_REV.1	FMT_SMR.1	Yes
FMT_SAE.1	FMT_SMR.1	Yes
	FPT_STM.1	Yes
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Yes
FPR_UNO.4	–	–
FPT_FLS.1	ADV_SPM.1	No
FPT_RVM.1	--	--
FPT_ STM.1	–	–
FRU_FLT.1	FPT_FLS.1	Yes
FTA_TAB.1	–	–
FTA_TAH.1	–	–
FTA_TSE.1	–	–
GRP_IFC.2	GRP_IFF.1	Yes
GRP_IFF.1	GRP_IFC.1	Yes, hierarchical component included

8.2.5 Rationale for Security Functional Requirement Dependencies for the TOE That Are Not Satisfied

FMT_MSA.3 Static attribute initialisation for FDP_ACF.1 Security attribute based access control (1) and (2) and for FDP_IFF.1 Simple security attributes

This security functional requirement has not been included because the FDP_ACF.1 Security attribute based access control (1) and (2) attributes are initialised by an administrator and because the FDP_IFF.1 Simple security attributes CipherSuite value attribute cannot be changed.

ADV_SPM.1 Informal security policy model for FPT_FLS.1 Failure with preservation of secure state

The document *NSM Secure State and Secure Values* describes how the TOE is kept in a secure state when a failure occurs.

8.2.6 Rationale for Satisfying Security Functional Component Dependencies for the IT Environment of the TOE

The only security functional requirement for the IT environment of the TOE is FPT_SEP.1 and this component has no dependencies.

8.2.7 Rationale for Satisfying Security Assurance Requirement Dependencies

Table 9 identifies the Security Assurance Requirements and their associated dependencies, and also indicates whether the ST explicitly addresses each dependency.

Table 9. Security Assurance Component Dependencies

Assurance Component	Dependencies	Dependency Satisfied?
ACM_CAP.2	–	–
ADO_DEL.1	–	–
ADO_IGS.1	AGD_ADM.1	Yes
ADV_FSP.1	ADV_RCR.1	Yes
ADV_HLD.1	ADV_FSP.1	Yes
	ADV_RCR.1	Yes
ADV_RCR.1	–	–
AGD_ADM.1	ADV_FSP.1	Yes
AGD_USR.1	ADV_FSP.1	Yes
ATE_COV.1	ADV_FSP.1	Yes
	ATE_FUN.1	Yes
ATE_FUN.1	–	–
ATE_IND.2	ADV_FSP.1	Yes
	AGD_ADM.1	Yes
	AGD_USR.1	Yes
	ATE_FUN.1	Yes

Assurance Component	Dependencies	Dependency Satisfied?
AVA_SOF.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes
AVA_VLA.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes
	AGD_ADM.1	Yes
	AGD_USR.1	Yes

8.2.8 Rationale for Security Functional Refinements

FAU_GEN.1 Audit data generation

In FAU_GEN.1.1, removed the auditable event, "start-up and shutdown of the audit functions", as the audit functions are automatically started and may not be shutdown.

FAU_SAA.1 Potential violation analysis

Removed "or combination" from FAU_SAA.1.2 as the nature of the TOE allows users to configure a limitless number of rules, and it is computationally infeasible for the TOE to analyse the combination of configuration events and the resulting audit events.

FAU_SAR.1 Audit review (1)

Modified, in FAU_SAR.1.1 (1), the phrase "…from the audit records" to the phrase "… from the last one hundred audit records via the NSM™ Remote Console", as only the last one hundred audit records may be viewed by users in the Audit-review role via the NSM™ Remote Console.

FAU_SAR.1 Audit review (2)

Modified, in FAU_SAR.1.1 (2), the phrase "…from the audit records" to the phrase "… from the audit records via the NSM™ Reporting System Server" for further clarification due to the refinement performed on FAU_SAR.1 (1).

FAU_SAR.2 Restricted audit review

Only users with explicit read access may view the audit records via the NSM™ Reporting System Server or the NSM™ Remote Console. Thus, provided clarification by modifying FAU_SAR.2.1 from the words "…the audit records, except those…" to the words "…the audit records via the NSM™ Reporting System Server and via the NSM™ Remote Console, except those…"

8.2.9 Rationale for Audit Exclusions

Table 10 lists the events that are normally subject to audit at the Minimal level of audit but are not audited by the TOE for the indicated reasons:

Table 10. Rationale for Audit Exclusions

Functional Component	Auditable Event	Rationale for Exclusion
FPT_STM.1	Changes to the time.	This audit requirement has not been included because: • The only security functionality that relies on TOE system time is the time stamping of audit log entries. Since the TOE maintains the sequence of audit entries in the log, regardless of changes in system time, any relevant changes in system time would be apparent. • Authorised users or applications executing on the TOE must initiate system time changes. Users are assumed to be knowledgeable of the applications they are running, and hence are aware of changes in system time they initiate. If the operating system itself changes system time (e.g., daylight saving time changes), the user is notified. • System time is maintained by the operating system. In this case, the TOE operating system, Windows® 2000, does not support a capability to audit system time changes.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 TOE Security Functions Rationale

Table 11 provides a mapping of Security Functions to Security Functional Requirements for the TOE and is followed by a discussion of how each Security Functional Requirement is addressed by the corresponding Security Function.

Table 11. Mapping of Security Functions to Security Functional Requirements

	F.SSL	F.LOCK	F.AUDEVT	F.AUDINF	F.AUDSEL	F.ROLE	F.TIME	F.ALARM	F.AUDRVW	F.AUDRPT	F.AUDSTO	F.AUTH	F.HIST	F.PASS	F.USER	F.ADMIN	F.ACTION	F.FAILSAFE	F.STARTUP
FAU_ARP.1								X											
FAU_GEN.1			X	X															
FAU_GEN.2			X																
FAU_SAA.1								X											
FAU_ SAR.1 (1)									X										
FAU_ SAR.1 (2)									X										
FAU_SAR.2									X										
FAU_SAR.3 (1)									X										
FAU_SAR.3 (2)										X									
FAU_SEL.1					X														
FAU_STG.2											X								
FAU_STG.4								X			X								
FDP_ACC.1 (1)												X							
FDP_ACC.1 (2)															X				
FDP_ACF.1 (1)												X							
FDP_ACF.1 (2)		X													X	X			
FDP_ IFC.1	X																		
FDP_ IFF.1	X																		
FDP_ROL.1															X				
FIA_AFL.1								X				X							
FIA_ATD.1												X			X				
FIA_SOS.1														X					
FIA_SOS.2														X					
FIA_UAU.1												X							
FIA_UAU.7												X							
FIA_UID.1												X							
FIA_USB.1															X				
FMT_ MOF.1															X				
FMT_MSA.1 (1)																X			
FMT_MSA.1 (2)															X				
FMT_ MTD.1															X				
FMT_REV.1																X			
FMT_SAE.1																X			

	F.SSL	F.LOCK	F.AUDEVT	F.AUDINF	F.AUDSEL	F.ROLE	F.TIME	F.ALARM	F.AUDRVW	F.AUDRPT	F.AUDSTO	F.AUTH	F.HIST	F.PASS	F.USER	F.ADMIN	F.ACTION	F.FAILSAFE	F.STARTUP
FMT_SMF.1																X			
FMT_SMR.1						X													
FPR_UNO.4															X				
FPT_FLS.1																		X	
FPT_RVM.1																			X
FPT_ STM.1							X												
FRU_ FLT.1																		X	
FTA_ TAB.1												X							
FTA_ TAH.1													X						
FTA_TSE.1												X							
GRP_IFC.2																	X		
GRP_IFF.1																	X		

FAU_ARP.1 *Security alarms*

F.ALARM satisfies the requirement for detecting violations of security policies based on audit data and security event data.

FAU_GEN.1 *Audit data generation*

F.AUDEVT and F.AUDINF combine to satisfy the requirement for generation of audit data for the specified set of TOE events.

FAU_GEN.2 *User identity association*

F.AUDEVT satisfies the requirement for appropriate user identity to be associated with each auditable event.

FAU_SAA.1 *Potential violation analysis*

F.ALARM satisfies the requirement for detecting security violations of security policies based on audit data and security event data.

FAU_SAR.1 *Audit review (1)*

F.AUDRVW satisfies the requirement for audit data review by providing users in the Audit-review role with limited capability to review audit records through the NSM™ Remote Console.

FAU_SAR.1 *Audit review (2)*

F.AUDRVW satisfies the requirement for audit data review by providing the Audit-review role with the capability to review audit records in a browser through the use of the NSM™ Reporting System Server.

FAU_SAR.2 *Restricted audit review*

F.AUDRVW satisfies the requirement for restricted audit review by only allowing only the Audit-review role to review audit records through the NSM™ Reporting System Server or through the NSM™ Remote Console.

FAU_SAR.3 *Selectable audit review (1)*

F.AUDRVW satisfies the requirements for allowing all users to order audit data during review based upon SQL queries.

FAU_SAR.3 *Selectable audit review (2)*

F.AUDRPT satisfies the requirements for allowing the Administrator role to search and sort audit data during review based upon SQL queries.

FAU_SEL.1 *Selective audit*

F.AUDSEL satisfies the requirement for the inclusion or exclusion of audit data based upon the event type, item info, NSM™ domain, server, IP address of NSM™ Remote Console (if applicable), communication port for NSM™ Remote Console (if applicable), and the version of the particular NSM™ component.

FAU_STG.2 *Protected audit trail storage*

F.AUDSTO satisfies the requirement for protected storage of audit data by preventing unauthorised deletion or modification and by cycling the audit records in case of audit storage exhaustion.

FAU_STG.4 *Prevention of audit data loss*

F.AUDSTO and F.ALARM combine to satisfy the requirement for prevention of audit data loss by cycling the audit records and sending an alarm, respectively, in the case of audit storage exhaustion.

FDP_ACC.1 *Subset access control (1)*

F.AUTH satisfies the requirement for access control to the TSF through authentication of all users.

FDP_ACC.1 *Subset access control (2)*

F.USER satisfies the requirement for access control for interaction with the TSF.

FDP_ACF.1 *Security attribute based access control (1)*

F.AUTH satisfies the requirement for access control to the TSF based on the security attributes of user name, password, and NSM™ domain.

FDP_ACF.1 *Security attribute based access control (2)*

F.USER satisfies the requirement for access control for interaction with the TSF based on the attributes of user name, user role, graph permissions, and graph status. F.LOCK ensures that only one user at a time can edit a graph. F.ADMIN allows an Administrator to disable a user's ability to change their own password for their account when the Administrator creates the account for the user.

FDP_IFC.1 *Subset information flow control*

F.SSL satisfies the requirement to enforce the use of the SSL protocol for inter-NSM™ component transfer of security event data.

FDP_IFF.1 *Simple security attributes*

F.SSL satisfies the requirement to enforce the use of the SSL protocol for inter-NSM™ component transfer of security event data based on the CipherSuite variable.

FDP_ROL.1 *Basic rollback*

F.USER satisfies the requirement by providing the user with the ability to rollback the listed operations.

FIA_AFL.1 *Authentication failure handling*

F.AUTH and F.ALARM satisfy the requirement to detect consecutive failed authentication attempts by locking the user account and generating an alarm.

FIA_ATD.1 *User attribute definition*

F.AUTH and F.USER combine to satisfy the requirement for user attributes.

FIA_SOS.1 *Verification of secrets*

F.PASS satisfies the requirement for quality metrics of user passwords.

FIA_SOS.2 *TSF generation of secrets*

F.PASS satisfies the requirement for generating and enforcing the use of user passwords that meet the desired metrics.

FIA_UAU.1 *Timing of authentication*

F.AUTH satisfies the requirement for user authentication.

FIA_UAU.7 *Protected authentication feedback*

F.AUTH satisfies the requirement for protected feedback during user authentication.

FIA_UID.1 *Timing of identification*

F.AUTH satisfies the requirement for user identification.

FIA_USB.1 *User-subject binding*

F.USER satisfies the requirement for associating the security attributes of a user with all subjects acting on behalf of that user.

FMT_MOF.1 *Management of security functions behaviour*

F.USER satisfies the requirement for restricting management of TSF behaviour by allowing only users with the proper privileges to manage the audit mechanism.

FMT_MSA.1 *Management of security attributes (1)*

F.ADMIN satisfies the requirement for restricting management of the identified security attributes to the Administrator role.

FMT_MSA.1 *Management of security attributes (2)*

F.USER satisfies the requirement by allowing all users to modify their own password.

FMT_MTD.1 *Management of TSF data*

F.USER satisfies the requirement for restricted management of TSF data by only allowing users with the proper privileges to modify the TSF configuration.

FMT_REV.1 *Revocation*

F.ADMIN satisfies the requirement for disabling of user accounts by allowing the Administrator role to do so.

FMT_SAE.1 *Time-limited authorisation*

F.ADMIN satisfies the requirement for time-limited authorisation by allowing the Administrator role to specify an expiration time for a user account, after which the account is disabled.

FMT_SMF.1 *Specification of management functions*

F.ADMIN provides the management functions for security functions, for security attributes, and for TSF data.

FMT_SMR.1 *Security roles*

F.ROLE satisfies the requirement for various security roles.

FPR_UNO.4 *Authorised user observability*

F.USER satisfies the requirement for authorised user observability by allowing users with privileges to view a graph to observe editing of the graph.

FPT_FLS.1 *Failure with preservation of secure state*

F.FAILSAFE satisfies the requirement for maintaining a secure state in the case of the identified failures.

FPT_RVM.1 *Non-bypassability of the TSP*

F.STARTUP satisfies the requirement for ensuring that TSP enforcement functions are executing successfully before any other function in the TSC is allowed to proceed.

FPT_STM.1 *Reliable time stamps*

F.TIME satisfies the requirement for reliable time stamps for inclusion in audit records.

FRU_FLT.1 *Degraded fault tolerance*

F.FAILSAFE satisfies the requirement for ensuring operation of the identified functions in the case of the identified failures.

FTA_TAB.1 *Default TOE access banners*

F.AUTH satisfies the requirement to provide a warning regarding TOE usage to the user prior to authentication.

FTA_TAH.1 *TOE access history*

F.HIST satisfies the requirement to provide an authentication history to the user.

FTA_TSE.1 *TOE session establishment*

F.AUTH satisfies the requirement for TOE session establishment by providing the ability to deny a session based on the status of a user account.

GRP_IFC.2 *Complete information flow control for graphs*

F.ACTION satisfies the requirement to pass the flow of all event data through the graphs.

GRP_IFF.1 *Simple attributes for graph creation*

F.ACTION satisfies the requirement to pass the flow of all event data through the graphs and respond according to the value of the identified event data attributes.

8.3.2 TOE Assurance Measures Rationale

Table 12 provides a mapping of Assurance Measures to Security Assurance Requirements and is followed by a short discussion of how the Security Assurance Requirements are addressed by the corresponding Assurance Measures.

Table 12. Mapping of Assurance Measures to Security Assurance Requirements

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
M.ID	X												
M.SYSTEM	X												

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
M.GETTOE		X											
M.SETUP			X										
M.SPEC				X	X								
M.TRACE						X							
M.DOCS							X	X					
M.TEST									X	X	X		X
M.PROVIDE											X		
M.SECASS												X	X

ACM_CAP.2 *Authorisation controls*

M.ID and M.SYSTEM combine to satisfy the requirement for configuration management.

ADO_DEL.1 *Delivery procedures*

M.GETTOE satisfies the requirement for delivery procedures.

ADO_IGS.1 *Installation, generation, and start-up procedures*

M.SETUP satisfies the requirement for installation, generation, and start-up procedures.

ADV_FSP.1 *Informal functional specification*

M.SPEC satisfies the requirement for a functional specification.

ADV_HLD.1 *Descriptive high-level design*

M.SPEC satisfies the requirement for a high-level design specification.

ADV_RCR.1 *Informal correspondence demonstration*

M.TRACE satisfies the requirement for design specifications that are consistent throughout the documentation.

AGD_ADM.1 *Administrator guidance*

M.DOCS satisfies the requirement for administrator guidance documentation.

AGD_USR.1 *User guidance*

M.DOCS satisfies the requirement for user guidance documentation

ATE_COV.1 *Evidence of coverage*

M.TEST satisfies the requirement for evidence that all TOE security functions have been tested.

ATE_FUN.1 *Functional testing*

M.TEST satisfies the requirement for evidence that TOE security functions have been tested.

ATE_IND.2 *Independent testing – sample*

M.TEST satisfies the requirement for evidence that TOE security functions have been tested. M.PROVIDE satisfies the requirement for providing a suitable TOE for testing.

AVA_SOF.1 *Strength of TOE security function evaluation*

M.SECASS satisfies the requirement for evidence that all TOE security functions have been examined to ensure their strength against threats.

AVA_VLA.1 *Developer vulnerability analysis*

M.TEST and M.SECASS combine to satisfy the requirement for evidence that the TOE has been examined and tested in an effort to discover vulnerabilities.

9 ACRONYMS AND ABBREVIATIONS

Acronym	Definition
ACCESS_SFP	Security Functional Policy for ACCESS control to NSM™ controlled objects
CC	Common Criteria for Information Technology Security Evaluation
CS	Central Server
EAL	Evaluation Assurance Level
EC	Event Consolidator
GRAPH_SFP	Security Functional Policy for the flow of security event data to NSM™ GRAPHs
GUI	Graphical User Interface
ID	IDentification
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
JVM	Java® Virtual Machine
LMP	Link Management Protocol
LOGIN_SFP	Security Functional Policy for authenticating (LOGging IN) to NSM™
MS	Microsoft
NSM™	Network Security Manager™
PC	Personal Computer
PP	Protection Profile
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength Of Function
SP	Service Pack
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSL_SFP	Security Functional Policy for the protection of event data, with SSL, that is transmitted between physically-separate components of the TOE
ST	Security Target
Syslog	System log Protocol
TCP	Transmission Control Protocol
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
URL	Uniform Resource Locator
WWW	World Wide Web