Hewlett-Packard

Network Node Manager Advanced Edition Software v7.51 with patch PHSS_35278.

Security Target V 1.13

Prepared for

Hewlett-Packard

January 11, 2007

By

CYGNACOM
SOLUTIONS

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table or Figure **Page**

Security Target Introduction

1.1 Security Target Identification

TOE Identification: HP Network Node Manager Advanced Edition Software v7.51 with patch PHSS_35278.

ST Title: HP Network Node Manager Advanced Edition Software v7.51 with patch PHSS_35278 Security Target

ST Version: Version 1.13

ST Authors: Debra Baker, Jenifer Wierum

ST Date: January 11, 2007

Assurance Level: EAL2

Registration: <To be filled in upon registration>

Keywords: Network Management, System Data Collection, and Security Target

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for HP Network Node Manager Advanced Edition Software v7.51 with patch PHSS_35278. Network Node Manager (NNM) is a network management system. NNM collects system data from across the targeted network, stores it in a database, and provides management capabilities. In addition, NNM includes an auto-baseline capability to automatically set alarm thresholds for collected data based on deviations from historical data. If these thresholds are exceeded, then NNM will generate an alarm. NNM is designed to help system administrators detect, solve, and prevent problems occurring in their targeted networks.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Sections 9 and 10, provide acronym definitions and references.

1.5 Acronyms

Table 1-1 Acronyms

Acronym	Definition
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
DMI	Desktop Management Interface
DMTF	Desktop Management Task Force
EAL	Evaluation Assurance Level
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
ID	Identifier
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IT	Information Technology
MAU	Media Access Unit
MIB	Management Information Base
NNM	Network Node Manager
OVO	HP OpenView Operations
OVW	OpenView Web
SF	Security Function
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol

1.6 References

Table 1-2 References

References
Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-002, Version 2.2, January 2004.
HP Network Node Manager Quick Start Installation Guide Solaris operating systems
HP Network Node Manager Managing Your Network with HP Network Node Manager Windows, HP-UX, and Solaris operating systems
HP Network Node Manager Welcome to NNM Windows, HP-UX, and Solaris operating systems

1.7 Terminology

Table 1-3 Customer Specific Terminology

Term	Definition
Alarm data	Alarm data is based on the System data that is collected from the managed nodes. NNM has the ability to have thresholds set, if these thresholds are exceeded, then NNM will generate an alarm.
Event	An event is also system data. An event is comprised of a single SNMP trap, SNMP information, or ICMP information. For example, a single SNMP trap is an event.
Event Database	The event database is comprised of the System data that is collected from the managed nodes.
Managed node	A managed node provides the TOE system data (traps and information) about the targeted network. This is also referred to as an object in the SNMP Network Management Model.
Object	Any managed node such as a host, router, switch, hub, and bridge.
SNMP agent	SNMP agent resides on a managed node and is an application that acts on behalf of an object to perform network management operations requested by the manager.
System data	The SNMP traps, SNMP information, and ICMP information collected from managed nodes.
Targeted network	The domain of network and host traffic to be analyzed by the TOE.

Table 1-4 CC Specific Terminology

Term	Definition
Authorized user	A user who may, in accordance with the TSP, perform an operation.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

2 TOE Description

2.1 Product Type

V7.51 of HP Network Node Manager Software with patch PHSS_35278 (NNM) is available in a Starter Edition (SE) or Advanced Edition (AE). The NNM SE is comprised of Classic Technology while NNM AE includes Classic Technology and Extended Topology. This software only TOE will focus on NNM AE with patch PHSS_35278.

Network Node Manager (NNM) Classic Technology is the foundation from which most of the HP OpenView products operate. NNM functions as a solution on its own, and can collect data for and forward data to other HP OpenView products. NNM provides network administrators with the ability to proactively monitor their targeted networks. NNM collects critical data from across the targeted network, stores it in a database, and provides management capabilities. In addition, NNM includes the capability to set alarm thresholds for collected data based on deviations from historical data. If these thresholds are exceeded, then NNM will generate an alarm.

NNM AE Extended Topology augments NNM Classic by discovering and displaying additional device connectivity information from the devices whose existence was discovered by NNM Classic. This information is stored in a relational database and can be used to diagnose network problems.

2.2 NNM Components

The evaluated product is comprised of the Network Node Manager (NNM) Server (2.2.1), NNM databases [embedded relational database (2.2.2.2) and operational databases (2.2.2.1)], NNM User Interfaces [Dynamic Views (2.2.3.2) and CLI (2.2.3.1)] and Syslog Agent (2.2.4). The product also includes two older GUIs that are NOT included in the TOE Boundary: Java GUI (2.2.3.4) and Motif GUI (2.2.3.3).

2.2.1 NNM Server

The NNM server performs the central processing functions of NNM. The entire software package, including the complete configuration, is stored on the NNM server. The NNM server provides the following security functions:

- **Auditing**

  NNM server is responsible for creating and recording TOE audit records for security related audit events. The audit log is stored on the NNM server host and is viewable via a command line interface as root.

- **Data Collection, Analysis, and Alarm Notification**

  Data Collection

  NNM Server collects data from targeted network devices. NNM polls for the status of targeted network devices, network topology changes, and configuration changes. Several protocols are used to maintain communication channels with each managed device on the targeted network. These include:

  - SNMPv1; SNMPv2
  - TCP/IP

- HTTP/HTTPS
- UDP
- ICMP
- ARP/RARP

NNM also uses other, lower-level families of protocols (sometimes referred to as services), such as the ARPA family, the Berkeley family, and the NFS family. These protocols are used for functions such as file transfer, e-mail, or remote login. All of these communication protocols are outside the scope of the TOE Boundary.

The Extended Topology model of recurring discovery differs from the continuous discovery present in NNM Classic. Extended Topology captures data about your network as it exists during the most recent discovery cycle, or the most recent previous discovery cycles. It does not update the data between discovery cycles. This means that only the layer 2 connections that exist during Extended Topology discoveries get recorded. In addition, device information (such as VLAN, port aggregation, and ATM data) is gathered only from devices that are accessible during the Extended Topology discoveries. An "accessible" device responds to SNMP requests from NNM. For this to happen, NNM must be configured to use the correct SNMP GET-Community name for the device.

Data Analysis

NNM actively sends notification when an important event occurs. The event is reflected by a change in the color of the device's symbol on the map, and is reported through NNM's Alarm Browser.

The event reduction features monitor incoming alarms to identify patterns of common network problems and post one meaningful alarm with all related alarms nested beneath for an identified problem.

Application Note: In the context of the TOE, the "alarm browser" is part of the Dynamic Views interface [See Section 2.2.3.2].

Alarm Notification

Thresholds can be configured so that NNM can monitor critical network devices. Once a threshold has been met or exceeded, NNM can be configured to send a notification to the alarm browser to advise that operating patterns are outside normal expectations.

- **Security Management**

The server provides the NNM Administrators, operating as "root" user in the OS, with command line interfaces (Section 2.2.3.1) to perform security management functions. The CLIs are used for password setting, database setting (e.g. Oracle, Solid, SQL Server), configuring the network behavior (e.g. polling cycles) and customization. NNM Administrators have an additional extended topology configuration capability available on the Dynamic Views GUI only when accesses on the NNM Server. NNM operators and NNM administrators have the ability to change their own password through Dynamic Views whether accessing Dynamics View remotely or locally to the NNM server.

- **User Data Protection (Access Control)**

  The NNM server identifies the user information and performs access control decision and enforcement. The GUI is presented only after successful identification and authorization of the user. Additional factors in the access control decision are role assignment of authorized user (NNM Administrator or NNM Operator) and whether the request is from the physical NNM server (local) vs remotely.

- **Identification and Authentication**

  The NNM server collects the identification and authentication information (username, password) via an HTML form provided by the NNM server from potential users of Dynamic Views GUI. The collection is performed via secure HTTPS/SSL communication between the web browser and the NNM server. The NNM server identifies the user information and performs access control decision and enforcement. The GUI is presented only after successful identification and authorization of the user. Since this is the primary access to NNM management stations, security auditing for unauthorized attempts will be logged. User accounts will be disabled after a certain number of consecutive failed attempts.

- **Partial Protection of the TSF**

  Working in concert with its platform, the TOE provides protection of its security functions through non-bypassability and domain separation. All user operations are conducted in the context of an associated session. The TOE manages these sessions to prevent one session from compromising another session. The TOE provides only well-defined interfaces to these sessions, and the sessions allocated only after successful authentication, or when a session is requested from the physically protected local console which is under procedural control. The TOE relies on its platform to operate correctly and to prevent unauthorized access to TOE data, stored executables, and management activities.

- **Partial Protected Data Transmission**

  The TSF permits the local users and remote users to initiate communication via the trusted path for initial user authentication and all communication between Dynamic Views GUI and the NNM Server. The TSF relies on the IT environment to provide protection of the trusted path from modification or disclosure using SSL.

2.2.2 NNM's Databases

NNM provides several operational databases, each designed to store specific kinds of data and used for a variety of purposes. In addition, NNM includes a Relational database that is used for data warehousing and Extended Topology data storage.

2.2.2.1 Operational Databases

NNM's operational databases—object, map, topology, trend, and event—can be thought of as a single logical database. These databases store the operational data used by NNM in binary Native Database Management format (NDBM), which provides for fast access of relatively static information.

- **The Object Database**

The object database contains semantic information about symbols on the map. The information is generic; that is, it is not customized to any specific application. The object database contains field definitions such as sysObjectID, vendor, and SNMP Agent. You can see the field values in the object database for a particular object through the Properties dialog box for that object.

- **Map Database**

The map database contains presentation information specific to each map. Examples of presentation information that is stored in the map database include the exact symbol placement on the map, the symbol associated with each object, and symbol labels. NNM updates the map database based on requests from the user, or from various NNM services.

- **Topology Database**

The topology database manages information critical to the management of IP nodes. It includes state information, such as time stamps indicating when the object last changed and when it should check the device configuration next. This information helps NNM detect changes and communicate them to various NNM services. The topology database is stored in a proprietary HP OpenView format.

- **Event Database**

The event database is the repository for SNMP traps and other events that are received by NNM. It also stores events that are output from the Event Correlation Service (ECS), which is used to reduce the number of events presented by correlating them. The objective of ECS is to report the most relevant event. In addition, the event database stores information for the event browser tools about the state of the events displayed in the web browser applications. The information in the event database is displayed in the Alarm Browser.

- **Trend Database**

The trend database (sometimes called the snmpCollect database) stores MIB data and threshold information that is gathered through the snmpCollect service (process). Information from the trend database is used in the Reporting and the Data Collection features, and can be viewed with the Graphing feature of NNM on a management station. The graphing feature can be accessed as a menu item under Dynamic Views.

- **Data Warehouse**

The NNM data warehouse stores data exported from the NNM databases into a relational database. The information in the data warehouse can be used to define customized reports. The NNM web Reporting interface can also be used to configure and view reports. NNM automatically starts exporting the appropriate data to the data warehouse when a report is created.

2.2.2.2 Extended Topology Database

The Extended Topology Database stores topology information related to NNM AE. The information stored in this database is used by Dynamic Views to present status information for the Node Status Summary tab under Dynamic Views. This relational database is the same one used for the Data Warehouse.

2.2.3 User Interfaces

2.2.3.1 Command-line interface

NNM Administrators, operating as “root” user in the OS, use command line interfaces to perform security management functions. CLIs are used for password setting, database setting (e.g. Oracle, Solid, SQL Server), configuring the network behavior (e.g. polling cycles) and customization.

The administrative Command Line Interfaces (CLIs) on the NNM Server can be grouped into following categories:

- **Installation and initial Configuration of the NNM/UNIX Management Server**
  CLIs are used for the initial installation of the NNM/UNIX Management Server application. This includes database setup, licensing and fundamental customer environment specific configuration and so on.

- **Customization and ongoing Maintenance**
  NNM maintenance includes SNMP community string management, managing/unmanaging devices, defining events/actions of events, map management via registration file changes, map customization, changes to databases (removal, creation, selection, password and account), viewing and maintenance of audit trail, threshold alarm setting, and polling,

- **Start/Stop, Troubleshooting**
  Allows an administrator to start/stop the NNM server related processes, tracing processes, run troubleshooting tools, etc.

2.2.3.2 Dynamic Views

Dynamic Views describes the family of browser-based views whose content is created as a result of choices made when the view is launched, and which continue to provide the most current status information available (continually updates the view). This user interface is designed to provide all users with a summary of the targeted network’s status, access to detailed alarms (alarm browser), and maps of the network infrastructure and services. The maps show the health of network devices and the location of trouble spots.

NNM presents many different browser based views of discovered nodes. NNM’s Neighbor, Node, Station, Internet, Network, Path, VLAN, Problem Diagnosis, HSRP, OSPF, OAD, IPv6, and Port-Address Mapping views show topology views and other information that supplement NNM’s map views. An example of the Neighbor view which shows a graphical representation of the selected device and the connector devices related to it, within a specified number of hops of the selected device is below.

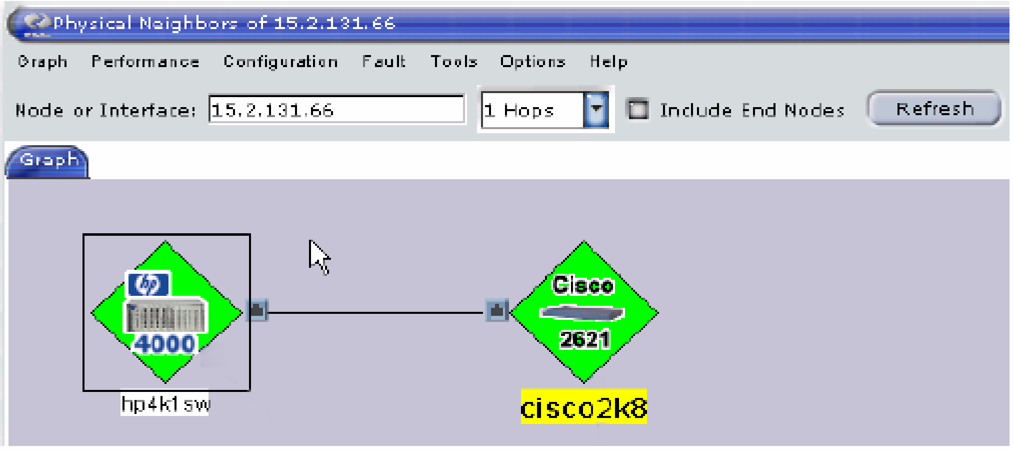

Figure 2-1 Neighbor view Example

The Dynamic Views GUI has one security functional interface (password change request) that is available for use by any authenticated user, no matter what grouping/role the user is included in or whether local or remote to the NNM Server.

The Dynamic Views GUI has one security functional interface (Extended Topology configuration) that is available for use by an authenticated user that has the role of NNM administrator and the user is physically on the NNM Server (local).

Dynamic Views provides the visual results of the alarms created by the NNM Server.

2.2.3.3 MOTIF GUI (OVW)

Network Node Manager's Open View for Windows (OVW) graphical user interface (MOTIF based) was the predecessor to the Dynamic Views GUI described above. This GUI was designed to provide all users with a summary of the targeted network's status, access to detailed alarms, and maps of the network infrastructure and services. This interface is still included in the installation to provide support for long time customers but is currently being migrated away from.

For the purpose of the CC evaluation, the OVW Motif GUI was NOT included in the TOE configuration because it is a remnant of the older operational UI technology that is being migrated away from. Product end users who want to maintain operations in compliance with the CC evaluation must not use this interface.

2.2.3.4 Java GUI (JOVW)

HP OpenView's Java-based web interface provides a mechanism for an authorized user to log onto and access NNM on the management server to display maps and alarm information from a remote web browser. This interface was an extension of the OVW Motif GUI that is being migrated away from.

Therefore, for the purpose of the CC evaluation, the JOVW was NOT included in the TOE configuration because it is a remnant of the older operational UI technology that is being migrated away from. Product end users who want to maintain operations in compliance with the CC evaluation must not use this interface.

2.2.4 Syslog Agent

The Syslog Integration functionality enables the management of network equipment from syslog messages and provides the ability to map syslog messages into SNMP traps for presentation or analysis. There are two deployment options for Syslog Integration:

2.2.4.1 NNM Standalone Configuration

The NNM standalone configuration consists of deploying an HP NNM Syslog agent on the NNM management station (host where the NNM Server component is installed). In short, the embedded syslog agent uses preconfigured templates to parse incoming syslog messages matching a certain pattern. The matched syslog messages are mapped to SNMP traps and displayed in the NNM alarm browser.

2.2.4.2 Open View Operations with NNM Configuration

There is an additional configuration for having the embedded syslog agent pass information on to an OVO management station. This configuration is not part of the TOE.

2.3 TSF Physical Boundary and Scope of the Evaluation

This is a software only TOE.

The evaluated configuration includes the following:

HP Network Node Manager AE software will be evaluated on the following operating system platform(s):

- NNM server (the embedded database and NDBM dbs, CLIs, Dynamic Views, and Syslog Agent will be installed on this machine) will be installed on the UNIX operating system HP-UX 11.11.
- NNM Dynamic Views will be access from a separate Windows 2000 workstation and on the Server with a compatible browser.

All machines (remote host for Dynamic Views, NNM Server, and Network devices for discovery) will be installed on a closed network with no connectivity outside the control of the entity for which NNM is being used to manage.

The TOE includes the following software only components:

- NNM Server (including the embedded database and NDBM dbs)
- NNM Dynamic Views (Java Web GUI)
- NNM Command Line Interfaces (System Management)
- NNM Syslog Agent (NNM Standalone server configuration)

The NNM Product includes the following software components that are outside the scope of the evaluation:

- The MOTIF OVW GUI (installed but not to be used)
- The JOVW GUI (installed but not to be used)
- Apache Tomcat (Tomcat is required to be configured to use SSL)/ Apache HTTP Server (Apache)
- Java Runtime Environment. (required for Dynamic Views TOE component in evaluated configuration)
    - SSL implementation used by Tomcat (required for evaluated configuration).

The TOE does not include the following:

- Underlying operating system (OS) software and hardware. (required for evaluated configuration)
- Internet Browser required for evaluated configuration on both the server (Mozilla) and separate PC (I.E. 6 SP 1 or higher) for Dynamic Views
- Adobe Reader (required to read .pdf manuals)
- Transport standards such as SNMP, HTTP, HTTPS, and ICMP implementations. (required for evaluated configuration)
- Any third-party optional database (Oracle, SQL, etc) that the NNM could be configured to use. (Option was not included in the evaluated configuration)

There will be network nodes for SNMP collection that could be running HP-UX 11.11, Solaris 9 OS, MS Windows 2003 SP1, and/or Red Hat Enterprise Linux 3.0 – Advanced Edition.

- All network node components are out of scope

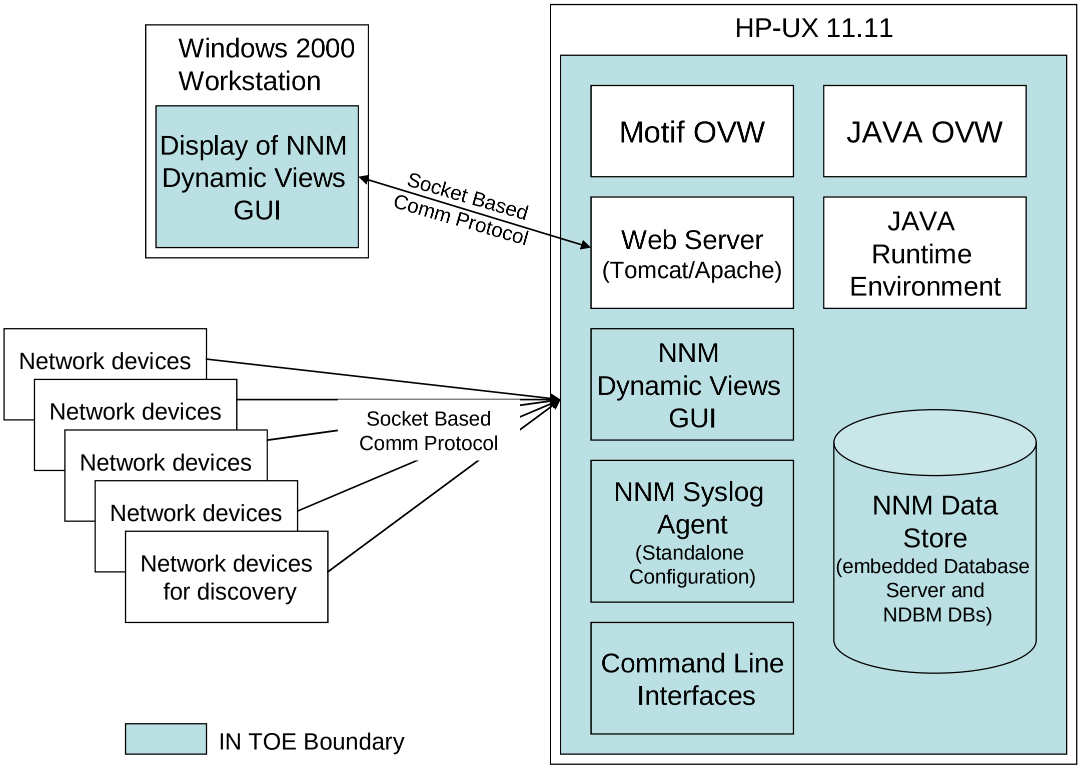
Windows 2000 Workstation
Display of NNM Dynamic Views GUI
Socket Based Comm Protocol
HP-UX 11.11
Motif OVW
JAVA OVW
Web Server (Tomcat/Apache)
JAVA Runtime Environment
Network devices
Network devices
Network devices
Network devices
Network devices for discovery
Socket Based Comm Protocol
NNM Dynamic Views GUI
NNM Syslog Agent (Standalone Configuration)
NNM Data Store (embedded Database Server and NDBM DBs)
Command Line Interfaces
IN TOE Boundary

Figure 2-2 HP NNM - Physical TOE Boundary

2.4 Logical Boundary

The TOE provides the following security features as described above:

- **Security Audit**
- **Security Management**
- **Data Collection, Analysis, and Alarm Notification**
- **Identification and Authentication**
- **User Data Protection (Access Control)**
- **Partial Protection of the TSF**
- **Partial Protected Data Transmission**

2.5 TOE Security Environment

It is assumed that the customer provides for the physical protection of the TOE.

NNM requires the underlying operating system and platform to provide user identification and authentication of root users accessing the CLI, file protection, audit protection, and reliable time stamps.

NNM requires that the operating system also provides Non-bypassability of the TSP and TSF domain separation.

The TOE relies on the IT Environment to secure the network path between NNM server and web browser (requires Tomcat/Apache to be configured to use SSL). All cryptographic functions are part of the IT Environment and not part of the TOE. The evaluated configuration tested the services provided by SSL. Testing did not include any cryptography verification.

It is assumed that there will be no untrusted users or software on the HP Network Node Manager NNM server, since it is recommended to be a dedicated system.

To administer NNM, the user must be trusted, trained and have OS “root” user privileges and access to perform Security Management duties.

It is assumed that users will protect their authentication data.

The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The following third-party components will be in the IT Environment:

- Operating system for NNM Server and Remote PC. (*Not provided with NNM product*)
  - Transport standards such as SNMP, HTTP, HTTPS, and ICMP implementations. (required for evaluated configuration)
- Internet Browser required for evaluated configuration on both the server (Mozilla) and separate PC (I.E. 6 SP 1 or higher) for Dynamic Views. (*Not provided with NNM product*)
- Adobe Reader required to read .pdf manuals. (*Not provided with NNM product*)
- Java Runtime environment. (*Supplied with and components installed with NNM product*)
- Tomcat / Apache HTTP Server. (*Supplied with and components installed with NNM product*)
  - Tomcat is configured to use SSL. (required for evaluated configuration)

The TOE security environment can be categorized as follows:

- **Identification and Authentication** – NNM relies on the underlying OS to provide user identification and authentication of all users of the TOE CLIs and the delineation of roles: root (also called super user) and other OS users. System Management functions are accomplished via command line interfaces that must be protected by the OS and can only be executed as the OS “root” user. The user must go through a second I & A (UNIX su command) in order to gain “root” access.
- **Partial Protection of TSF** - NNM relies on the underlying OS and hardware to provide security capabilities for the TOE’s protection (executables, audit logs, databases, and data). For the TOE’s own protection the IT Environment includes requirements that relate to the integrity of the TSF. These include Non-bypassability of the TSP, TSF domain separation, access control, identification and authentication, audit storage, and a reliable time-stamp.
- **Partial Trusted Path -** NNM also relies on Tomcat/Apache configured to use SSL to provide communication protection for users trying to access Dynamic Views on the NNM server via the web browser.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

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

Table 3-1 Assumptions for the IT Environment

1	A.AdmTra	Administrators are non-hostile, appropriately trained, have OS “root” user privileges, and follow all administrative guidance, including guidance on setting passwords. However, administrators are capable of error.
2	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the HP Network Node Manager Server host.
3	A.Physical	Physical protection is assumed to be provided by the environment. The TOE hardware and software is assumed to be protected from unauthorized physical access.
5	A.Users	It is assumed that users will protect their authentication data.

3.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE must counter the following threats to security:

Table 3-2 Threats

1	T.FailAnalyze	The TOE may fail to identify and alert vulnerabilities or inappropriate activity based on the association of system data received from all managed nodes vulnerable to attack. The assets at risk are the managed nodes which can include the TOE.
2	T.FailReact	The TOE may fail to alert authorized personnel of inappropriate activity or operations outside of normal thresholds. The assets at risk are the managed nodes which can include the TOE.
3	T.Mismgmt	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorised access to resources protected by the TOE.
4	T.Privil	An unauthorised user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
5	T.Tamper	An attacker may attempt to modify, view, or delete TSF programs and data.
6	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 Security Objectives for TOE

1	O.Audit	The TOE will provide the capability to detect, create, and view records of security relevant events.
2	O.AnalyzeData	The TOE will apply sampling and analytical processes and information to derive conclusions (past, present, or future) on the collected data from managed nodes.
3	O.CollectData	The TOE will collect and record system and network data from the managed nodes.
4	O.React	The TOE will send an alarm if a configured threshold has been exceeded.
5	O.Roles	The TOE will maintain the roles of: NNM Administrator and NNM operator
6	O.SecMgt	The TOE will provide the functionality to enable authorized administrator(s) to effectively manage the TOE and its security functions.
7	O.Access	The TOE will provide its authorized administrators with the means of controlling and limiting access to TSF data on the basis of user identity, password, and user roles, in accordance with the specification of the management of TSF data.
8	O.Authorize	The TOE will be able to identify and authenticate (in accordance to the TOE's password and authentication failure handling policy) potential web users prior to allowing access to authorized TOE functions and data
9	O.NonBypass	The TSF will ensure that its protection mechanisms cannot be bypassed.
10	O.Protect	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure.
11	O.Partial_TrustedComm	The TOE in concert with its IT Environment will provide a trusted channel using SSL between the TOE and its environment.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT Environment are as follows:

Table 4-2 Security Objectives for IT Environment

12	OE.AuditProtect	The IT Environment will provide the capability to protect audit information from unauthorized deletion, modification, and viewing.
13	OE.Time	The IT Environment will provide reliable time stamps.
14	OE.Roles	The IT Environment will maintain the roles of: "root" and other users.
15	OE.SecMgt	The IT Environment will provide the functionality to enable authorized administrator(s) to effectively manage the TOE and its security functions.
16	OE.Access	The IT Environment will provide its authorized administrators with the means of controlling and limiting access to TSF data on the basis of user identity, password, and user roles, in accordance with the specification of the management of TSF data.

17	OE.Authorize	The IT Environment will be able to identify and authenticate root users on the OS prior to allowing access to authorized TOE functions and data.
18	OE.NonBypass	The IT Environment will ensure that its protection mechanisms cannot be bypassed.
19	OE.Protect	The IT Environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure.
20	OE.Partial_TrustedComm	The IT Environment in concert with the TOE will provide a trusted channel using SSL between the TOE and its environment.

4.2.2 Security Objectives for Non-IT Security Environment

The Non-IT security objectives are as follows:

Table 4-3 Security Objectives for Non-IT Environment

21	ON.Install	Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security.
22	ON.NoUntrusted	The administrator will ensure that there are no untrusted users and no untrusted software on the NNM server.
23	ON.Operations	The TOE will be managed and operated in a secure manner as outlined in the supplied guidance.
24	ON.ProtectAuth	Users will ensure that their authentication data is held securely and not disclosed to unauthorised persons.
25	ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
26	ON.Physical	Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT Environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, explicitly stated requirements derived from Part 2 of the CC, and assurance components from Part 3 of the CC.

5.1 Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 2 and paragraph 2.1.4 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]***.*
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***<u>italicized bold and underlined text</u>***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. “*” refers to all iterations of a component.
- *Explicitly Stated Requirements* will be noted with a “_EXP” added to the component name.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *NIAP and CCIMB Interpretations* have been reviewed. Relevant Interpretations are included and are noted in Interpretation Notes. Interpretation Notes are denoted by *italicized text.* The original CC text modified by the interpretation is not denoted nor explained.
- *Comments* are provided as an aid to the ST author and evaluation team. These items will be deleted in the final version of the ST.

5.2 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC, CC interpretations, and explicit components, summarized in the Table 5-1 below.

Table 5-1 Functional Components

Item	Component	Component Name
1.	FAU_GEN.1	Audit data generation

Item	Component	Component Name
2.	FAU_SAR.1	Audit Review
3.	CA_SDC_EXP.1	System data collection
4.	CA_ANL_EXP.1-1	Analyzer analysis
5.	CA_ANL_EXP.1-2	Analyzer analysis
6.	CA_RCT_EXP.1	Analyzer react
7.	FDP_ACC.1-1	Subset access control
8.	FDP_ACF.1-1	Security attribute based access control
9.	FIA_AFL.1	Authentication failure handling
10.	FIA_SOS.1	Verification of secrets
11.	FIA_UID.2-1	User Identification before any action
12.	FIA_UAU.2-1	User authentication before any action
13.	FMT_MTD.1-1	Management of TSF data
14.	FMT_SMF.1	Specification of Management Functions
15.	FMT_SMR.1	Security Roles
16.	FPT_SEP_EXP_TSF.1	Partial TSF domain separation by the TOE
17.	FPT_RVM_EXP_TSF.1	Partial Non-bypassability of the TSP by the TOE.
18.	FTP_TRP_EXP_TSF.1	Partial Trusted Path by the TOE

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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

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

b) All auditable events for the **[*not specified*]** level of audit; and

c) **[*the following auditable events:***

- ***Changes to databases***
  - ***Removal, creation***
  - ***Database type used (Oracle, Solid, SQL Server)***
  - ***Password and account changes***
- ***Changes to menus for dynamic views***
- ***Run of backup and restore command***
- ***URL access***
- ***Login to Dynamic Views GUI.*]**

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: **[*other audit relevant information*]**

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*root*]** with the capability to read **[*all audit information*]** from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

Application Note: The 'root' user is the NNM administrator.

5.2.2 Class CA: Collection and Analysis Requirements

CA_SDC_EXP.1 System data collection

Hierarchical to: No other components

CA_SDC_EXP.1.1 The System shall be able to collect the following information from the managed node(s): see column 1 of Table 5-2.

CA_SDC_EXP.1.2 At a minimum, the System shall collect and record the following information:

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

b) The additional information specified in the Details column of Table 5-2 System Data.

Table 5-2 System Data

Managed node	Information	Details
Object (host, router, switch, hub, bridge)	SNMP traps	Date and time of the trap, type of trap, subject identity, and the outcome (success or failure) of the trap, and detailed information in the form of a description. *Application Note: SNMP traps and events are basically synonymous. Events are SNMP traps defined by NNM using NNM Event IDs that are unique and allow NNM to add other NNM-specific information such as the object IDs.* *Almost all daemon processes, ipmap (ovw sub process), alarm browsers, and Reporting use events*. *Application Note: The matched syslog messages are mapped to SNMP traps. Therefore, there is no separate listing for syslog messages.*
	SNMP information	TCP/IP and UDP Polling and discovering, data collection and select operations on the device (querying or setting MIB values)
	ICMP information	Used by polling and discovery to determine access to a network device and the network path used to get to the device.
	HTTP Information	Used by polling and discovery to determine if a HTTP server is being used on a computer.

Dependencies: No dependencies.

CA_ANL_EXP.1-1 Analyzer analysis

Hierarchical to: No other components

CA_ANL_EXP.1.1-1 The TOE shall perform sampling on all system data received.

CA_ANL_EXP.1.2-1 The TOE shall record within each analytical result at least the following information:

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

Dependencies: CA_SDC_EXP.1 System data collection.

CA_ANL_EXP.1-2 Analyzer analysis

Hierarchical to: No other components

CA_ANL_EXP.1.1-2 The TOE shall perform signature analysis function on all system data received.

Dependencies: CA_SDC_EXP.1 System data collection.

CA_RCT_EXP.1 Analyzer react

Hierarchical to: No other components.

CA_RCT.1.1 The TOE shall send an alarm to the alarm browser upon detection of a potential security violation.

Application Note: In the context of the TOE, the "alarm browser" is part of the Dynamic Views interface. This interface is the equivalent of the "event browser" which is part of the Motif and Java OVW interface which are not included in this evaluation.

Dependencies: CA_SDC_EXP.1 System data collection

CA_ANL_EXP.1 Analyzer analysis

5.2.3 Class FDP: User Data Protection

FDP_ACC.1-1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1-1 The TSF shall enforce the **[*TOE Access Control SFP*]** on **[**

Subjects: Dynamic Views users

Objects: Dynamic Views GUI

***Operations: execute*].**

Dependencies: FDP_ACF.1-1 Security attribute based access control

Application Note: This is for access control of potential Dynamic View GUI users.

FDP_ACF.1-1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1-1 The TSF shall enforce the **[*TOE Access Control SFP*]** to objects based on the following: **[**

Subjects (Dynamic Views users):

username, password & roles

Objects (Dynamic Views GUI):

Remote Operator/Administrator Dynamic Views GUI web pages

Local Administrator Dynamic Views GUI web pages

Local Operator Dynamic Views GUI web pages

].

FDP_ACF.1.2-1 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

1. Subjects must be included in the TOE configuration file.

2. Subject's supplied username and password must match the username and password stored in the TOE configuration file.

3. Subject's account must not be disabled via the failed access attempts lockout feature.

]

FDP_ACF.1.3-1 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[**

1. When requesting user's session is initiated on the NNM Server (local) and user's role equals NNM administrator; access will be granted to the Dynamic Views for the NNM Administrator.

2. When requesting user's session is initiated on the NNM Server (local) and user's role equals NNM operator; will be granted access to the Dynamic Views for NNM operators.

3. When requesting user's session is initiated off the NNM Server (remote) and user's role equals either role (NNM administrator or NNM operator); will be granted access to the Dynamic Views for NNM operators.

].

FDP_ACF.1.4-1 The TSF shall explicitly deny access of subjects to objects based on the following rules: **[**

1. ***Subject's account is disabled via the failed access attempts lockout feature.***

2. Subjects not included in the TOE configuration file.

3. Subject's supplied username and/or password that do not match the username and password stored in the TOE configuration file.

].

Dependencies: FDP_ACC.1-1 Subset access control

FMT_MSA.3 Static attribute initialization

Application Note: This is for access control of potential Dynamic View GUI users.

5.2.4 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when **[*5*]** unsuccessful authentication attempts occur related to **[*successive user login attempts via the Dynamic Views GUI*]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[*disable the user account*].**

Dependencies: FIA_UAU.1 Timing of authentication.

Application Note: This is for authentication of potential Dynamic View GUI users.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[**

- ***Minimum password length: 8 characters***
- ***Requires one numeric character***
- ***Requires one special character***
- ***Requires one lower case character***
- ***Requires one upper case character***

].

Dependencies: No dependencies.

Application Note: This is for authentication of potential Dynamic View GUI users.

FIA_UAU.2-1 User authentication before any action

Hierarchical to: FIA_UAU.1.

FIA_UAU.2.1-1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

Application Note: This is for authentication of potential Dynamic View GUI users.

FIA_UID.2-1 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1-1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Application Note: This is for identification of potential Dynamic View GUI users.

5.2.5 Class FMT: Security Management

FMT_MTD.1-1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1-1 The TSF shall restrict the ability to **[*see operations specified in Table 5-3*]** the TSF Data **[*as specified in Table 5-3 to the role as specified in Table 5-3*].**

Dependencies: FMT_SMR.1-1 Security roles

FMT_SMF.1 Specification of Management Functions

Table 5-3 Management of TSF Data through Dynamic Views

Roles	**Allowed Operations on TSF Data (Management Functions)**
NNM Admin (Via the Dynamic Views GUI initiated from the NNM server)	• Password Change (own account only) • Extended Topology configuration.
NNM Admin (via the Dynamic Views GUI initiated remote from the NNM Server)	• Password Change (own account only)
NNM Operator	• Password Change (own account only)

Application Note: The security related configuration function, Extended Topology Configuration is only available to an administrator who logs into Dynamic View while physically being on the server. The configuration option is not available to anyone, including an admin, when logging into Dynamic Views remotely.

Application Note: This is for the Management of TSF available through Dynamic Views. Management of TSF data available for the command line interfaces, which must be protected by the IT Environment, is defined in the IT Environment SFR section.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

CLI

- ***Configuration (on/off), View, Reset (Delete) audit log***
- ***Backup/Restore/Reset(delete) System data***
- ***Licensing Tool (adding, removing)***
- ***Change password to the relational db (extended)***
- ***Syslog Agent Template modification***
- ***Configuration (on/off) Syslog Agent***
- ***Change/modify/delete Data Analysis rules and definitions***
- ***Modify/delete configuration file for username, password, and role attributes for Dynamic Views***
- ***Configuration (on/off/modify) of Extended Topology***
- ***Configuration/Viewing of SNMP parameters***

Dynamic Views

- ***Configuration (modify) of Extended Topology***
- ***Changing own password***

].

Dependencies: No Dependencies

Application Note: The security related configuration function, Extended Topology Configuration is only available to an administrator who logs into Dynamic View while physically being on the server

FMT_SMR.1-1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1-1 The TSF shall maintain the roles **[*NNM Administrator and NNM operators*].**

FMT_SMR.1.2-1 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

Application Note: This is for the roles of authorized Dynamic View GUI users.

5.2.6 Class FPT: Protection of the TSF

FPT_RVM_EXP_TSF.1 Partial Non-bypassability of the TSP by the TOE

Hierarchical to: No other components.

FPT_RVM_EXP_TSF.1.1 The TSF, when invoked by the underlying platform, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No Dependencies

FPT_SEP_EXP_TSF.1 Partial TSF domain separation by the TOE

Hierarchical to: No other components.

FPT_SEP_EXP_TSF.1.1 The TSF, when invoked by the underlying host platform, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_EXP_TSF.1.2 The TSF, when invoked by the underlying host platform, shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No Dependencies

Application Note: The TOE subjects are the user sessions.

5.2.7 Class FTP: Trusted path/channels

FTP_TRP_EXP_TSF.1 Partial Trusted Path by the TOE

Hierarchical to: No other components.

FTP_TRP_EXP_TSF.1.1: The TSF shall provide a communication path between itself and remote and local users that is logically distinct from other communication paths and relies on the IT environment to provide protection of the trusted path from modification or disclosure using SSL.

FTP_TRP_EXP_TSF.1.2 The TSF shall permit the local users and remote users to initiate communication via the trusted path.

FTP_TRP_EXP_TSF.1.3 The TSF shall require the use of the trusted path for initial user authentication and all communication between Dynamic Views GUI and its users (via web browser).

Dependencies: No Dependencies

5.2.8 Strength of Function

The strength of function (SOF) requirement applies to the authentication mechanism that satisfies the specified FIA_UAU.2 SFR user authentication before any action. This mechanism is invoked for users accessing the TOE over the network interface using HTTPS to gain access to Dynamic Views. The TOE includes a password policy function to meet the FIA_SOS.1 and FIA_AFL.1 requirements, and these are used to constrain the passwords used to satisfy FIA_UAU.2. The SOF metric of resistance of greater than 1 month to password guessing attacks applies for this authentication mechanism. A minimum SOF strength level claim for entire TOE is not applicable because the IT environment provides the authentication mechanism for users of the TOE's CLI functions.

5.3 Security requirements for the IT Environment

HP Network Node Manager requires that the operating system platform to provide reliable time stamps.

Table 5-4 Functional Components for the IT Environment

Item	Component	Component Name
19.	FAU_STG.1	Protected audit trail storage
20.	FDP_ACC.1-2	Subset access control
21.	FDP_ACF.1-2	Security attribute based access control
22.	FIA_UAU.2-2	User authentication before any action
23.	FIA_UID.2-2	User identification before any action
24.	FMT_MSA.1	Management of security attributes
25.	FMT_MSA.3	Static attribute initialisation
26.	FMT_MTD.1-2	Management of TSF data
27.	FMT_SMR.1-2	Security roles
28.	FPT_RVM_EXP_PFM.1	Partial Non-bypassability of the TSP by the platform
29.	FPT_SEP_EXP_PFM.1	Partial TSF domain separation by the platform
30.	FPT_STM.1	Reliable time stamps
31.	FTP_TRP_EXP_PFM.1	Partial Trusted Path by the platform

5.3.1 Class FAU: Security Audit

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 **Refinement:** The ***IT Environment*** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 **Refinement:** The ***IT Environment*** shall be able to **[*prevent*]** unauthorised modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.3.2 Class FDP: User Data Protection

FDP_ACC.1-2 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1-2 **Refinement:** The ***IT Environment*** shall enforce the **[*OS Access Control SFP*]** on **[**

Subjects: root user*, other OS users

Objects: NNM command line interface executables,

***Operations: execute*].**

Dependencies: FDP_ACF.1-2 Security attribute based access control

Application Note: In order to have "root" user access the logged in user must belong to the OS's administrator group and issue the unix command "su" successfully. The "administration group" equates to the "sys:" identifier in the group configuration file (/etc/group) for the host operating systems used for this evaluation.

FDP_ACF.1-2 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1-2 **Refinement:** The ***IT Environment*** shall enforce the **[*OS Access Control SFP*]** to objects based on the following: **[**

Subjects (root):

Assigned Administration Group

Objects (NNM command line interface executable):

NNM command line interface executable (Influences configuration and operation of the TOE)

].

FDP_ACF.1.2-2 **Refinement:** The ***IT Environment*** shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

1. Subjects included in the administration group have root privilege.

2. Subjects may execute NNM command line interface executables if the subject belongs to the administration group.

3. Subjects not included in the administration group do not have execute privilege for NNM command line interface executables.**]**

FDP_ACF.1.3-2 **Refinement:** The ***IT Environment*** shall explicitly authorise access of subjects to objects based on the following additional rules: **[*no additional rules*].**

FDP_ACF.1.4-2 **Refinement:** The ***IT Environment*** shall explicitly deny access of subjects to objects based on the following rules: **[*no additional explicit deny rules*].**

Dependencies: FDP_ACC.1-2 Subset access control

FMT_MSA.3 Static attribute initialization

5.3.3 Class FIA: Identification and Authentication

FIA_UAU.2-2 User authentication before any action

Hierarchical to: No other components.

FIA_UAU.2.1-2 **Refinement:** The ***IT Environment*** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

Application Note: This for authentication of potential CLI users.

FIA_UID.2-2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1-2 **Refinement:** The ***IT Environment*** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Application Note: This for identification of potential CLI users.

5.3.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 **Refinement:** The ***IT Environment*** shall enforce the **[*OS Access Control SFP*]** to restrict the ability to **[*modify, delete*]** the security attributes **[*OS: administrator group, TOE: username, password, role*]** to **[*root*].**

Dependencies: [FDP_ACC.1-2 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR.1-2 Security roles

FMT_SMF.1 Specification of Management Functions

Application Note: The root user, who is also the NNM administrator, must add a user to the administrator group in order for that user to have access to the NNM executables needed to perform NNM administrator duties. The root user is also the one that must configure the TOE's configuration file (via CLI) to provide access to the Dynamic Views GUI.

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 **Refinement:** The ***IT Environment*** shall enforce the **[*OS Access Control SFP*]** to provide **[*restrictive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 **Refinement:** The ***IT Environment*** shall allow the **[*root*]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1-2 Security roles

FMT_MTD.1-2 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1-2 **Refinement:** The ***IT Environment*** shall restrict the ability to **[*see operations specified in Table 5-4*]** the TSF Data **[*as specified in Table 5-4 to the role as specified in Table 5-4*].**

Dependencies: FMT_SMR.1-2 Security roles

FMT_SMF.1 Specification of Management Functions

Table 5-5 Management of TSF Data through CLIs

Roles	Allowed Operations on TSF Data (Management Functions)
root (Via the command line interface)	• **Configuration (on/off), View, Reset (Delete) audit log** • **Backup/Restore/Reset(delete) System data** • **Licensing Tool (adding, removing)** • **Change password to the relational db (extended)** • **Syslog Agent Template modification** • **Configuration (on/off) Syslog Agent** • **Change/modify/delete Data Analysis rules and definitions** • **Modify/delete configuration file for username, password, and role attributes for Dynamic Views** • **Configuration (on/off/modify) of Extended Topology** • **Configuration/Viewing of SNMP parameters**

Application Note: This is for the Management of TSF data available through command line interfaces. Management of TSF through Dynamic Views, which must be protected by the TOE, is defined in the TOE SFR section.

FMT_SMR.1-2 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1-2 **Refinement:** The ***IT Environment*** shall maintain the roles **[*root and other OS users*].**

FMT_SMR.1.2-2 **Refinement:** The ***IT Environment*** shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

Application Note: This is for the roles of authorized CLI users.

5.3.5 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP_PFM.1 Partial Non-bypassability of the TSP by the platform

Hierarchical to: No other components.

FPT_RVM_EXP_PFM.1.1 The security functions of the host platform shall ensure that the host platform security policy enforcement functions are invoked and succeed before each function within the scope of control of the host platform is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP_PFM.1 Partial TSF domain separation by the platform

Hierarchical to: No other components.

FPT_SEP_EXP_PFM.1 The security functions of the host platform shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host platform.

FPT_SEP_EXP_PFM.2 The security functions of the host platform shall enforce separation between the security domains of subjects in the scope of control of the host platform.

Dependencies: No dependencies

Application Note: The subjects for the host platform are the subjects in execution.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT Environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.3.6 Class FTP: Trusted path/channels

FTP_TRP_EXP_PFM.1 Partial Trusted Path by the platform

Hierarchical to: No other components.

FTP_TRP_EXP_PFM.1.1: The IT Environment shall provide a communication path between itself and remote and local users that is logically distinct from other communication paths and protection of the communicated data from modification or disclosure using SSL.

FTP_TRP_EXP_PFM.1.2 The IT Environment shall initiate or permit the local users and remote users to initiate communication via the trusted path.

FTP_TRP_EXP_PFM.1.3 The IT Environment shall require the use of the trusted path for initial user authentication and all communication between Dynamic Views GUI and its users (via web browser).

Dependencies: No Dependencies

5.4 *TOE Security Assurance Requirements*

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-6.

Table 5-6 EAL2 Assurance Components

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

The following sections describe the IT Security Functions of the Network Node Manager (NNM) Server, an embedded database, and NNM User Interfaces. Together these components provide the security functions which satisfy the TOE security functional requirements. This section includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met.

Table 6-1 Security Functional Requirements mapped to Security Functions

SFRs	Security Class	Security Functions	Sub-functions
FAU_GEN.1	Security audit	Audit	AU-1
FAU_SAR.1	Security audit	Audit	AU-2
CA_SDC_EXP.1	Collection and Analysis	Collection, Analysis, Alarm Notification	CA-1
CA_ANL_EXP.1-1	Collection and Analysis	Collection, Analysis, Alarm Notification	CA-2
CA_ANL_EXP.1-2	Collection and Analysis	Collection, Analysis, Alarm Notification	CA-3
CA_RCT_EXP.1	Collection and Analysis	Collection, Analysis, Alarm Notification	CA-4
FIA_UID.2-1	Identification and Authentication	Identification and Authentication	I&A-1
FIA_UAU.2-1	Identification and Authentication	Identification and Authentication	I&A-1
FIA_SOS.1	Identification and Authentication	Identification and Authentication	I&A-2
FIA_AFL.1	Identification and Authentication	Identification and Authentication	I&A-3
FMT_MTD.1-1	Security management	Security management	SM-1
FMT_SMF.1	Security management	Security management	SM-1
FMT_SMR.1-1	Security management	Security management	SM-1
FDP_ACC.1-1	User Data Protection	Access Control	AC-1
FDP_ACF.1-1	User Data Protection	Access Control	AC-1
FPT_RVM_EXP_TSF.1	Protection of the TSF	Partial Protection of the TSF	TSP-1
FPT_SEP_EXP_TSF.1	Protection of the TSF	Pratial Protection of the TSF	TSP-1
FTP_TRP_EXP_TSF.1	Trusted path/channels	Partial Trusted Path/Channel	TPC-1

6.1.2 Audit

6.1.2.1 AU-1 Audit events (FAU_GEN.1)

There is an audit log file stored on the NNM Server as a single ASCII file in a protected directory. The audit trail record is made up of entries that are single line of text. The text includes: Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Auditable events include:

- Startup and Shutdown of Audit Function (which is the same as the startup and shutdown of the system).
- Changes to databases - removal, creation
- Changes to databases - database type used (Oracle, Solid, SQL Server)
- Changes to databases - Password and account changes
- Changes to menus for dynamic views
- Run of backup and restore
- URL access
- Login to Dynamic Views GUI*

*Information for audit is partially provided by Tomcat/Apache logging which is not part of the TOE.

There is no log file management therefore, files continue to grow. An authorized administrator should periodically check these files and when they get large the files should be saved or trimmed. The IT Environment is responsible for providing a timestamp and making sure that the audit log is protected from unauthorized deletion and modification. (IT ENV: FPT_STM.1, FAU_STG.1)

6.1.2.2 AU-2 Audit events (FAU_SAR.1)

The TOE provides a CLI to view the audit trail. The CLI is only accessible to an authorized administrator who has been given root access to the operating system. The information is displayed in a continuous list format that provides the administrator with the ability to select audit records based on audit event type, time, login (username identity), and url login (host identity).

6.1.3 Security Management

6.1.3.1 SM-1 Specification of Management Functions (FMT_MTD.1-1, FMT_SMF.1, FMT_SMR.1-1)

Security Management capabilities are mainly limited to command line interfaces which must be protected by the IT Environment. There are 2 security functions that are available via the Dynamics View GUI interface. The security management functions provided are as follows:

CLI

- Configuration (on/off) *(ovauditcfg.ovpl),* View (ovauditview.ovpl), Reset (OS Delete File) audit log.
- Backup/Restore/Reset(delete) System data *(OVbackup.ovpl, ovrestore.ovpl, and ovalarmadm).*
- Licensing Tool (adding, removing) *(ovautoLic, ovnnmInstallLic, ovnnmPassword).*
- Change password to the relational db (extended) *(ovdwconfig.ovpl)*
- Syslog Agent Template modification *(ovsyslogcfg, ovsysloggen)*
- Configuration (on/off) Syslog Agent*(setupSyslog.ovpl)*
- Change/modify/delete Data Analysis rules and definitions(xnmcollect, xnmevents, xnmpolling, ecsmgr, ovet_toposet)
- Modify/delete of username, password, and role attributes in the configuration file for use of the Dynamic Views environment. *(dvUsersManager.ovpl)*
- Configuration (on/off/modify) of the Extended Topology *(setupExtTopo.ovpl)*

- Configuration of and viewing of SNMP parameters (i.e. polling interval, community strings, time-out value, retry count, and remote port) used by NNM for data collection. (xnmsnmpconf, statusIntervalConf.ovpl)

Dynamic Views

- Configuration (on/off) of the extended topology database *(only available when Dynamic Views is accessed from on the NNM Server and the authorized user's role equals NNM Administrator)*
- Changing own password (*all authorized user roles*)

The TOE is required to provide access control to prevent unauthorized users from gaining access to the Dynamic Views interface for the NNM administrator. The TOE maintains roles distinguishing between NNM administrators and NNM operators. The roles are assigned when the user account is created by "root" using a CLI (FMT_MSA.1.1-2). The security related configuration function, Extended Topology Configuration is only available to an NNM administrator who logs into Dynamic View while physically being on the server. The configuration option is not available to anyone, including the NNM administrator, when logging into Dynamic Views remotely.

The security function for changing one's own password through Dynamic Views is available to all authorized users/roles whether local or remote.

The IT Environment is required to provide the access control to prevent unauthorized users from gaining access to the CLIs. Authorized users are those who have been given "root" access privilege to the operating system. In order to have "root" user access the logged in user must belong to the OS's administrator group and issue the unix command "su" successfully. The "administration group" equates to the "sys:" identifier in the group configuration file (/etc/group) for the host operating systems used for this evaluation. (IT ENV: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1-2, FMT_SMR.1-2)

Application Note: Unlocking a user account that has been locked due to failed login attempts is the equivalent of resetting the password. Therefore, unlocking a user account is not listed as a separate security function.

6.1.4 Collection, Analysis, and Alarm Notification

6.1.4.1 CA-1 System data collection (CA_SDC_EXP.1)

HP NNM collects system data directly from the targeted network via well known communication protocols from the targeted network objects. NNM uses several protocols to maintain communication channels with each managed device on the targeted network. These include:

- SNMPv1; SNMPv2
- TCP/IP
- HTTP/HTTPS
- UDP
- ICMP
- ARP/RARP

NNM also uses other, lower-level families of protocols (sometimes referred to as services), such as the ARPA family, the Berkeley family, and the NFS family. These protocols are used for functions such as file transfer, e-mail, or remote login.

The Syslog Agent is another source of the collected data. In the evaluated configuration the embedded Syslog Agent uses preconfigured templates to parse incoming syslog (from host OS) messages matching a certain pattern. The matched syslog messages are mapped to SNMP traps and displayed in the NNM alarm browser. These templates are customizable via a CLI by an authorized administrator.

The TOE collects and records the following information: Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Sources for Information collected includes: SNMP traps (including Syslog entries converted to traps), SNMP Information, ICMP Information, and HTTP Information.

The collection of data happens automatically at startup and on predefined polling intervals. The system can is designed to discover new nodes for monitoring and collecting information from a predefined/configurable list. The modifying of the polling interval is strictly a security management function and can be accomplished via a CLI by an authorized administrator. Managing and un-managing of nodes is also considered a day-to-day operation and not a security management function. Therefore, managing and un-managing of nodes can also be accomplish via the Dynamic Views GUI interface by an authorized user or by CLIs by an authorized administrator.

The Extended Topology model of recurring discovery differs from the continuous discovery present in NNM Classic. Extended Topology captures data about your network as it exists during the most recent discovery cycle, or the most recent previous discovery cycles. It does not update the data between discovery cycles. This means that only the layer 2 connections that exist during Extended Topology discoveries get recorded. In addition, device information (such as VLAN, port aggregation, and ATM data) is gathered only from devices that are accessible during the Extended Topology discoveries. An “accessible” device responds to SNMP requests from NNM. For this to happen, NNM must be configured to use the correct SNMP GET-Community name for the device. The configuration and modification of the SNMP GET-Community name per device is considered a day-to-day operation and not a security management function. Therefore, this activity can be accomplished via the Dynamic Views GUI interface by an authorized user or by CLIs by an authorized administrator.

6.1.4.2 CA-2 Analyzer analysis (CA_ANL_EXP.1-1)

HP NNM performs sampling on all system data received. HP NNM records within each SNMP collect analytical result at least the following information: Date and time of the result, type of result, and identification of data source. HP NNM will detect a state change of a device and will report this. A timestamp is recorded when a state change occurs.

NNM contains pre-defined event reduction configurations so that the user sees fewer alarms that show the relationships and dependencies between network events. Event reduction involves processing events based previous, current, or subsequent events.

In addition, NNM includes an auto-baseline capability to automatically set alarm thresholds for collected data based on deviations from historical data. If these thresholds are exceeded, then NNM will generate an alarm. Threshold events give authorized users a way to be notified of traffic patterns that are outside normal expectations. For example, an authorized user can set a threshold to monitor disk utilization on a server. If the amount of free disk falls below the set threshold, NNM can notify an operator, or take other predetermined actions (such as mailing a message).

All configured alarm events are viewed through the NNM Alarm Browser.

6.1.4.3 CA-3 Analyzer analysis (CA_ANL_EXP.1-2)

HP NNM will perform signature analysis function on all collect data as it is received.   Signature analysis involves the use of patterns corresponding to known protocols. For example, if the collected snmp or icmp data is inaccurately packaged, then it is not trusted and dropped. If the collected data is correct, then the data is allowed to populate the database for analysis performed by CA-2 above.

There are no user interfaces to this analyzer and it is not configurable by the end user.

6.1.4.4 CA-4 Analyzer react (CA_RCT_EXP.1)

The Alarm Browser presents alarm data via the Dynamic Views GUI interface. Through the Alarm Browser, an authorized user can filter alarms and take actions on specific alarms. All alarms are global to all web users, as are acknowledgments, delete, change category, and change severity functions. The web-based Alarm Browser service, ovalarmsrv, is started by ovstart when an authorized administrator starts an NNM session on the management station.

The alarm browser can be used for the following:

- View Error, Threshold, Status, Configuration, Application Alert (Audit alarms* and major application issues such as a process terminating unexpectedly), and Problem Diagnosis Alarms.
- Acknowledge/Unacknowledge alarms.
- Move alarms to a different category.
- Assign alarm severities.
- Filter alarms.
- Delete alarms.
- Examine alarm details to find correlated events.

**Application Note: The Audit alarms (shown in the Alarm Browser) are not the equivalent to the audit trail which is a separate file.*

All instantiations of the Dynamic Views interface and CLIs share the same event database and configuration files for alarms. Therefore, no matter which Alarm Browser is used, the displayed list of alarms remains current at all times. Whenever someone acknowledges an alarm, deletes an alarm, or changes severity for an alarm everyone on the team sees the change.

6.1.5 Access Control

6.1.5.1 AC-1 Access Control (FDP_ACC.1-1, FDP_ACF.1-1)

The TOE relies on two access control policies. One the TOE provides and the second one the OS system provides.

The TOE provides security attribute access control to protect the Dynamic Views GUI from unauthorized users. The TOE Access Control SFP relies on the username & password security attribute for determining whether the requestor is authorized to interact with the Dynamic View TOE component.

The following is the rules for access control decisions:

1. Subjects must be included in the TOE configuration file.
2. Subject’s supplied username and password must match the username and password stored in the TOE configuration file.

3. Subject’s account must not be disabled via the failed access attempts lockout feature.

The requesting user’s I&A information must pass all of the 3 rules in order to be granted access to the Dynamic Views interface.

Once the requesting user has been granted access, the TOE uses the assigned role to the user and the originating IP address of the requesting user’s session to determine which Dynamic View functions the user is allowed to have.

1. When the requesting session is from a remote machine, i.e from the physical NNM server, the Dynamic Views interface for an operator is displayed.

2. When the requesting session is from the local NNM server and the authorized user’s role is an NNM operator, the Dynamic Views interface for an NNM operator will be displayed.

3. When the requesting session is from the local NNM server and the authorized user’s role is an NNM administrator, the Dynamic Views interface for an NNM Administrator (has extended topology configuration) will be displayed.

Failed and successful access attempts generate audit events.

The OS provides access control to prevent non-root users from executing the CLIs for security management. In order to have “root” user access the logged in user must belong to the OS’s administrator group and issue the unix command “su” successfully. The “administration group” equates to the “sys:” identifier in the group configuration file (/etc/group) for the host operating systems used for this evaluation (IT ENV: FDP_ACC.1-2, FDP_ACF.1-2).

6.1.6 Identification and Authentication

6.1.6.1 I&A-1 Identification and Authentication (FIA_UAU.1-2 & FIA_UID.2-1)

NNM requires each user to be successfully identified and authenticated with a password before being allowed any other actions.

NNM provides I & A of users attempting to access the Dynamic Views GUI. The TOE collects the username and password via a HTML form provided by the server. The collection is performed via secure HTTPS/SSL communication between the web browser and the NNM server (Tomcat/Apache must be configured to use SSL). The supplied information is then verified against the TOE’s configuration file to ensure an exact match. A password mechanism is used for authentication. The TOE’s configuration file does not store the passwords in the clear

A failed login attempt is responded too with a generic Access Not Allowed web page, a failed access attempt audit event is generated, and a counter for failed login attempts is increased by one. The Dynamic Views home page does not get deployed to the requesting user’s browser until successful I & A.

NNM relies on the Operating System to provide I & A of the *root* user before being allowed to manage TOE configuration through the CLI (IT ENV: FIA_UAU.2-2 & FIA_UID2-2).

6.1.6.2 I&A-2 Password Mechanism (FIA_SOS.1)

The password mechanism ensures that the assigned password (initial password set by the NNM administrator or the authorized user changes password request) meets a hard-coded password policy of a minimum of 8 characters where there is at least one character each of upper case, lower case, special, and numeric type.

A change password request requires the user to enter the current password and enter the new password twice. The TOE then verifies the requester's current password. If the password is not correct then the password is not changed, the user is notified (via a pop-up window) of an incorrect password, an audit record is generated, and the input window is then re-presented to the requester.

If the password matches the new password inputs are checked to see if they match. If they do not match the user is notified of the error and the input window is then re-presented to the requester. If they do match the new password is checked to see if it meets the password policy criteria. If the password does not meet the password policy criteria then the user is notified of the error with a pop-up window that explains the password policy criteria. If the requested password meets the password policy criteria then the TOE will change the current password to the twice verified new password.

6.1.6.3 I&A-3 Authentication Failure handling (FIA_AFL.1)

The TOE keeps track of the number of sequential failed authentication attempts made to a particular username. If the number of failed authentication reaches 5 then the TOE will disable the user's account by overwriting the password field with a non-valid password string and generate an audit event. The only way to unlock the user's account is having the NNM administrator re-set the password field to a valid password using a command line interface.

6.1.7 Partial Protection of the TSF

6.1.7.1 TSP-1 TOE Self Protection (FPT_RVM_EXP_PFM.1, FPT_SEP_EXP_PFM.1)

The TOE ensures that security protection enforcement functions are invoked and succeed before each function within its scope of control is allowed to proceed. The TOE's domain is the NNM server and Dynamic Views. All user operations are conducted in the context of an associated session. These sessions are allocated only after successful authentication. User operations are checked for conformance to the granted level of access, and rejected if not conformant. The sessions are destroyed when the corresponding user sessions end. Communications between Dynamic Views and the NNM server is accomplished through a requirement that Tomcat/Apache being configured to use SSL. (See Partial Trusted Path/Channel below)

Since the TSF is software, it relies on the IT environment OS and underlying hardware to ensure that the Operating System DAC Security Policy enforcement functions are invoked and succeed before each function within the Operating System's Scope of Control is allowed to proceed, and to support non-bypassability. To support non-bypassability, the system data files stored on the operating system are binary executables, this prevents any user from modifying the files, only the TSF generates the files during installation. Further protection is provided by the underlying assumption that the TOE is maintained in a physically secure environment with no untrusted users or software. (IT Env: FPT_RVM_EXP_PFM.1, FPT_SEP_EXP_PFM.1)

6.1.8 Partial Trusted Path/Channel

6.1.8.1 TPC-1 Trusted Path (FTP_TRP_EXP_TSF.1)

The TSF provides a communication path between itself and remote and local users that is logically distinct from other communication paths. The TSF relies on the IT environment to provide protection of the trusted path from modification or disclosure using SSL. The TSF permits the local users and remote users to initiate communication via the trusted path for initial user authentication and all communication between Dynamic Views GUI and the NNM Server.

The collection of I&A information is performed via secure HTTPS/SSL communication between the web browser and the NNM server (Tomcat/Apache must be configured to use SSL). HTTPS and Tomcat are considered external to NNM, and as such, they are considered part of the IT environment. (IT Env: FPT_TRP_EXP_PFM.1)

6.2 SOF Claims

The strength of function (SOF) requirement applies to the authentication mechanism that satisfies the specified FIA_UAU.2 SFR user authentication before any action. This mechanism is invoked for users accessing the TOE over the network interface using HTTPS to gain access to Dynamic Views. The TOE includes a password policy function to meet the FIA_SOS.1 and FIA_AFL.1 requirements, and these are used to constrain the passwords used to satisfy FIA_UAU.2. The SOF metric of resistance of greater than 1 month to password guessing attacks applies for this authentication mechanism. This metric is adequate to handle a potential attacker that is unsophisticated, with access to only standard equipment and public information about the TOE.

A minimum SOF strength level claim for entire TOE is not applicable because the IT environment provides the authentication mechanism for users of the TOE's CLI functions.

6.3 Assurance Measures

The HP Network Node Manager satisfies the assurance requirements for Evaluation Assurance Level EAL2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-2 Assurance Measures and How Satisfied

Item	Component	Evidence Requirements	How Satisfied
1	ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	NNM7 51_Config_Mgmt_v2 1.doc
2	ADO_DEL.1	Delivery Procedures	F1-11729 (C) NNM 7.51 Engl.xls F1-11733-B (Word)USB update NNM 7 51.doc More info on delivery.doc MSO Product Structure Guidelines.ppt NNM AE-SE 7.51 Pull Letter with EMEA.doc
3	ADO_IGS.1	Installation, generation, and start-up procedures	HP Network Node Manager Quick Start Installation Guide Managing Your Network with NNM Using Extended Topology NNM Security Advisory Guide ManPages Release Notes HP NNM 7.51
4	ADV FSP.1	Functional Specification	FSP interfaces idx 11-16-2006-hl

Item	Component	Evidence Requirements	How Satisfied
5	ADV_HLD.1	High-Level Design	
6	ADV_RCR.1	Representation Correspondence	FSP_interfaces_idx_11-16-2006-hl
7	AGD_ADM.1	Administrator Guidance	HP Network Node Manager Installation Quick Start Reporting and Data Analysis with Network Node Manager Creating and Using Registration Files A Guide to Scalability and Distribution for Network Node Manager Integrating HP OpenView Reporter NNM NIAP Security WhitePaper Release notes Dynamic Views online Help Welcome to Network Node Manager Managing Your Network with NNM Using Extended Topology NNM Security Advisory Guide ManPages
8	AGD_USR.1	User Guidance	Dynamic Views online Help Welcome to Network Node Manager Managing Your Network with NNM Using Extended Topology NNM Security Advisory Guide ManPages
9	ATE_COV.1	Test Coverage Analysis	TestCoverage_11-16-2006.xls
10	ATE_FUN.1	Test Documentation	Test Procedures.txt Test Scripts Test Results (details/general stataus,Journal)
11	ATE_IND.2	TOE for Testing	TOE for Testing
12	AVA_SOF.1	SOF Analysis	HP_NNMSOFAnalysisv0.1(2006-11-16).doc
13	AVA_VLA.1	Vulnerability Analysis	NNM Security Advisory Guide Vulnerability/Product.xls Vulnerability/NNMSecurityPage.htm

7 PP Claims

The HP Network Node Manager Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Assumptions

Table 8-1 shows that all of the assumptions are addressed by Non-IT security objectives. Rationale is provided for each Assumption in the table.

Table 8-1 All Threats to Security Countered

Item	Assumption ID	Non-IT Objective Addressing Assumption	Rationale
1	A.AdmTra	ON.Person	This objective provides for competent personnel to administer the TOE.
		ON.Install	This objective ensures the TOE is delivered, installed, managed, and operated by competent individuals.
		ON.Operations	This objective ensures the TOE is managed and operated in a secure manner as outlined in the supplied guidance.
2	A.NoUntrusted	ON.NoUntrusted	This objective provides for the protection of the TOE from untrusted software and users.
3	A.Physical	ON.Physical	This objective provides for the physical protection of the TOE software.
4	A.Users	ON.ProtectAuth	This objective provides for users protecting their authentication data.

8.1.2 Threats to Security

Table 8-2 shows that all the identified threats to security are countered by Security Objectives for the TOE and IT Environment. Rationale is provided for each Threat in the table.

Table 8-2 All Assumptions Addressed

Item	Threat	Security Objective	Rationale
1	T.FailAnalyze	O.CollectData	O.CollectData mitigates this threat by collecting and storing system and network data from the managed nodes.
		O.AnalyzeData	O.AnalyzeData mitigates this threat by applying sampling and analytical processes and information to derive conclusions (past, present, or future) on the collected data from managed nodes.
2	T.FailReact	O.React	O.React mitigates this threat by sending an alarm if a configured threshold has been exceeded.
3	T.Mismgmt	O.Roles	O.Roles mitigates this threat by providing roles that coorespond to specific functions available to an NNM administrator vs NNM operator
		O.SecMgt	O.SecMgt mitigates this threat by providing the functionality to enable authorized aministrator(s) to effectively manage the TOE and its security functions through Dynamic Views.

		OE.Roles	OE.Roles mitigates the threat by the IT Environment maintaining the roles of “root” and other users.
		OE.SecMgt	OE.SecMgt mitigates this threat by providing the functionality to enable authorized aministrator(s) to effectively manage the TOE and its security functions through Command Line Interfaces.
4	T.Privil	O.Access	O.Access mitigates the threat by providing authorized administrators with the means of controlling and limiting access to TSF data on the basis of user identity, password, and user roles, in accordance with the specification of the management of TSF data through Dynamic Views GUI.
		O.Authorize	O.Authorize mitigates the threat by: identifying and authenticating Dynamic Views GUI web users, prior to allowing access to authorized TOE functions and data.
		OE.Access	OE.Access mitigates the threat by providing authorized administrators with the means of controlling and limiting access to TSF data on the basis of user identity, password, and user roles, in accordance with the specification of the management of TSF data through Command Line Interfaces.
		OE.Authorize	OE.Authorize mitigates the threat by: identifying and authenticating root users on the OS prior to allowing access to authorized TOE functions and data.
		ON.Operations	ON.Operations mitigates this threat by managing and operating the TOE in a secure manner as outlined in the supplied guidance.
		ON.Physical	ON.Physical mitigates this threat by ensuring the portions of the TOE critical to the security policy are protected from any physical attack.
5	T.Tamper	O.NonBypass	O.NonBypass mitigates the threat by ensuring that its protection mechanisms cannot be bypassed.
		O.Protect	O.Protect mitigates the threat by maintaining a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure.
		O.Partial_Trusted Comm	O.Partial_TrustedComm mitigates the threat by ensuring that communication channels prevent the capture of login information that could lead to bypassing the protection mechanisms.
		OE.NonBypass	OE.NonBypass mitigates the threat by ensuring that its protection mechanisms cannot be bypassed.
		OE.Protect	OE.Protect mitigates the threat by maintaining a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure.
		OE.Partial_Trusted Comm	OE.Partial_TrustedComm mitigates the threat by ensuring that communication channels prevent the capture of login information that could lead to bypassing the protection mechanisms using SSL.
6	T.Undetect	O.Audit	O.Audit mitigates this threat by providing the capability to detect, create, and view records of security relevant events.
		OE.AuditProtect	OE.AuditProtect mitigates the threat by providing the capability to protect audit information from unauthorized deletion, modification, and viewing.

		OE.Time	OE.Time helps to mitigate this threat by ensuring that audit records have correct timestamps.

8.1.3 Reverse Mapping

The following tables are provided to show completeness by demonstrating all security objectives for the TOE and Environment map to at least one threat or assumption.

Table 8-3 Reverse Mapping of TOE Security Objectives to Threats

Item	Security Objective	Threat
1	O.Audit	T.Undetect
2	O.AnalyzeData	T.FailAnalyze
3	O.CollectData	T.FailAnalyze
4	O.React	T.FailReact
5	O.Roles	T.Mismgmt
6	O.SecMgt	T.Mismgmt
7	O.Access	T.Privil
8	O.Authorize	T.Privil
9	O.NonBypass	T.Tamper
10	O.Protect	T.Tamper
11	O.Partial_TrustedComm	T.Tamper

Table 8-4 Reverse Mapping of Security Objectives for the Environment to Threats/ Assumptions

Item	Security Objective	Threat/Assumption
12	OE.AuditProtect	T.Undetect
13	OE.Time	T.Undetect
14	OE.Roles	T.Mismgmt
15	OE.SecMgt	T.Mismgmt
16	OE.Access	T.Privil
17	OE.Authorize	T.Privil
18	OE.NonBypass	T.Tamper
19	OE.Protect	T.Tamper
20	OE.Partial_TrustedComm	T.Tamper
21	ON.Install	A.AdmTra
22	ON.NoUntrusted	A.NoUntrusted
23	ON.Operations	A.AdmTra T.Privil
24	ON.ProtectAuth	A.Users
25	ON.Person	A.AdmTra

26	ON.Physical	A.Physical T.Privil

8.2 *Security Requirements Rationale*

8.2.1 Functional Requirements

Table 8-5 shows that all of the security objectives of the TOE and IT environment are satisfied. Rationale for each objective is included in the below table.

Table 8-5 All Objectives Met by Functional Components

Item	Security Objective	SFR ID	SFR Title	Rationale
Audit TOE Support				
1	O.Audit	FAU_GEN.1	Audit data generation	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that an administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event.
		FAU_SAR.1	Audit Review	FAU_SAR.1 provides the ability to review the audits in a user-friendly manner.
Audit IT Environment Support				
12	OE.AuditProtect	FAU_STG.1	Protected audit trail storage	FAU_STG.1 restricts the ability to modify audit records and requires the IT Environment (OS) to protect the files. This ensures the integrity of the audit trail is maintained.
13	OE.Time	FPT_STM.1	Reliable time stamps	FPT_STM.1.1 requires that the IT Environment (OS) provide reliable time stamps for TSF functions.
Collection, Analysis, and Alarm Notification TOE Support				

2	O.CollectData	CA_SDC_EXP.1	System data collection	CA_SDC_EXP.1 requires the collection and recording of system information from the managed node(s).
3	O.AnalyzeData	CA_ANL_EXP.1-1	Analyzer analysis	CA_ANL_EXP.1.1-1 The TOE performs sampling on all system data received. CA_ANL_EXP.1.2-1 The TOE records within each analytical result at least the following information: a) Date and time of the result b) Type of result c) Identification of data source
		CA_ANL_EXP.1-2	Analyzer analysis	CA_ANL_EXP.1.1-2 requires the performance of a signature analysis function on all system data received.
4	O.React	CA_RCT_EXP.1	Analyzer react	CA_RCT.1.1 the TOE sends an alarm to the alarm browser upon detection of a potential security violation.
Security Management TOE Support				
5	O.Roles	FMT_SMR.1-1	Security Roles	FMT_SMR.1-1 requires a role distinction between NNM administrators and NNM operators. These roles allow for the restriction of security functions to the appropriate user.
6	O.SecMgt	FMT_MTD.1-1	Management of TSF data	FMT_MTD.1-1 Provides for the restriction of Dynamic Views security managements functions to associated roles.
		FMT_SMF.1	Specification of Management Functions	FMT_SMF.1.1 requires that the TSF provide specific management functions
Security Management IT Environment Support				

14	OE.Roles	FMT_SMR.1-2	Security roles	FMT_SMR.1-2 requires IT Environment (OS) have a role distinction of “root” and other OS users. These roles allow for the restriction of security functions to the “root”.
15	OE.SecMgt	FMT_MTD.1-2	Management of security attributes	FMT_MTD.1-2 Provides for the restriction of the TOE CLIs to the IT Environment (OS) user ”root”.
		FMT_MSA.1	Management of security attributes	FMT_MSA.1.1 allows IT Environment (OS) user “root” to manage the specified security attributes needed to protect the TOE CLIs.
		FMT_MSA.3	Static attribute initialisation	FMT_MSA.3.1 ensures that the default values of the IT Environment (OS) security attributes are appropriately restrictive in nature.
User Data Protection TOE Support				
7	O.Access	FDP_ACC.1-1	Subset access control	FDP_ACC.1-1 requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.
		FDP_ACF.1-1	Security attribute based access control	FDP_ACF.1.1-1 allows the TSF to enforce access based upon security attributes. Furthermore, the TSF may have the ability to explicitly authorise or deny access to an object based upon security attributes.
User Data Protection IT Environment Support				
16	OE.Access	FDP_ACC.1-2	Subset access control	FDP_ACC.1-2 requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the OS.

		FDP_ACF.1-2	Security attribute based access control	FDP_ACF.1.1-2 allows the OS to enforce access based upon security attributes and named groups of attributes. Furthermore, the OS may have the ability to explicitly authorise or deny access to an object based upon security attributes.
Identification and Authentication TOE Support				
8	O.Authorize	FIA_UAU.2-1	User Authentication before any action	FIA_UAU.2-1 requires that administrators and other users authenticate themselves to the TOE before performing duties. This covers the Dynamic Views interface.
		FIA_UID.2-1	User Identification before any action	FIA_UID.2-1 requires that users identify themselves to the TOE before any action will be allowed by the TSF. This covers the Dynamic Views interface.
		FIA_AFL.1	Authentication Failure Handling	FIA_AFL.1 provides for a stronger authentication mechanism by forcing a lockout of a user account that has failed authentication several time in a row.
		FIA_SOS	Verification of secrets	FIA_SOS.1 provides the constraints for a password mechanism used for authentication.
Identification and Authentication IT Environment Support				
17	OE.Authorize	FIA_UAU.2-2	User Authentication before any action	FIA_UAU.2-2 requires that administrators and other users authenticate themselves as “root” to the OS before performing administrative duties. This covers the Command Line Interface.
		FIA_UID.2-2	User Identification before any action	FIA_UID.2-2 requires that users identify themselves to the OS before any action will be allowed by the OS. This covers the Command Line Interface.
Protection of the TOE Security Functions TOE Support				

9	O.NonBypass	FPT_RVM_EXP_TSF.1	Partial Non-bypassability of the TSP by the TOE.	FPT_RVM_EXP_TSF.1 ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since interfaces may otherwise exist that would provide a user with access to TOE resources regardless of the defined policies. This includes controlling the accessibility to interfaces, as well as what access control is provided within the interfaces. The explicitly specified version is used to distinguish the aspects of FPT_RVM provided by the TOE vs. the aspects provided by the IT environment.
10	O.Protect	FPT_SEP_EXP_TSF.1	Partial TSF domain separation by the TOE	FTP_SEP_EXP_TSF.1 ensures the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version is used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment.
Protection of the TOE Security Functions IT Environment Support				

18	OE.NonBypass	FPT_RVM_EXP_PFM.1	Non-bypassability of the TSP by the platform	FPT_RVM_EXP_PFM.1 ensures that the IT Environment makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Without this non-bypassability requirement, the IT Environment could not be relied upon to completely enforce the security policies, since interfaces may otherwise exist that would provide a user with access to TOE resources regardless of the defined policies. This includes controlling the accessibility to interfaces, as well as what access control is provided within the interfaces. The explicitly specified version is used to distinguish the aspects of FPT_RVM provided by the TOE vs. the aspects provided by the IT environment.
19	OE.Protect	FPT_SEP_EXP_PFM.1	Partial TSF domain separation by the platform	FTP_SEP_EXP_PFM.1 ensures the IT Environment provides a domain that protects itself from untrusted users. If the IT Environment cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version is used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment.
	Trusted Path TOE Support			
11	O.Partial_TrustedComm	FTP_TRP_EXP_TSF.1	Partial Trusted Path by the TOE	FTP_TRP_EXP_TSF.1 ensures a trusted communications path for potential users to authenticate to the NNM Server in order to gain access to Dynamics view.
	Trusted Path IT Environment Support			
20	O.Partial_TrustedComm	FTP_TRP_EXP_PFM.1	Partial Trusted Path by the platform	FTP_TRP_EXP_PFM.1 ensures a trusted communications path using SSL enabled Tomcat/Apache web server for potential users to authenticate to the NNM Server in order to gain access to Dynamics view.

Table 8-6 Reverse mapping of SFRs to Security Objectives

Note: Table 8-6 has been included as a consistency check to show that each SFR maps back to at least one security objective.

Item	SFR ID	Security Objective
1	FAU_GEN.1	O.Audit
2	FAU_SAR.1	O.Audit
3	CA_SDC_EXP.1	O.CollectData
4	CA_ANL_EXP.1-1	O.AnalyzeData
5	CA_ANL_EXP.1-2	O.AnalyzeData
6	CA_RCT_EXP.1	O.React
7	FDP_ACC.1-1	O.Access
8	FDP_ACF.1-1	O.Access
9	FIA_AFL.1	O.Authorize
10	FIA_SOS.1	O.Authorize
11	FIA_UID.2-1	O.Authorize
12	FIA_UAU.2-1	O.Authorize
13	FMT_MTD.1-1	O.SecMgt
14	FMT_SMF.1	O.SecMgt
15	FMT_SMR.1-1	O.Roles
16	FPT_SEP_EXP_TSF.1	O.Protect
17	FPT_RVM_EXP_TSF.1	O.NonBypass
18	FTP_TRP_EXP_TSF.1	O.Partial_TrustedComm
19	FAU_STG.1	OE.AuditProtect
20	FDP_ACC.1-2	OE.Access
21	FDP_ACF.1-2	OE.Access
22	FIA_UAU.2-2	OE.Authorize
23	FIA_UID.2-2	OE.Authorize
24	FMT_MSA.1	OE.SecMgt
25	FMT_MSA.3	OE.SecMgt
26	FMT_MTD.1-2	OE.SecMgt
27	FMT_SMR.1-2	OE.Roles
28	FPT_RVM_EXP_PFM.1	OE.NonBypass
29	FPT_SEP_EXP_PFM.1	O.Protect
30	FPT_STM.1	OE.Time
31	FTP_TRP_EXP_PFM.1	OE.Partial_TrustedComm

8.2.2 Dependencies

Table 8-7 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. If the TOE dependency is met by an SFR in the IT Environment an (E) will be next to the reference number.

Table 8-7 TOE Dependencies Satisfied

Item	SFR ID	SFR Name	Dependencies	Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	E(19)
2	FAU_SAR.1	Audit Review	FAU_GEN.1	1
3	CA_SDC_EXP.1	System data collection	None	N/A
4	CA_ANL_EXP.1-1	Analyzer analysis	CA_SDC_EXP.1	3
5	CA_ANL_EXP.1-2	Analyzer analysis	CA_SDC_EXP.1	3
6	CA_RCT_EXP.1	Analyzer react	CA_SDC_EXP.1 CA_ANL_EXP.1*	3 4,5
7	FDP_ACC.1-1	User Data Protection	FDP_ACF.1-1	8
8	FDP_ACF.1-1	Security attribute based access control	FDP_ACC.1-1 FMT_MSA.3	7 E(25)
9	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	12(H)
10	FIA_SOS.1	Verification of secrets	None	N/A
11	FIA_UID.2-1	User Identification before any action	None	N/A
12	FIA_UAU.2-1	User Authentication before any action	FIA_UID.1	11(H)
13	FMT_MTD.1-1	Management of TSF data	FMT_SMR.1-1 FMT_SMF.1	15 14
14	FMT_SMF.1	Specification of Management Functions	None	N/A
15	FMT_SMR.1-1	Security Roles	FIA_UID.1	11(H)
16	FPT_RVM_EXP_TSF.1.	Partial Non-bypassability of the TSP by the TOE	None	N/A
17	FPT_SEP_EXP_TSF.1	Partial TSF domain separation by the TOE	None	N/A
18	FTP_TRP_EXP_TSF.1	Partial Trusted Path by the TOE	None	N/A

Table 8-8 IT Environment Dependencies are Satisfied

Item	SFR ID	SFR Name	Dependencies	Reference
19	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	T(1)
20	FDP_ACC.1-2	Subset access control	FDP_ACF.1-2	21
21	FDP_ACF.1-2	Security attribute based access control	FDP_ACC.1-2	20
			FMT_MSA.3	25
22	FIA_UAU.2-2	User authentication before any action	FIA_UID.1	23(H)
23	FIA_UID.2-2	User identification before any action	None	N/A
24	FMT_MSA.1	Management of security attributes	FDP_ACC.1-2	20
			FMT_SMF.1	T(14)
			FMT_SMR.1-2	27
25	FMT_MSA.3	Static attribute initialisation	FMT_MSA.1	24

Item	SFR ID	SFR Name	Dependencies	Reference
			FMT_SMR.1-2	27
26	FMT_MTD.1-2	Management of TSF data	FMT_SMR.1 FMT_SMF.1	27 T(14)
27	FMT_SMR.1-2	Security roles	FIA_UID.1	23(H)
28	FPT_RVM.1	Non-bypassability of the TSP	None	N/A
29	FPT_SEP.1	TSF domain separation	None	N/A
30	FPT_STM.1	Reliable time stamps	None	N/A
31	FTP_TRP_EXP_PFM.1	Partial Trusted Path by the platform	None	N/A

8.2.3 Rationale why dependencies are not met

All dependencies are met.

8.2.4 Strength of Function Rationale

The strength of function (SOF) requirement applies to the authentication mechanism that satisfies the specified FIA_UAU.2 SFR user authentication before any action. This mechanism is invoked for users accessing the TOE over the network interface using HTTPS to gain access to Dynamic Views. The TOE includes a password policy function to meet the FIA_SOS.1 and FIA_AFL.1 requirements, and these are used to constrain the passwords used to satisfy FIA_UAU.2. The SOF metric of resistance of greater than 1 month to password guessing attacks applies for this authentication mechanism. A minimum SOF strength level claim for entire TOE is not applicable because the IT environment provides the authentication mechanism for users of the TOE’s CLI functions.

8.2.5 Assurance Rationale

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.6 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, each of the SFRs builds on the others. For example, FAU_GEN.1 details the auditable events generated by the TSF. FAU_SAR.1 provide for an administrator to be able to view the audit trail in a selective manner. The IT Environment provides the timestamp and protection of the audit trail (FPT_STM.1 and FUA_STG.1).

FMT_SMF.1, FMT_MTD.1-1, and FMT_MTD.1-2 specifies the functional management of TSF Data and the restriction of identified functions to the administrator for Dynamic Views and “root” for CLIs. Installation functions (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM) documents the management functions which are mainly command line interfaces (that requires IT environment protected) and Dynamic Views GUI (that requires the TOE protection).

Both the TOE and the IT environment are required to identify and authenticate users prior to allowing access to the TSF (FIA_UID.2 and FIA UAU.2). The TOE uses the access rules identified in FDP_ACC.1-1 and FDP_ACF.1-1 to satisfy FIA_UID.2-1, FIA_UAU.2-1. The access rules for authentication require a password mechanism that is constrained by FIA_SOS.1. The authentication mechanism is further strengthened via a user lockout feature constrained by authentication failure handling requirement FIA_AFL.1. All of these requirements work in concert to restrict access to the Dynamic Views GUI to the NNM administrator or NNM operator (FMT_SMR.1-1).

The IT environment uses the access rules identified in FDP_ACC.1-2 and FDP_ACF.1-2 to satisfy FIA_UID.2-2 and FIA_UAU.2-2. The access rules for authentication are defined in FDP_ACC.1-2 and FDP_ACF.1-2. The IT environment must be able to delineate between “root” and other users (FMT_SMR.1-2). The security management functions that are command line interfaces are restricted to the “root” user of the operating system. Since all management of security attributes, used for restricting access to both CLI (FDP_AC*-2) and the Dynamic Views GUI (FDP_AC*-1), can only be modify by root, the FMT requirements FMT_MSA.1. and FMT_MSA.3 are only identified in the IT Environment.

CA_SDC_EXP.1 makes sure the TOE is able to collect the specified system data from the managed nodes on the target network. CA_ANL_EXP.1-1 requires the TOE to perform sampling on all data. CA_ANL_EXP.1-2 requires the TOE to perform signature analysis on all system data received. CA_RCT_EXP.1 requires the TOE to send a notification via alarm browser upon detection of a potential security violation.

The partial TOE self-protection requirements, FPT_RVM_EXP_TSF.1, and FPT_SEP_EXP_TSF.1 apply to the TOE, while the FPT_RVM_EXP_PFM.1, and FPT_SEP_EXP_PFM.1 apply to the IT Environment. Protected data transmission requirement, FTP_TRP_EXP_TSF.1 and FTP_TRP_EXP_PFM.1 and applies to initial user authentication and all communication between Dynamic Views GUI and its users (via web browser).

8.2.7 Explicitly Stated Requirements Rationale

CA_SDC_EXP.1, CA_ANL_EXP.1*, and CA_RCT_EXP.1 had to be explicitly stated because the CC Part 2 does not have any collection and analysis related SFRs that can describe the functions of the TOE.

FPT_SEP_EXP_*.* had to be explicitly stated because in the Basic Robustness Guide, it is recommended to explicitly state FPT_SEP_EXP_*.* in this manner. FPT_RVM_EXP_*.* and FTP_TRP_EXP_*.* had to be explicitly stated because they all provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. According to CCIMB RI#19, which states the following: “Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-9 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-9 Mapping of Functional Requirements to TOE Summary Specification

Item	Functional Requirement		Requirement is met by:	
			Security Function Ref. No	Rationale
1	FAU_GEN.1	Audit data generation	AU-1	Specifies the types of events to be audited by the NNM sever. Specifies the information to be recorded in an audit record.
2	FAU_SAR.1	Audit Review	AU-2	Provides the administrator with the ability to select audit records based on audit event type, time, login (username identity), and url login (host identity).
3	CA_SDC_EXP.1	System data collection	CA-1	Specifies that the TOE collects the specified system data.
4	CA_ANL_EXP.1-1	Analyzer analysis	CA-2	Specifies that the TOE performs sampling analysis on all system data received.
5	CA_ANL_EXP.1-2	Analyzer analysis	CA-3	Specifies that the System performs signature analysis on all system data received.
6	CA_RCT_EXP.1	Anaylzer react	CA-4	Specifies that alarms are sent to the alarm browser upon detection of a security violation.
7	FDP_ACC.1-1	User Data Protection	AC-1	Specifies the subjects and objects that access control is applied.
8	FDP_ACF.1-1	User Data Protection	AC-1	Specifies rules of access to the defined subjects and objects.
9	FIA_AFL.1	Identification and Authentication	I&A-3	Specifies the handling of authentication failures.
10	FIA_SOS.1	Identification and Authentication	I&A-2	Specifies password rules for use in authentication.
11	FIA_UID.2-1	Identification and Authentication	I&A-1	Specifies that users must be identified prior to being allowed access to TSF mediated actions. Counterpart restriction is in IT Environment.
12	FIA_UAU.2-1	Identification and Authentication	I&A-1	Specifies that users must be authenticated prior to being allowed access to TSF mediated actions. Counterpart restriction is in IT Environment.
13	FMT_MTD.1-1	Security management	SM-1	Specifies the restriction of security management to NNM administrators via Dynamic Views. Counterpart restriction is in IT Environment for “root” via CLIs.

Item	Functional Requirement		Requirement is met by:	
			Security Function Ref. No	Rationale
14	FMT_SMF.1	Security management	SM-1	Specifies the security management functions provided by the Dynamic Views and CLIs
15	FMT_SMR.1-1	Security management	SM-1	Defines roles of NNM administrator and NNM operator for restrictions to the Dynamic Views GUI. Counterpart restriction is in IT Environment for “root” and other users.
16	FPT_SEP_EXP_TSF.1	Partial Protection of the TSF	TSP-1	Ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Counterpart requirement is in IT Environment.
17	FPT_RVM_EXP_TSF.1	Partial Protection of the TSF	TSP-1	Ensures the TSF provides a domain that protects itself from untrusted users. Counterpart requirement is in IT Environment.
18	FTP_TRP_EXP_TSF.1	Partial Trusted path/channel	TPC-1	Ensures a trusted communications path for potential users to authenticate to the NNM Server Counterpart requirement is in IT Environment.

8.3.2 Assurance Measures

Table 6-2 lists the Assurance Measures and how they are satisfied. The mappings of assurance requirements to assurance measures are straightforward and self-explanatory. The assurance measures are defined by reference to the documents that will satisfy the corresponding assurance requirement. As a result, the justification that the assurance measure(s) will meet the assurance requirement(s) is implied.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.