Juniper your Net.

Security Target for Juniper Networks JUNOScope IP Service Manager 8.2R2

Version 1.1
July 2007

Prepared for:
Juniper Networks
1194 North Mathilda Avenue
Sunnyvale
California 94089
USA

Prepared by:
BT
Aldershot TE
Ordnance Road, Aldershot
Hampshire, GU11 2AH
UK

Contents

List of tables

1 ST Introduction

1.1 ST Identification

TOE Identification: Juniper Networks JUNOScope IP Service Manager 8.2R2

ST Identification: Security Target for Juniper Networks JUNOScope IP Service Manager 8.2R2

Assurance Level: Evaluation Assurance Level (EAL) 3, augmented with ALC_FLR.3.

ST Author: BT

Keywords: IP, Service Manager

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, plus applicable CCMB and UK national interpretations up to 1 September 2006. Where specific changes result from application of an interpretation or precedent this is noted in the security target.

1.2 ST Overview

The TOE is the JUNOScope IP Service Manager, also referred to as JUNOScope within this document, on Sun Solaris version 9/04 and 10.

JUNOScope provides tools for managing routers via a web based interface, giving a network operator access to the day-to-day tasks required to manage a network of routers, including monitoring, configuration management, inventory management, software management and administration.

The chapters of this Security Target are structured in accordance with the families in the [CC] ASE class, with the various rationales required by the ASE families collated in section 7.

1.3 CC Conformance

The TOE is Part 2 conformant, Part 3 conformant, and meets the requirements of EAL3 augmented with ALC_FLR.3.

1.4 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.
  - The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. For an example, see FMT_SMR.1 in this security target.
  - The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text*. For an example, see FAU_GEN.1 in this security target.

- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value]. For an example, see FIA_ATD.1 in this security target.
- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration sequence letter following the component identifier. For example, see FMT_MTD.1 in this security target.

- User privilege in accessing the TOE is based on the usergroup association. A usergroup can be configured with one of the four access levels available: administrator, read-write, read-only or nobody[1]. Users belonging to the administrator group have full access to all devices managed by the TOE, including the administrative tasks of TOE, e.g. creating a new user, and a new device. Read-only and read-write usergroups can be applied to one or more devices at a finer granular level. Users belonging to the nobody usergroup have no access to any device except the login to TOE. The term "user" refers to a user that belongs to any of the four usergroups mentioned above.

[1] Also referred to as "no one"

2 TOE Description

2.1 TOE Identification

The TOE is the JUNOScope IP Service Manager release 8.2R2 running on Sun Solaris version 9/04 and 10

2.2 TOE Type

The TOE is software to monitor and manage router operations centrally

2.3 Product Description

2.3.1 JUNOScope Service Manager

The JUNOScope software is an element management application that provides tools for managing IP services for the M-Series, T-Series and J-Series routing platforms.

JUNOScope element management tools include:

Looking Glass for viewing real-time device operational, diagnostic and troubleshooting information. This includes showing outstanding alarms on a router.;

Configuration Manager for archiving, importing, comparing, displaying and restoring the configuration files on devices in the network. The Configuration Manager also includes a Web-based Configuration Browser and a Configuration Editor for managing configuration file content. The device configuration files are referred to as “revisions” and are stored in the “Configs” repository as shown in Figure 1.

Inventory Management System for scanning software, license, and hardware inventory and activity, such as additions, deletions or changes of inventory on selected devices on the network. The Inventory Management System also allows viewing of predefined reports or generation of custom reports.

Software Management System for network-wide deployment and installation of JUNOS software images (bundles, packages, patches).

Monitoring logs for viewing the status of completed, scheduled or pending operations. An audit log allows viewing of the status of all authentication activities and privileged operations performed by authorized users.

Settings (administration) for modification of JUNOScope settings. JUNOScope administration tools allow:

- Definition of user IDs and passwords used to log in to a device;
- Definition of usergroup, its associated users and device access privilege;
- Definition of how to connect to devices and the authentication information used to log in;
- Connection of the JUNOScope software to devices in the network;
- Definition of a dynamic group of devices so JUNOScope tasks can operate on many devices at the same time;
- Application of labels to statically organize a large group of devices in the network so that JUNOScope operations, such as archive a configuration or inventory scan, can be performed;

- Setting the date, time and interval when a JUNOScope software operation is to occur on devices in the network;
- Setting up local accounts and template accounts so that local users and users with RADIUS accounts can log in to JUNOScope with appropriate permissions;
- Setting up an authentication policy for users with local accounts and remote RADIUS accounts to authenticate to JUNOScope;
- Setting up RADIUS authentication server host information so that users with RADIUS accounts can log in to JUNOScope with appropriate permissions;
- Setting up RADIUS accounting server host information so that authentication records and privileged operations can be audited;
- Import and export of all JUNOScope settings data to the local file system;
- Creation, editing, viewing and running saved operations, such as archive, restore and inventory scan.

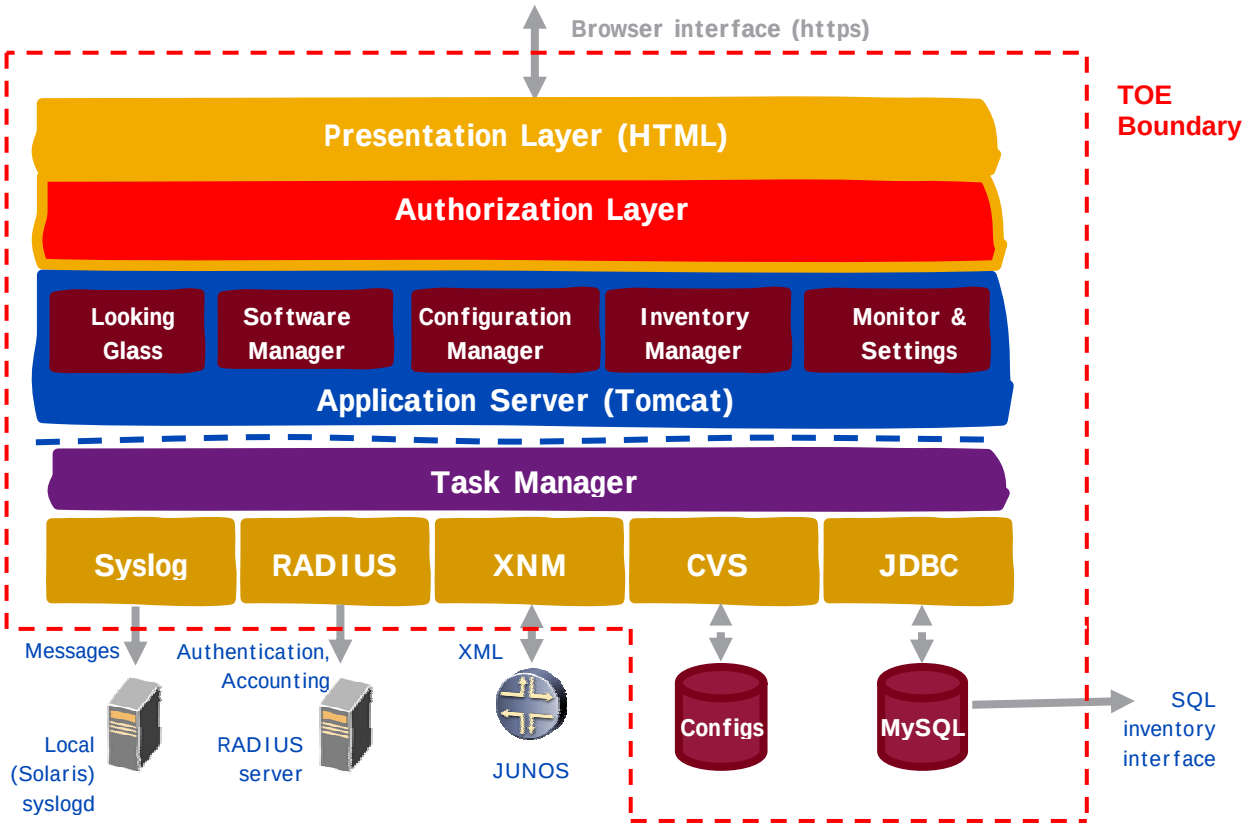

Figure 1 JUNOScope architecture

Access to JUNOScope software is controlled by username and password. The software enforces an authentication policy for each user. The JUNOScope administrator can edit the user authentication policy, including locking the account, specifying maximum login attempts, and setting an access window in which failed login attempts occur. JUNOScope tasks are controlled under a privilege mechanism. There are four levels of authorization for users/usergroups: nobody, read-only, read-write, and administrator.

The JUNOScope software provides audit logging of user authentication activity, and privileged operations that change information in the JUNOScope system and on the network to an internal audit log, the system log server, and an optional RADIUS accounting server if one is configured.

2.3.2 Network Connections

2.3.2.1 JUNOScope to Router connection

JUNOScope is a web server application that runs on a UNIX workstation. The JUNOScope software is a client of the JUNOScript server that runs on the router. The JUNOScope software connects to the JUNOScript server, which allows connection to routers via SSL (authentication to the routers for the query and upload of policies is transparent). The JUNOScope software uses the JUNOScript Application Programming Interface (API) to interact with the router, sending and receiving information in Extensible Markup Language (XML) for operations such as archiving, restoring and browsing a configuration file, and obtaining router status information.

The JUNOScope software connects to Juniper routing platforms running the current JUNOS software release and including at least two previous releases. Previous releases of JUNOS are outside the scope of this evaluation.

2.3.2.2 JUNOScope to Browser connection

The administrator connects to JUNOScope via a browser running on a client workstation.

The JUNOScope software provides security between the client and the server. SSL[2] is available between the JUNOScope server and the client web browser. All communication is encrypted between the client Web browser and the JUNOScope server.

Management access from a browser to JUNOScope first requires exchange of X.509 digital certificate to instigate an HTTPS connection, prior to a login request.

2.3.3 TOE Boundaries

The TOE is a software-only TOE installed on a Sun Solaris 9/04 or Solaris 10 platform, with Sun's Java Cryptography Extension installed, including JRE 1.4.2_13.

There is no security functionality provided by the browser the administrator uses to connect to JUNOScope. The only requirement of the browser is a functional aspect; namely that the browser has Javascript enabled.

2.3.3.1 Physical Boundary

The TOE operates within the physical boundary of the server Sun Server that runs the JUNOScope software.

The JUNOScope software has no physical interfaces, access being provided via the physical interfaces of the Sun Server (console[3] and network).

2.3.3.2 Logical Boundaries

The logical boundaries of the TOE are defined by the functions that can be carried out at the TOE external interfaces. These functions include identification and authentication for the administrative functions, management of the security configurations, audit and protection of the TOE itself. These can be carried out either via a console directly connected to the Sun Solaris platform or terminal session, or via a browser on a client workstation connected over the LAN. (The only requirement of the client browser for management is that Javascript is enabled.)

[2] SSL is outside the scope of the TOE as this is implemented by the underlying operating system.
[3] An interface to JUNOScope functionality from the Solaris console is only available during the installation and reconfiguration of JUNOScope

- Identification and Authentication

  The TOE requires users to provide unique identification and authentication data before any administrative access to JUNOScope is granted. The TOE provides four levels of authority for users, providing administrative flexibility. Administrators have the ability to define usergroups and their authority and they have complete control over the TOE. Authentication services can be handled either internally (fixed passwords) or through an authentication server in the IT environment, such as a RADIUS server (the external authentication server is considered outside the scope of the TOE).

- Security Management

  JUNOScope uses XML (JUNOScript) to interact with the router to view and modify configuration information. The ability to access the management functions is constrained according to the user's group association, and authentication to the router from JUNOScope is transparent to the user. The management functions available are described in Section 2.3.1 above.

- Audit

  JUNOScope auditable events are stored in the JUNOScope database and are subsequently sent to the system log server. Audit events cover authentication activity and privileged operations. Audit records include the date and time, event category, event type, username and client IP address. The audit log can be viewed only by an administrator. Search and sort facilities are provided.

The following interfaces are excluded from the evaluation:

- Inventory interface to MySQL

  OSS/BSS inventory integration via a published SQL API for JUNOScope Inventory datastore. This is a query interface directly into the database which stores the data collected from the network devices. This interface is excluded from the evaluation as it merely provides a method of querying the datastore, and does not provide a method to access any of the management functions. This interface is to be disabled in the evaluated configuration.

- XML-based Admin Settings import/export interface

  An interface is provided to import/export required JUNOScope database data from/to another JUNOScope server (encrypted or in clear text form). Such a farm configuration of multiple JUNOScope servers is not considered in the evaluated configuration.

3 TOE Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed.

The statement of TOE security environment defines the following:

- Threats that the TOE is designed to counter;
- Assumptions made on the operational environment and the method of use intended for the TOE;
- Organizational security policies with which the TOE is designed to comply.

3.1 Assumptions

The following usage assumptions are made about the intended environment of the TOE.

3.1.1 Physical Assumptions

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

3.1.2 Personnel Assumptions

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

3.1.3 IT Environment Assumptions

A.EAUTH External authentication services will be available via RADIUS.

A.THREAT The threat level in the environment where the TOE will be deployed is considered low.

A.ACCESS Access to data and processes on the Solaris platform underlying the TOE will be restricted to authorised personnel (i.e. JUNOScope Installer).

A.CRYPTO Management traffic will be protected using SSL.

3.2 Threats

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.

T.OPS An unauthorized process or application may gain access to the TOE security functions and data, inappropriately changing the configuration data for the TOE security functions.

T.DEVCONF An unauthorized user or process may gain access to change the configuration of a network device held on the TOE, inappropriately changing the archived configuration of the device.

T.CONFLOSS Failure of network components may result in loss of configuration data that cannot quickly be restored.

T.NOAUDIT	Unauthorized changes to the TOE configuration and other management information will not be detected.

3.3 Organizational Security Policies

There are no organizational security policies that the TOE must meet.

4 Security Objectives

4.1 Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

O.EADMIN	The TOE must provide services that allow effective management of its functions, TSF data and user data.
O.AMANAGE	The TOE management functions must be accessible only by authorized users.
O.ACCESS	The TOE must only allow authorized users and processes (applications) to access protected TOE functions and data.
O.ROLBAK	The TOE must enable rollback of router configurations to a known state.
O.AUDIT	Users must be accountable for their actions in administering the TOE.

4.2 IT Security Objectives for the Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OE.EAUTH	A RADIUS server must be available for external authentication services.
OE.BYPASS	The IT environment for JUNOScope must ensure that the TOE is not bypassed and will provide access control to TOE processes and files.
OE.BROWSE	The IT environment must secure the communication channel between the browser interface and the TOE.
OE.CRYPTO	SSL must be enabled for all management traffic.

4.3 Non-IT Security Objectives for the Environment

OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.ADMIN	Authorized users must follow all administrator guidance.
OE.EAL	The TOE must be certified to EAL3 with flaw remediation (ALC_FLR.3).

5 IT Security Requirements

5.1 Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. This section organises the SFRs by CC class. Table 5.1 identifies all SFRs implemented by the TOE (JUNOScope). Following the table the components are listed, showing completed operations.

Security Functional Class	Security Functional Components
Audit (FAU)	Security alarms (FAU_ARP.1)
	Audit data generation (FAU_GEN.1)
	User identity association (FAU_GEN.2)
	Potential violation analysis (FAU_SAA.1)
	Audit review (FAU_SAR.1)
	Protected audit trail storage (FAU_STG.1)
User data protection (FDP)	Basic rollback (FDP_ROL.1)
	Subset access control (FDP_ACC.1)
	Security attribute based access control (FDP_ACF.1)
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Verification of secrets (FIA_SOS.1)
	User authentication before any action (FIA_UAU.2)
	Multiple authentication mechanisms (FIA_UAU.5)
	User identification before any action (FIA_UID.2)
Security management (FMT)	Management of security attributes (FMT_MSA.1)
	Static attribute initialization (FMT_MSA.3)
	Management of TSF data (FMT_MTD.1a)
	Management of TSF data (FMT_MTD.1b)
	Management of security functions behaviour (FMT_MOF.1)
	Specification of Management Functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
TOE access (FTA)	TSF-initiated termination (FTA_SSL.3)
	TOE session establishment (FTA_TSE.1)

Table 5.1 Security Functional Components for JUNOScope

5.2 Security Functional Requirements for JUNOScope

5.2.1 Audit (FAU)

5.2.1.1 Security alarms (FAU_ARP.1)

FAU_ARP.1.1
The TSF shall take [the following action: lock the user account once the user authentication policy is violated[4]] upon detection of a potential security violation.

5.2.1.2 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1
The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [User login/logout;
d) Login attempt fails due to invalid username and/or password;
e) User session timeout;
f) Configuration is committed on a device;
g) Configuration is archived from a device;
h) Configuration is restored on a device;
i) User account created/changed (usergroup association)/deleted;
j) User password changed;
k) Device added/changed/deleted;
l) Label association changed;
m) Access method changed;
n) Authentication information changed;
o) Deletion of audit records;
p) RADIUS server configuration added/changed/deleted;
q) Software image is imported;
r) Software image is deleted;
s) Software image is downloaded/installed to a device;
t) Usergroup is created/changed (device access privilege)/deleted;
u) User account is locked/unlocked]

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,[no information]; and
c) [Client IP address where applicable].

5.2.1.3 User identity association (FAU_GEN.2)

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

5.2.1.4 Potential violation analysis (FAU_SAA.1)

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

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

[4] The authentication policy consists of a maximum login attempts bound by an access window. The account will remain locked until the administrator manually unlocks it.

a) Accumulation or combination of [number of failed login attempt audit records as specified by the Administrator] known to indicate a potential security violation;
b) [no other events].

5.2.1.5 Audit review (FAU_SAR.1)

FAU_SAR.1.1
The TSF shall provide [administrators] with the capability to read [all 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.

5.2.1.6 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1
The TSF shall protect the stored audit records from unauthorised deletion.

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

5.2.2 User data protection (FDP)

5.2.2.1 Basic rollback (FDP_ROL.1)

FDP_ROL.1.1
The TSF shall enforce [the access control SFP] to permit the rollback of the [committed configuration change] on the [router tables].

FDP_ROL.1.2
The TSF shall permit operations to be rolled back within the [configurations archived within the TOE].

5.2.2.2 Subset access control (FDP_ACC.1)

FDP_ACC.1.1
The TSF shall enforce [the access control SFP] on

- [subjects: users
- Objects: device revisions stored in “configs” database
- Operations: operations that view/create data in “configs” database].

5.2.2.3 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1
The TSF shall enforce [the access control SFP] to objects based on the following:

- [Subjects: users
- Subject security attributes: user permissions, user group membership
- Objects: device revisions stored in “configs” database
- Object security attributes: device the revision was created from].

Application Note:
The user permission is inherited from the predefined user groups (see FMT_SMR.1) as follows:

User group	**Permission level**
Administrator	superuser
Read-write user	read-write;
Read-only user	read-only
Nobody	none

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

- The user can display or compare the revisions of a device only if the user is a member of a user group to which the device is associated and the user permissions include “read-only” or “read-write”.
- The user can edit current device revision only if the user is a member of a user group to which the device is associated and the user has the “read-write” permission.
- The user can create a revision of a device only if the user is a member of a user group to which the device is associated and the user has the “read-write” permission.
- The user can perform a restore rollback function to restore a revision to a device only if they are a member of the administrator or read-write user groups.
- A member of the administrator user group has full permissions to access the revisions of any device managed by the JUNOScope software.

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

FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on ~~the~~ [non of the rules in FDP_ACF.1.2 matching].

5.2.3 Identification and authentication (FIA)

5.2.3.1 User attribute definition (FIA_ATD.1)

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

5.2.3.2 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [password minimum length of 6 characters with at least one change of character set (upper, lower, numeric, other)].

5.2.3.3 User authentication before any action (FIA_UAU.2)

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

5.2.3.4 User identification before any action (FIA_UID.2)

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

5.2.3.5 Multiple authentication mechanisms (FIA_UAU.5a)

FIA_UAU.5.1a
The TSF shall provide [internal fixed password mechanism and external server (RADIUS) mechanism] to support user authentication.

FIA_UAU.5.2a
The TSF shall authenticate any user's claimed identity according to the [authentication mechanism specified by an authorized user].

5.2.4 Management (FMT)

5.2.4.1 Application Note for FMT:

The "management access control SFP" is specified through the restrictions detailed in the management security functional requirements (i.e. those taken from the FMT class). These functions detail the manner in which different management functions are constrained to particular administrator roles.

5.2.4.2 Management of security attributes

FMT_MSA.1.1
The TSF shall enforce the [management access control SFP] to restrict the ability to [query, modify, delete] the security attributes [user permissions, user group membership and device/user group association] to [Administrators].

5.2.4.3 Static attribute initialization

FMT_MSA.3.1
The TSF shall enforce the [management access control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2
The TSF shall allow the [Administrators] to specify alternative initial values to override the default values when an object or information is created.

5.2.4.4 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1.1a
The TSF shall restrict the ability to [view, add, modify, delete] the [devices, access methods, groups, schedules, authentication information, user accounts (local authentication, user group authorization, authentication policy)] to [Administrators].

5.2.4.5 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1.1b
The TSF shall restrict the ability to [view, delete] the [audit trail] to [Administrators].

5.2.4.6 Management of security functions behaviour(FMT_MOF.1)

FMT_MOF.1.1
The TSF shall restrict the ability to [modify] the function [operation of the user session timeout function] to [TOE application installer].

5.2.4.7 Specification of Management Functions (FMT_SMF.1)

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

a) download/install software images;

b) configure devices;

c) configure groups;

d) configure schedules;

e) configure access methods;

f) configure users (local authentication, user group authorization, authentication policy) ;

g) configure authentication information;

h) provide the audit trail for review;

i) configure the interval of inactivity following which a user session is terminated].

5.2.4.8 Security roles (FMT_SMR.1)

FMT_SMR.1.1
The TSF shall maintain the roles [read-only user, read-write-user, administrator, nobody].

Application notes:
TOE application installer is a distinct role of TSF such that it does not have any users associated with this role. The TOE application installer creates the initial administrator account, specifies the server ports which TOE listens to, database password and other parameters during the installation. This installer role is not visible nor accessible to any other users.
The "nobody" group allows a user account to be created without access permission to any device.

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

5.2.5 TOE access (FTA)

5.2.5.1 TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1
The TSF shall terminate an interactive session after a [specified inactivity time period].

5.2.5.2 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1
The TSF shall be able to deny session establishment based on [IP address].

5.3 IT Environment Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the IT Environment. This section organizes the SFRs by CC class. Table 5.2 identifies all SFRs implemented by the IT Environment and indicates the ST operations performed on each requirement.

Security Functional Class	Security Functional Components
Identification and authentication (FIA)	Multiple authentication mechanisms (FIA_UAU.5)
Protection of the TSF	Reliable time stamps (FPT_STM.1)
Protection of the TSF	TSF Domain Separation (FPT_SEP.1)

Table 5.2 IT Environment Security Functional Components

5.3.1 Identification and authentication (FIA)

5.3.1.1 Multiple authentication mechanisms (FIA_UAU.5b)

FIA_UAU.5.1b

The TOE environment shall provide [an external server (RADIUS) mechanism] to support user authentication.

FIA_UAU.5.2b
The TOE environment shall authenticate any user's claimed identity according to the [RADIUS authentication mechanism as specified by an authorized user].

5.3.2 Protection of the TSF (FPT)

5.3.2.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1
The TOE environment shall be able to provide reliable time stamps for use by the TOE.

5.3.2.2 TSF Domain Separation (FPT_SEP.1)

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

FPT_SEP.1.2
The TOE environment shall enforce separation between the security domains of subjects in the TSC.

5.4 Minimum strength of function

The minimum strength of function required for the TOE is SOF-medium.

5.5 Security Assurance Requirements

The following table describes the TOE security assurance requirements drawn from Part 3 of the CC. The security assurance requirements represent EAL3, augmented with ALC_FLR.3.

Assurance Class	**Assurance Components**
Configuration Management (ACM)	*Authorisation controls (ACM_CAP.3)*
	TOE CM coverage (ACM_SCP.1)
Delivery and operation (ADO)	*Delivery procedures (ADO_DEL.1)*
	Installation, generation, and start-up procedures (ADO_IGS.1)
Development (ADV)	*Informal functional specification (ADV_FSP.1)*
	Security enforcing high-level design (ADV_HLD.2)
	Informal correspondence demonstration (ADV_RCR.1)
Guidance documents (AGD)	*Administrator guidance (AGD_ADM.1)*
	User guidance (AGD_USR.1)
Life cycle support (ALC)	*Identification of security measures (ALC_DVS.1)*
	Systematic flaw remediation (ALC_FLR.3)
Tests (ATE)	*Analysis of coverage (ATE_COV.2)*

	Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	*Examination of guidance (AVA_MSU.1)*
	Strength of TOE security function evaluation (AVA_SOF.1)
	Developer vulnerability analysis (AVA_VLA.1)

Table 5.3 TOE Assurance Components

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 User Data Protection

FDP_ACC.1 Subset access control and FDP_ACF.1 Security attribute based access control

Configuration Manager provides users with the capability to manage device revisions (archived router configurations),

Access to router configurations (revisions) is based upon the user group membership of the user. User group membership of the user determines the user's permission (superuser, read-write, read-only, none). Also, devices are associated with user groups (a single device may be added to the user group authorization of multiple user groups). A user only has access to revisions of a given device if the user and device are associated with the same user group. The type of access the user has to the device revision is further determined by the user group membership, in accordance with the pre-defined user groups (see application note to FDP_ACC.1):

Configuration Manager function	Superuser	Read-write	Read-only	None
Configuration Editor	✓	✓	-	-
Archive	✓	✓	-	-
Compare	✓	✓	✓	-[5]
Display	✓	✓	✓	-
Restore	✓	✓	-	-

FDP_ROL.1 Basic rollback

JUNOScope can be used to restore a device revision. This is used to store a configuration that can later be used for rollback, and when rollback is to be performed it allows specification of which saved configuration is to be used.

6.1.2 Identification and Authentication

FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes: user name, authentication data (password or an authentication server in the IT environment), and their privileges.

[5] Although the user will be able to see the links to display device configuration, they will not have permission to access any device information and so these links will always be empty. So effectively the users with "None" privilege will not be able to to display device configurations.

FIA_SOS.1 Verification of secrets

Locally stored authentication data for fixed password authentication is a case-sensitive, alphanumeric value. The password has a minimum length of 6 characters with at least one change of character set (upper, lower, numeric, other), and can be up to 40 ASCII characters in length (control characters are not recommended).[6]

FIA_UAU.2 User authentication before any action. FIA_UAU.5 Multiple authentication mechanisms and **FIA_UID.2 User identification before any action**

The TOE requires users to provide unique identification and authentication data (passwords) before any administrative access to the system is granted.

The JUNOScope software supports two methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS).

With local password authentication, you configure a password for each user allowed to log into JUNOScope. RADIUS is an authentication method for validating users whose user credentials are stored external to JUNOScope. RADIUS is a distributed client/server systems—the RADIUS client runs on JUNOScope, and the server runs on a remote network system.

If the identity specified is defined locally, the TOE will successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Alternatively, if the TOE is configured to work with a RADIUS server, the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless, no administrative actions are allowed until successful authentication as an authorized administrator.

Authentication data can be stored either locally or on a separate server. The separate server must support either the RADIUS protocol to be supported by the TOE.

6.1.3 Security Management

FMT_MSA.1 Management of Security Attributes and FMT_MSA.3 Static Attribute Initialization

The administrator can manage user group authorization; assigning devices and users to user groups. When a new instance of any of these objects is created, they are created with nil ‘values’, and the administrator has to enter an initial value for each security attribute of the object.

FMT_MTD.1 Management of TSF Data

The TOE provides the ability for the administrator to manage the configuration of the TOE (manage the TOE data) as follows:

1. View, add, modify or delete the configuration of:
    - devices
    - access methods
    - groups
    - schedules

[6] This function is the only function to which a strength of function claim is applicable.

- authentication information
- users (local authentication, user group authorization, authentication policy)

2. View and delete the audit trail.

FMT_MOF.1 Management of functions in TSF

The TOE restricts the management of the user session timeout function to TOE installer.

FMT_SMF.1 Management of Security Functions

The TOE provides the ability to manage the following security functions:

a) Configure devices;
b) Download/install software images
c) Configure groups
d) Configure schedules
e) Configure access methods
f) Configure users (local authentication, user group authorization, authentication policy);
g) Provide the audit trail for review;
h) Configure session termination following user inactivity.

FMT_SMR.1 Security Roles

The TOE has four pre-defined roles/usergroups. When a new user account is created, it must be assigned one of these roles.

a) Administrator: this role can perform all management functions on the TOE. A user with this role can manage user accounts (create, delete, modify), view and modify the TOE settings information, and full access to the routers via all functions available.
b) Read-write user: this role has full access to the routers via all functions available, but without any access to the TOE settings,
a) Read-only user: this role can read router configuration, but cannot modify any configuration, nor perform any operation which results in a change to the TOE or the routers being managed, e.g. software upgrade.
b) Nobody: this role is denied access to all TOE functions except login.

6.1.4 Audit

FAU_GEN.1 Audit data generation

JUNOScope creates and stores audit records for the following events:

a) Start-up and shutdown of the audit function;
b) User login/logout;
c) Login attempt fails due to invalid username and/or password;
d) User session timeout;
e) Configuration is committed on a device;
f) Configuration is archived from a device;
g) Configuration is restored on a device;
h) User account created/changed/deleted;
i) User password changed;
j) Device added/changed/deleted;
k) Label association changed;
l) Access method changed;

m) Authentication information changed;
n) Deletion of audit records;
o) RADIUS server configuration added/changed/deleted;
p) Software image is imported;
q) Software image is deleted;
r) Software image is downloaded/installed to a device
s) Usergroup is created/changed (device access privilege)/deleted;
t) User account is locked/unlocked

FAU_GEN.2 User identity association

JUNOScope will record within each audit record the following information:
a) Date and time of the event, type of event, subject (user) identity, and the outcome (success or failure) of the event; and
b) Client IP address where applicable.

FAU_SAR.1 Audit review

Administrator can review and sort all audit records via the audit log table. Administrator can analyze audit records by applying filters, such as event category, event type, last updated timestamp, and associated user.

FAU_SAA.1 Potential violation analysis and **FAU_ARP.1 Security alarms**

An audit record is generated each time a failed authentication attempt is made. If the maximum number of authentication attempts, as configured by the administrator, is reached within the time period specified by the administrator then the account is locked and an audit record generated identifying that the account has been locked.

FAU_STG.1 Protected audit trail storage

JUNOScope users with Administrator privilege can select audit log records for deletion. Such deletions will be audited locally, and the record will be written to the syslog server and remote RADIUS servers.

6.1.5 TOE access

FTA_SSL.3 TSF-initiated termination

A user session will be terminated by TOE once it has been idle for a period of time which exceeds the inactivity timeout configured.

FTA_TSE TOE session establishment

The TOE will restrict or deny client access from specific IP addresses or subnets.

The user session is established (between the browser client and TOE) using HTTPS, protected via SSL[7].

6.2 Assurance Measures

Table 6.1, below, identifies the deliverables that will meet the assurance requirements of Common Criteria EAL 3. The identified deliverables describe the approach taken to meet the assurance requirements, and meet all of the assurance requirements contained in this assurance package.

[7] SSL is outside the TOE, as it is implemented in the operating system.

Table 6.1 Assurance Measures

Assurance Class	Assurance Components	Assurance Measures (Juniper documentation)
Security target (ASE)	*All*	This security target meets all of the requirements within class ASE.
Configuration Management (ACM)	*Authorisation controls (ACM_CAP.3)*	Configuration Management Procedures for Juniper Delivery Procedures for Juniper Installation Guide for the Juniper Configuration Guide for the Juniper Release Notes for Juniper The Configuration Management Procedures describe the use of a configuration management system that meets the requirements of ACM_CAP.3. All documentation required by ACM_SCP.1 is held under configuration control. The Delivery procedures describe secure delivery process to preserve the integrity of the TOE, meeting the requirements of ADO_DEL.1 . The Common Criteria Guide, Installation Guide, Configuration Guide and Release Notes provide information on how to bring the delivered TOE into an operational state in accordance with ADO_IGS.1.
	TOE CM coverage (ACM_SCP.1)	
Delivery and operation (ADO)	*Delivery procedures (ADO_DEL.1)*	
	Installation, generation, and start-up procedures (ADO_IGS.1)	
Development (ADV)	*Informal functional specification (ADV_FSP.1)*	Functional Specification for JUNOScope This document describes the external interfaces to the TOE in a manner consistent with the requirements of ADV_FSP.1.
	Security enforcing high-level design (ADV_HLD.2)	High-level design for JUNOScope This document describes the TOE in terms of subsystems, and documents the interfaces between them.
	Informal correspondence demonstration (ADV_RCR.1)	Correspondence demonstration for JUNOScope A description of correspondence between the TOE summary specification and the high-level design is provided by means of cross-references in this document.
Guidance documents (AGD)	*Administrator guidance (AGD_ADM.1)*	Installation Guide for JUNOScope Configuration Guide for JUNOScope Command reference Guide for JUNOScope Release Notes for JUNOScope CC Evaluated Configuration Guide for JUNOScope These documents provide detailed guidance on the administration of the TOE in a secure manner. They also provide information on achieving the evaluated configuration.
	User guidance (AGD_USR.1)	

Assurance Class	Assurance Components	Assurance Measures (Juniper documentation)
Life cycle support (ALC)	*Identification of security measures (ALC_DVS.1)*	Development Security for Juniper. This document defines the procedures used to maintain the security of the development environment. These measures provide a combination of procedural, personnel and technical measures that safeguard the integrity and confidentiality of the TOE.
	Systematic flaw remediation	Configuration Management Procedures This document includes a description of the problem reporting procedure used to log, track and report flaws.
Tests (ATE)	*Analysis of coverage (ATE_COV.2)*	Testing plan and analysis for JUNOScope The test documentation describes how each external security functional interface is tested, and also how it is demonstrated that the subsystem interfaces are also operating correctly. The documentation describes the test environments used, the tests that are carried out, and the results that are expected and obtained. The TOE is made available to the evaluators for testing.
	Testing: high-level design (ATE_DPT.1)	
	Functional testing (ATE_FUN.1)	
	Independent testing – sample (ATE_IND.2)	
Vulnerability assessment (AVA)	*Strength of TOE security function evaluation (AVA_SOF.1)*	Strength of function analysis for JUNOScope The strength of function analysis provides an analysis of the password mechanism that demonstrates that the SOF claims are upheld.
	Examine of guidance (AVA_MSU.1)	The evidence provided for AGD_ADM.1 and ADO_IGS.1 will detail the guidance provided to the administrator for secure operation of the TOE.
	Developer vulnerability analysis (AVA_VLA.1)	Vulnerability analysis for JUNOScope Juniper carries out and documents an analysis of the TOE deliverables searching for weaknesses that might allow an attacker to violate the TOE security policy. This analysis is provided to the evaluators.

7 Rationale

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

- Security objectives
- Security functional requirements
- Security assurance requirements
- Dependencies
- Security functions
- Mutual support

7.1 Rationale for Security Objectives

This section shows that all assumptions and threats are countered by security objectives, and that each security objective addresses at least one assumption or threat.

7.1.1 Rationale for Security Objectives for the TOE

This section provides a mapping of TOE security objectives to those threats that the TOE is intended to mitigate, and to those assumptions that must be met.

	T.PRIVIL	T.OPS	T.DEVCONF	T.CONFLOSS	T.NOAUDIT	A.LOCATE	A.NOEVIL	A.EAUTH	A.THREAT	A.CRYPTO	A.ACCESS
O.EADMIN	✓		✓	✓							
O.AMANAGE	✓	✓	✓								
O.ACCESS	✓	✓	✓								
O.ROLBAK				✓							
O.AUDIT	✓	✓	✓		✓		✓				

Table 7.1 TOE Security Objectives Rationale

O.EADMIN This objective is to provide effective management tools that help prevent unauthorised access and exploitation of system privileges (T.PRIVIL) and help to recover from failures (T.CONFLOSS). Also this objective is also to provide effective management of user data and therefore helps to counter the threat T.DEVCONF.

O.AMANAGE The objective to limit access to management functions helps counter the threats of unauthorised access to privileged functions and data (T.PRIVIL, T.DEVCONF, T.OPS).

O.ACCESS This objective addresses the need to protect the TOE's operations and data. This helps counter the threats of unauthorised access (T.PRIVIL, T.DEVCONF, T.OPS).

O.ROLBAK The objective to restore previous configurations (user data) helps recover from loss of configuration data (T.CONFLOSS).

O.AUDIT This objective serves to discourage and detect inappropriate use of the TOE, and as such helps counter T.PRIVIL, T.OPS, T.NOAUDIT and T.DEVCONF. It also helps to support the assumption A.NOEVIL, by recording actions of users.

7.1.2 Rationale for Security Objectives for the Environment

This section provides a mapping of environment security objectives to those threats that the environment is expected to counter, and to those assumptions that must be met.

	T.PRIVIL	T.OPS	T.DEVCONF	T.CONFLOSS	T.NOAUDIT	A.LOCATE	A.NOEVIL	A.EAUTH	A.THREAT	A.CRYPTO	A.ACCESS
OE.EAUTH	✓							✓			
OE.BYPASS	✓	✓									✓
OE.BROWSE	✓		✓								
OE.CRYPTO			✓							✓	
OE.PHYSICAL						✓					
OE.ADMIN							✓				
OE.EAL									✓		

Table 7.2 Environment Security Objectives Rationale

OE.EAUTH The objective to have an authentication server in the TOE environment helps to mitigate the threat of unauthorised access (T.PRIVIL), and supports the assumption that such a server is present (A.EAUTH).

OE.BYPASS The objective that the underlying platform provides access control and protection to JUNOScope management functions and data helps to mitigate the threats that unauthorised users gain access to the TOE SFs and data (T.PRIVIL, T.OPS) and supports the assumption (A.ACCESS) that access is controlled to JUNOScope data and processes.

OE.BROWSE The objective to secure the communication channel between the browser interface and the TOE helps to mitigate the threat that unauthorised users gain access to the TOE SFs (T.PRIVIL) and that unauthorised changes could be made to the network configuration through interception of management traffic (T.DEVCONF).

OE.CRYPTO The objective to use SSL to protect management traffic supports the assumption that cryptography is used to protect management traffic (A.CRYPTO) a) preventing unauthorised users from gaining access to and being able to modify network device configuration data when it is transferred between the TOE and the network device, and b).helping to prevent interception of communication between the browser and the TOE (T.DEVCONF interception of configuration data between TOE and device).

OE.PHYSICAL The objective to provide physical protection for the TOE supports the assumption that the TOE will prevent unauthorised physical access (A.LOCATE).

OE.ADMIN The objective that users should follow administrator guidance supports the assumption that they will not be careless, wilfully negligent or hostile (A.NOEVIL).

OE.EAL This objective for assurance is appropriate to the level of threat assumed in A.THREAT.

7.2 Rationale for Security Requirements

7.2.1 Rationale for TOE security functional requirements

This section demonstrates that all security objectives for the TOE are met by security functional requirements for the TOE, and that each security functional requirement for the TOE addresses at least one security objective for the TOE.

	O.EADMIN	O.AMANAGE	O.ACCESS	O.ROLBAK	O.AUDIT
FAU_ARP.1	✓				✓
FAU_GEN.1	✓				✓
FAU_GEN.2					✓
FAU_SAA.1	✓				✓
FAU_SAR.1	✓	✓	✓		✓
FAU_STG.1		✓			✓
FDP_ROL.1				✓	
FDP_ACC.1	✓	✓	✓		
FDP_ACF.1	✓	✓	✓		
FIA_ATD.1		✓	✓		✓
FIA_SOS.1		✓	✓		
FIA_UAU.2		✓	✓		
FIA_UAU.5		✓	✓		
FIA_UID.2		✓	✓		
FMT_MSA.1	✓	✓	✓		
FMT_MSA.3	✓	✓	✓		
FMT_MTD.1a	✓	✓	✓		
FMT_MTD.1b	✓	✓	✓		
FMT_MOF.1	✓	✓	✓		
FMT_SMF.1	✓	✓	✓	✓	✓
FMT_SMR.1	✓	✓	✓	✓	✓

	O.EADMIN	O.AMANAGE	O.ACCESS	O.ROLBAK	O.AUDIT
FTA_SSL.3		✓			
FTA_TSE.1		✓			

Table 7.3 Security functional requirements rationale

FAU_ARP.1 This component takes action following detection of potential security violations, and therefore contributes to meeting O.EADMIN and O.AUDIT

FAU_GEN.1 This component outlines what events must be audited, and aids in meeting O.AUDIT, and provides the effective management of the audit function to help meet O.EADMIN .

FAU_GEN.2 This component required that each audit event be associated with a user, and aids in meeting O.AUDIT.

FAU_SAA.1 This component helps to detect potential security violations, and aids in meeting O.AUDIT and provides the effective management of the alarm function to help meet O.EADMIN.

FAU_SAR.1 This component requires that the audit trail can be read, and aids in meeting O.AUDIT, and ensures the SF to read the audit trail is only accessible by authorised users, helping to meet O.EADMIN, O.AMANAGE and O.ACCESS.

FAU_STG.1 This components ensures that audit records are not deleted in an unauthorised manner (O.AMANAGE) and users remain accountable for their actions (O.AUDIT).

FDP_ROL.1 This component allows the function to provide router configurations to be managed and restored (rollback), and aids in meeting O.ROLBAK.

FDP_ACC.1 This component specifies the security attributes on which the policy to control access to device revisions is based and therefore helps in meeting O.EADMIN, O.AMANAGE and O.ACCESS.

FDP_ACF.1 This component specifies the rules controlling access to the device revisions and therefore helps in meeting O.EADMIN, O.AMANAGE and O.ACCESS.

FIA_ATD.1 This component exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. The component aids in meeting O.AMANAGE, O.ACCESS and O.AUDIT.

FIA_SOS.1 This component specifies metrics for authentication, and aids in meeting objectives to restrict access; O.AMANAGE and O.ACCESS.

FIA_UAU.2 This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access; O.AMANAGE and O.ACCESS.

FIA_UAU.5a This component ensures multiple authentication mechanisms are provided to authenticate users to the TOE. As such it aids in meeting objectives to restrict access; O.AMANAGE and O.ACCESS.

FIA_UID.2 This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access; O.AMANAGE and O.ACCESS.

FMT_MSA.1 This component restricts the ability to modify security attributes that enforce the access control SFP and as such aids in meeting O.AMANAGE and O.ACCESS, and provides effective management of the related TSF data, helping to meet O.EADMIN.

FMT_MSA.3 This component restricts the ability to modify the initial values of the security attributes that enforce the access control SFP and as such aids in meeting O.AMANAGE and O.ACCESS, and provides effective management of the related TSF data, helping to meet O.EADMIN.

FMT_MTD.1a This component restricts the ability to modify configuration details, and as such aids in meeting O.AMANAGE and O.ACCESS, and provides effective management of the related TSF data, helping to meet O.EADMIN.

FMT_MTD.1b This component restricts the ability to control the audit trail, and as such aids in meeting O.AMANAGE and O.ACCESS, and provides effective management of the related TSF data, helping to meet O.EADMIN.

FMT_MOF.1 This component relates to control of the user session timeout function, and as such aids in meeting O.AMANAGE, O.ACCESS and O.EADMIN.

FMT_SMF.1 This component lists the security management functions that must be controlled. As such it aids in meeting O.EADMIN, O.AMANAGE, O.ACCESS, O.ROLBAK and O.AUDIT.

FMT_SMR.1 Each of the components in the FMT class listed above relies on this component. It defines the roles on which access decisions are based. As such it aids in meeting O.EADMIN, O.AMANAGE, O.ACCESS, O.ROLBAK and O.AUDIT.

FTA_SSL.3 This component limits the period of inactivity before a user session is terminated, and hence reduces the chance of unauthorised access. As such it aids in meeting O.AMANAGE.

FTA_TSE.1 This component limits the range of locations from which a user session can be established, and hence reduces the chance of unauthorised access. As such it aids in meeting O.AMANAGE.

7.2.2 Rationale for TOE Environment Security Functional Requirements

Multiple authentication mechanisms FIA_UAU.5b

This component was chosen to ensure that multiple authentication mechanisms are used appropriately in all attempts to authenticate to the TOE. This component traces back to and aids in meeting the following objective: OE.EAUTH. Its presence under TOE environment security functional requirements is to address authentication using an external authentication server.

Reliable time stamps FPT_STM.1

This component was included to ensure the underlying platform of the TOE provides a reliable time stamps for audit records and aids in meeting O.AUDIT.

TSF Domain Separation FPT_SEP.1

This component was included to ensure the underlying platform of the TOE provides domain separation for TOE and non-TOE processes, helping to meet OE.BYPASS.

OE.CRYPTO/OE.BROWSE

This objective was specified to ensure that all management traffic (both between the browser and the TOE and between the TOE and the managed network device) is protected from network sniffing through encryption of the packets in accordance with the SSL standard. Any algorithms and key sizes specified in the SSL standard (as defined in www.ietf.org/rfc/rfc2246.txt. SSLv3 corresponds to TLSv1) are acceptable to meet this requirement.

7.2.3 Rationale for Security Assurance Requirements (SAR)

The ST is requires EAL3 assurance, augmented with ALC_FLR.3.

EAL3 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs.

Systematic flaw remediation was added to demonstrate that the developer has effective procedures in place to address any security issues identified in the product, ensuring the customers are notified how the issues are addressed.

The chosen assurance level as supported by OE.EAL is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

SOF-medium is defined in [CC] Part 1 as “provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential”. This claim relates to the resistance of TSF’s Identification and Authentication security function with authentication data meeting the requirements of FIA_SOS.1. The authentication interface is one which is generally subject to increased attack due to its probabilistic/permutational nature, so a higher level of resistance in this interface is appropriate. This is consistent with the objectives for the TOE, specifically O.AMANAGE that states management functions must be accessible by authorized users, thereby identifying the identification and authentication mechanism to be a key barrier for the protection of the TOE against unauthorized use.

7.2.4 Dependencies Rationale

All functional and assurance requirements dependencies indicated in [CC] have been satisfied. Dependencies on FIA_UAU.1 and FIA_UID.1 have been satisfied through inclusion of the hierarchical components FIA_UAU.2 and FIA_UID.2, respectively.

7.3 TOE Summary Specification Rationale

This section illustrates that the security functions as described in the TOE Summary Specification (Section 6) are necessary and sufficient to implement the SFRs and SARs.

	User data protection	Identification and authentication	Security management	Audit	TOE Access
FAU_ARP.1				✓	
FAU_GEN.1				✓	
FAU_GEN.2				✓	
FAU_SAA.1				✓	
FAU_SAR.1				✓	
FAU_STG.1				✓	
FDP_ROL.1	✓				
FDP_ACC.1	✓				
FDP_ACF.1	✓				
FIA_ATD.1		✓			
FIA_SOS.1		✓			
FIA_UAU.2		✓			
FIA_UAU.5a		✓			
FIA_UID.2		✓			
FMT_MSA.1			✓		
FMT_MSA.3			✓		
FMT_MTD.1a		✓	✓		✓
FMT_MTD.1b			✓		
FMT_MOF.1			✓		✓
FMT_SMF.1		✓	✓	✓	✓
FMT_SMR.1		✓	✓		
FTA_SSL.3					✓
FTA_TSE.1					✓

Table 7.4 Security functions rationale

The **User Data Protection function** allows the user to manage the device revisions (FDP_ACC.1, FDP_ACF.1), including initiating rollback of the device configuration (FDP_ROL.1)

The **Identification and Authentication Function** requires that users be identified (FIA_UID.2, FIA_ATD.1) and authenticated (FIA_UAU.2, FIA_ATD.1) before being granted access to any other TOE functions. The authentication data must be at least 6 characters long and be comprised of a minimum of two character sets (FIA_SOS.1).

Authentication can be achieved through either local password or external RADIUS authentication (FIA_UAU.5a).

The function is controlled by administrators (FMT_SMF.1, FMT_SMR.1, FMT_MTD.1a), who may modify user attributes, the authentication method and manage the number of permitted authentication attempts (FMT_MTD.1a).

The claimed strength of function for the password mechanism is SOF-Medium. This is consistent with the overall claim for the TOE of SOF-Medium.

The **Security Management Function** permits the users to perform the following actions (view/modify according to their permissions (FMT_SMR.1)):

- Manage access methods to connect between client and server (FMT_SMF.1, FMT_MTD.1a);
- Manage groups (FMT_SMF.1, FMT_MTD.1a);
- Manage schedules (FMT_SMF.1, FMT_MTD.1a);
- Manage authentication information (FMT_SMF.1, FMT_MTD.1a);
- Manage users (local authentication, user group authorization, authentication policy);
- Manage devices (as represented in the TOE) (FMT_SMF.1, FMT_MTD.1a);
- Download/install software images (FMT_SMF.1);

The TOE installer can perform the following security management action:

- Modify the user session timeout function (FMT_MOF.1, FMT_SMF.1).

The administrator can also manage the following security attributes, creating instances of them in the TOE and specifying alternative initial values for the attributes: user permissions, user group membership and device. user group association (FMT_MSA.1, FMT_MSA.3).

The **Audit Function** provides a reliable audit trail of network connections and other events (FAU_GEN.1) that can be viewed and deleted only by an administrator (FMT_SMF.1, FMT_MTD.1b, FAU_SAR.1, FAU_STG.1). For all events the Audit Function will record the:

- Date and time of the event (FAU_GEN.1), using the date and time information provided by the IT environment (underlying Solaris platform);
- The identity of the user (FAU_GEN.2);
- Type of event or service (FAU_GEN.1);
- Success or failure of the event (FAU_GEN.1).

The TOE can be configured to monitor sequences of events (FAU_SAA.1) and take action when they occur (FAU_ARP.1).

The **TOE Access Function** provides for TSF initiated session termination (FTA_SSL.3, FMT_SMF.1, FMT_MTD.1a), and for restrictions on session establishment (FTA_TSE.1, FMT_MOF.1).

7.4 IT security functions mutually supportive

The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 7.3.), as each of the IT security functions can be mapped to one or more SFRs, as demonstrated in Table 7.4.

8 Acronyms

ACM	Access Control Management
AGD	Administrator Guidance Document
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CC	Common Criteria
CM	Control Management
CVS	Concurrent Versions System
EAL	Evaluation Assurance Level
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
IP	Internet Protocol
JDBC	Java Database Connectivity
OSS/BSS	Operation Support Systems/Business Support Systems
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
SF	Security Functions
SFR	Security Functional Requirements
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control
XML	Extensible Markup Language
XNM	XML-based Network Management