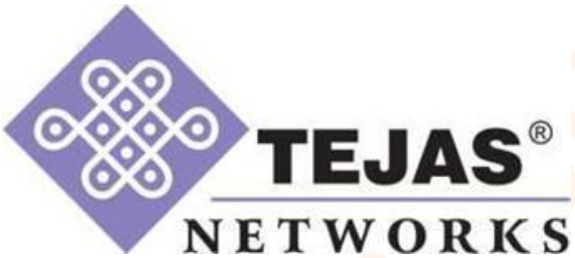


Security Target
Of
TJ5500 NMS (Network Management System)
&
TJ5100 EMS (Element Management System)
Version 8.1

TPN: 400-DOC000140-E

"This is a ***Controlled Document***". No other document should be referred unless and until Tejas Networks replaces this document with the latest version. Only documents with controlled copy stamped should be used.

Template ID: D – GD;Ver 1.00

Revision History:

Revision	Date	Author	Reason	Reviewed By	Approved By
1.0	20/10/2018	Divyesh Kumar	Initial draft	Mathan	Kannan
1.1	15/03/2019	Divyesh Kumar	Physical boundary diagram and EMS Audit Event table updated.	Mathan	Kannan
1.2	02/04/2019	Divyesh Kumar	Physical boundary diagram and EMS Audit Event table updated.	Mathan	Kannan
1.3	05/06/2019	Divyesh Kumar	ST updated as per the OR-dt050519	Mathan	Kannan
1.4	29/06/2019	Divyesh Kumar and Mathan	ST updated as per the OR-dt260619	Mathan	Kannan
1.5	26/03/2021	Mathan	ST updated with S/W version	Mathan	Kannan
1.6	02/07/2021	Divyesh	Modified SFR	Mathan	Prasad
1.7	28/07/2021	Divyesh	Modified SFR	Mathan	Prasad
1.8	26/08/2021	Divyesh	TOE summary modified	Mathan	Prasad
1.9	04/04/2022	Divyesh	Review comment implemented	Mathan	Prasad

Table of Contents

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title : Security Target of TJ5500 NMS (Network Management System) and TJ5100 EMS (Element Management System) version 8.1.

ST Revision : 1.9

ST Publication Date : 04/04/2022

1.2 TOE Reference

TOE Reference: TJ5500 NMS (Network Management System) and TJ5100 EMS (Element Management System)

Product	Evaluated TOE (S/W) Version
TJ5500	8.1
TJ5100	8.1
TJ5500 Client	8.1

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1: ST Organization and Section Descriptions

1.4 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
MD5	Message Digest 5
NTP	Network Time Protocol
OSP	Organizational Security Policy
PKCS	Public-Key Cryptography Standards
RFC	Request for Comment
RSA	Rivest Shamir Adelman
SA	Security Association
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
SYSLOG	System Log
SFTP	Secure file transfer protocol
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Function
VPN	Virtual Private Network
TejOS	Tejas Operating System
POTP	Packet optical transport platform
SRRD	System requirement document
PTN	Packet transport network
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
SMTP	Simple Mail Transfer Protocol
POP3	Post Office Protocol 3
IMAP4	Internet Message Access Protocol 4
FCAPS	Fault, Configuration, Accounting, Performance and Security Management.
VPN	Virtual Private Network
OS	Operating System
NOC	Network Operation Center
CORBA	Common Object Request Broker Architecture
OSS	Operation Support System

Table 2: Acronyms Used in Security Target

1.5 Conventions

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., (1), (2), (3)).

1.6 TOE Overview

TOE Type: Network Management System (TJ5500) and Element Management System (TJ5100).

TOE components providing control and monitoring functions for NE components that provide packet/optical transport services. These systems are intended for use in SP (Service Provider) environments.

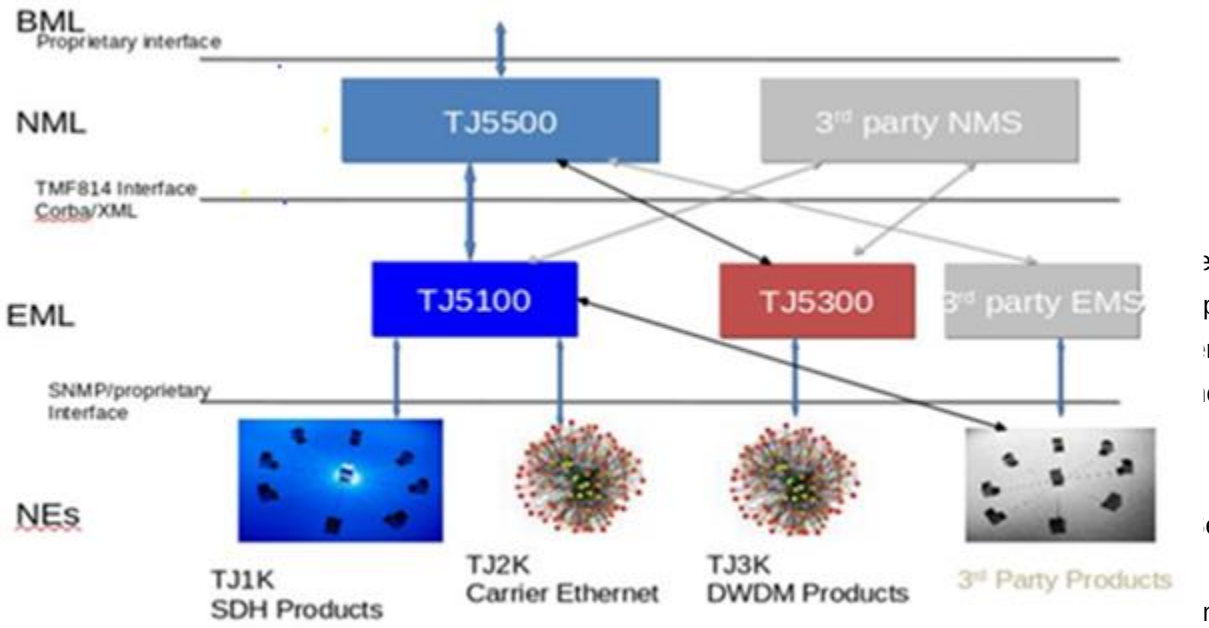
TJ5500 is referred as NMS and TJ5100 is referred as EMS. TJ5500 supports TJ5100 through the TMF 814 Interface. Each EMS instance has a unique EMS name.

TJ5500

TJ5500 is a Network Management System which offers single window operation into the network for Fault, Configuration and Security management for carrier networks. The TJ5500 offers full FCAPS functionality support across the various Tejas product portfolios – SDH (TJ1000 Series), Carrier Ethernet (TJ2000 Series), DWDM (TJ3000) series and iPASOLINK 250/650.

The TJ5500 is designed keeping in mind that service provider networks are heterogeneous in terms of equipment vendors, technology and manageability domains. With the unique "Map assisted walk-through" method of circuit provisioning, The TJ5500 enables the network operator to create circuits spanning multiple EMSs. TJ5500 is a scalable product that can manage very large networks comprising of tens of thousands of NEs. An advanced, intuitive user interface enables the NoC teams to optimize operational cost through faster and more efficient operations.

The TJ5500 concept is based on layered architecture in accordance with the TMF 814 standard for compliant layer architecture. Separate layers make up the management structure. The lowest level, the Network Element Layer (NEL), constitute the embedded agent software of the NEs. The second layer, the Element Management Layer (EML), controls many individual NEs. While the third layer, the Network Management Layer (NML), controls the main network management functions. This architecture is illustrated in following figure.



ements
persed
rs with
etwork
ecurity
Circuit
n each
NE.

TMF 814 standard based CORBA interface is provided by EMS to communicate with Network Management Systems (NMS) and Operation Support Systems (OSS).
EMS server communicates to Network Elements using with SNMP or HTTP/HTTPS protocol. Alarms from NE are received as SNMP traps. EMS clients (Java Swing based) connect to EMS server using CORBA interfaces. Alarms and configuration change notifications are sent from EMS server to client using one way CORBA notification.

EMS client can be launched from web browsers using javaws/jnlp mechanism. User access the TJ5100 functions via the TJ5500 GUI. TJ5500 automatically invokes TJ5100 functionality to perform user-requested operations involving NEs.

TJ5100 user accounts are maintained separately from TJ5500 user accounts. However, for this evaluation, all user accounts are managed in TJ5500 and accounts are automatically uploaded from TJ5500 to TJ5100. Each user is associated with one of the profile to limit the functions that may be performed.
Security and Configuration related operations performed by users are audited, and the audit records can only be viewed by authorized users. Configuration information and audit records are stored in MySQL database.

TOE supports the following functionalities:

- Alarms - Describes filtering and managing alarms
- Topology - Manages partitions, EMS and nodes
- Circuit Management - Creates, discovers and manages circuits
- Security - Manages users and their profiles
- Administration- Manages audit logs, fail-over and schedule recurring/non-recurring operations

The TOE Provides secure remote access to internal network resources, such as:

- Web-based traffic, including Web pages and Web-based applications.
- Java applets, including Web applications that use java applets.
- File traffic, including file servers and directories
- Client/Server applications
- Email Clients based on SMTP protocols.
- All network traffic.

All requests from NMS Client to NMS server are encrypted using TLSv1.2, TLSv1.3 / HTTPS 256-bit encryption. All non-encrypted requests (e.g. HTTP) are redirected to HTTPS, which ensures the connection is encrypted. Each request is subject to administratively defined access control and authorization policies, such as dual-factor or client-side digital certificate authentication, before the request is forwarded to an internal resource.

SSH terminal emulation sessions is used to access the Linux server for Installation and commissioning of TOE, to Perform SFTP transfer of reports and backups to remote machines and to perform operations on the DB server in clustering mode.

All Security and Configuration related Operations performed by users are audited, and the audit records can only be viewed by authorized users.

Features under evaluation

- Manages users and their profiles
- User Identification and Authentication
- Audit log generation and verification
- User Session Management

- Client IP Configuration
- Password complexity and usage settings configuration
- Cryptographic Support
- Trusted Path/Channels
- Topology: Dashboard, Topological View, Manage TL, Manage EMS, and Manage Nodes
- Circuit Management.

Features not under evaluation

- Alarms/Fault: Filtering and managing alarms
- Configuration: Ethernet, GPON, Ports and Manage Customers.
- Planning: All Planning features are not under evaluation.

1.7 TOE Description

The TOE is an integrated management application offering single window operation for end-to-end network management. It supports provisioning, operations & management of Packet Transport Networks, DWDM, SDH/SONET, GPON and OTN based services. This provide a unified management solution to manage multi-technology networks. The management functionality provides multiple roles in order to enable multiple levels of access for users. The managed appliances may be divided into different groups within the management platforms, with access to groups restricted on a per-user basis.

The TOE consists of:

- One instance of the TJ5500 server component executing on RHEL server 8.2 or higher version (64-bit).
- One instance of the TJ5100 server component executing on the same server as the TJ5500 server.
- One or more instances of the TJ5500 client-side application. The instances may be installed on Windows 7/ Windows 10/ Red Hat Enterprise Linux 8.2 or higher version workstations.

1.7.1 Physical Boundary

Figure 2 and 3 illustrate the physical scope and the physical boundary of the overall solution and tie together all of the components of the TOE and the constituents of the operational environment of the TOE. The TOE is a software only product. The TOE has two logical interfaces: End User and Admin interface. The Admin and End User interface to the TOE includes a Web-Based user interface.

The TOE includes a Tomcat Web Server developed by the Apache Software Foundation, which is being used to provide main interface for both users and administrators of the TOE. The web server provides users interface to perform operations via HTTPS.

The web server provides administrators an interface to administrate the TOE using a web browser. The web server component is included as part of the TOE.

The TOE boundary is shown below:

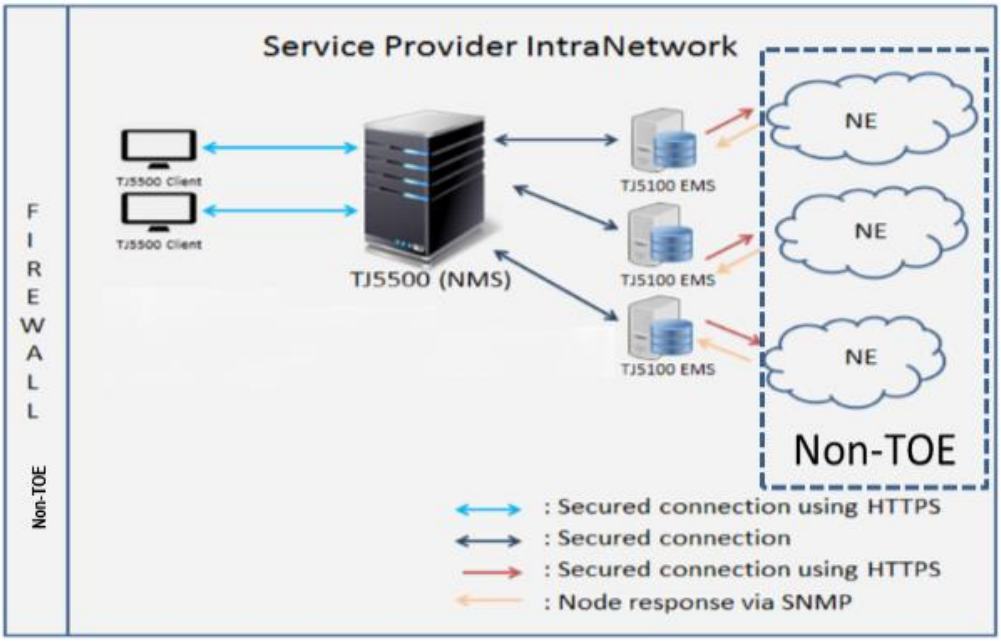


Figure 2: TOE Physical boundary

All communication paths shown in above diagram are secure.

- The entire Service provider Intra Network is firewall protected.
- TJ5500 Clients and TJ5500 Server communicate via HTTPS Secure channel.
- TJ5500 and TJ5100 servers communicate via secure channel.
- TJ5100 server and NE communicate via HTTPS/SNMP.

The physical boundary of the TOE is depicted in the following diagram (shaded items are within the TOE boundary).

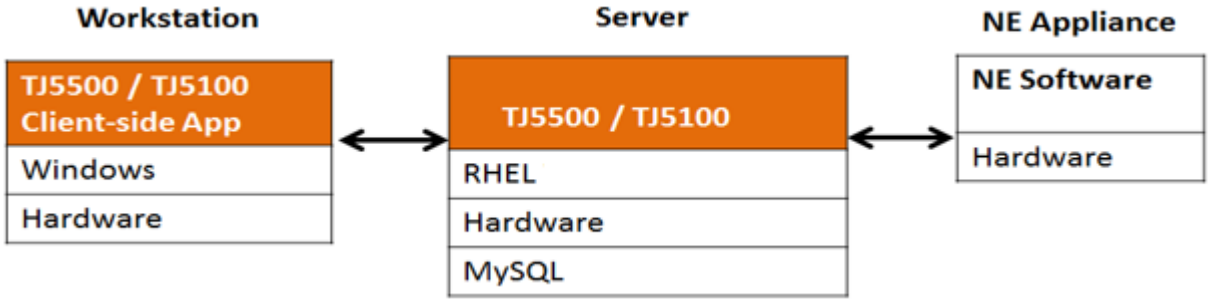


Figure 3: TOE Boundary

The following tables show hardware and software components included in TOE and Non-TOE:

S/N	Part Number	VERSION / MODEL NUMBER
1	400-SW0000106-S	TJ5500 Version 8.1
2	400-SW0000106-S	TJ5100 Version 8.1
3	400-DOC000118-E	TJ5500 operation manual (User interface guide)
4	400-DOC000117-E	TJ5500 Installation and Commissioning Guide
5	400-DOC000116-E	TJ5100 operation manual (User interface guide)
6	400-DOC000115-E	TJ5100 Installation and Commissioning Guide

Table 3: TOE Delivery details

Final software package (TOE) will be burn in CD and it will be handover to Final assembly (packing) team. The logistic team will send the TOE to the corresponding customer.

Non-TOE Description

One or more instances of NE software executing on supported appliances which is Non-TOE. The software is pre-installed on appliances by Tejas. The modular appliances may be populated via any supported combination of modules/cards.

Server Requirements:

The table below lists the hardware and the software requirements of the server where TJ5500 has to be installed.

Non-TOE Components of TJ5500 & TJ5100	Version / Model No.	
Hardware	Processor	64-bit Dual processor Quad Core Intel 3.0 GHz or higher (8 cores in total with HT Enabled)
	Memory	• 32 GB Physical Memory (RAM) • 2*600 GB Hard Disk Drive in RAID1
Software	Operating System	RHEL server release 8.2 / later version (ootpa) (64-bit)
	Messaging/JMS	Apache Active MQ - 5.13.0 / later version
	Platform	Java Development Kit 8, Update 171 (JDK 8u171)
	Database	MySQL Version 5.7.22 / later version(64-bit)

Table 4: Configuration for the Non-TOE

Client System Requirements:

The table below lists the hardware and the software requirements of the client system for accessing the TJ5500 application.

Non-TOE Components of TJ5500 Client	Version / Model No.	
Hardware	Processor	Intel/AMD Quad core (3GHz)
	Memory	• 8 GB Physical Memory (RAM) • 40 GB Hard Disk Drive
Software	Client Configuration	19 inch TFT monitor supporting 1280x1024 or 1366 x 768 or 1920 × 1080 resolution with "true color" graphics card of same resolution.
	Operating System	Windows 10 /Red Hat Enterprise Linux 8.3
	Platform	Java JRE 8 Update 171

Non-TOE Components	Version / Model No.
Client	Firefox browser running on Windows 10 OS
RADIUS or TACACS+ AAA Server	This includes any authentication server that can be leveraged for remote user authentication.
Hardware (NE- Network element)	• TJ1400 POTP / PTN • TJ1600 POTP / PTN • TJ1270

Table 5: Non-TOE Components

1.7.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Security Audit	TJ5500 / TJ5100 generate audit records for security events. The User with associated administrator profile or profile which has permission to view audit log have ability to view audit logs.
Cryptographic Operations	TJ5500 / TJ5100 supports secure communications between users and the TOE and between TOE components. This encrypted traffic prevents modification and disclosure of user information.
User Data Protection	TJ5500 / TJ5100 provide an information flow security policy. The security policy limits traffic to specified ports.
Identification and Authentication	All users are required to perform identification and authentication before any information flows are permitted. Additionally, administrators must be authenticated before performing any administrative functions
Security Management	TJ5500 / TJ5100 provide a wide range of security management functions. Administrators can configure the TOE, the information flow policy and audit and user manager manages users and security policies.

TOE Access	TJ5500 / TJ5100 provide time initiated termination of any interactive session open for more than configured duration. NMS protects all concurrent sessions from compromise by enforcing a timeout. When a session becomes idle for 30 minutes or reaches a maximum configured lifetime of 120 minutes, the session gets time out and entry gets clean up from session table. TJ5500 / TJ5100 provides whitelisting of Client IP address
Protection of the TSF	TJ5500 / TJ5100 provide a timestamp for its own use. The timestamp is generated from the clock provided by the OS.

Table 6: Logical Boundary Descriptions

1.8 TOE Configuration details

The following configuration restrictions apply to the evaluated configuration

- The default profiles in NMS are not modified and the associations between those Profiles and pre-defined User Groups are not changed. Additional Profiles and User Groups may be created to provide customized Roles.
- User Accounts are defined in NMS and can be synced between NMS and EMS.
- All control and monitoring of NEs after they have been added to NMS is performed via NMS only.
- The Inactivity Timeout for all User Accounts is configured as a numeric value (not “Unlimited”) to force inactive sessions to be locked or terminated.
- Password complexity and usage settings are configurable.
    - Default Minimum Password Length: 8
    - Default Maximum Password Length: 110
    - Default no of allowed Special Character: 1
    - Default no of Numeric Number: 1
    - Default no of Upper case letter: 1
    - Default no of Lower case letter: 1
    - Default Password expiration: 45 days
    - Default Max Unsuccessful Login Attempts: 5
    - Login Reactivation: 5 minutes
    - Default Inactivity Timeout: 30 minutes
    - Strong Password Enforcement: Enable

- The Installation and Commissioning Guide provides information on installing the product and to initially configuring it to the point of verifying its proper operation in the network.

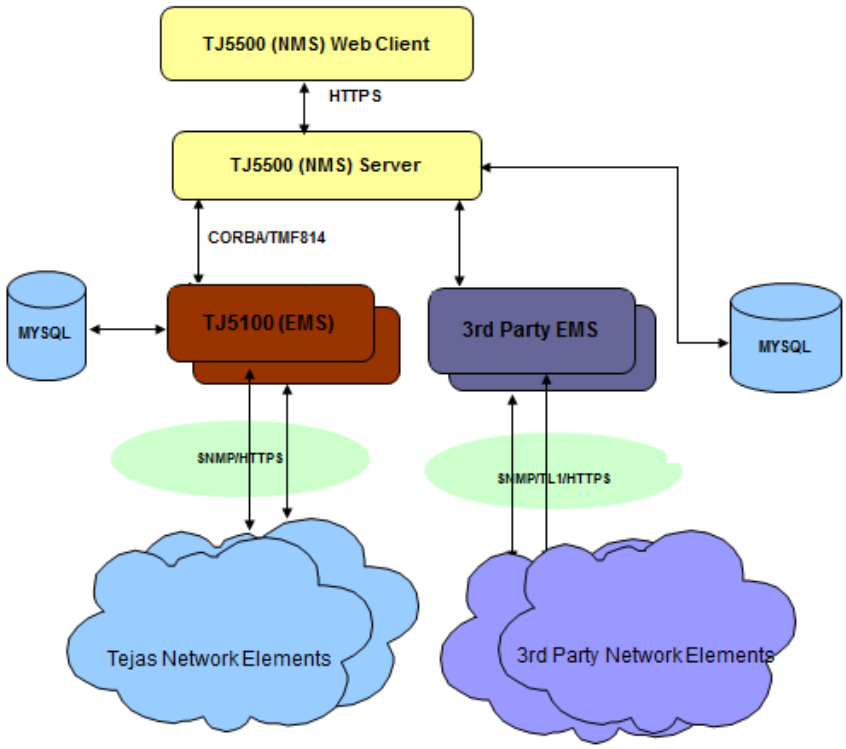
1.9 TOE Software component details

Software version

- TJ5500 Version 8.1
- TJ5100 Version 8.1
- TJ5500 Client 8.1

1.10 TOE Application Network Diagram

Following is the TOE application network diagram.



TOE	Non-TOE
TJ5500 (NMS) web client TJ5500 NMS Server TJ5100 (EMS)	➢ 3rd party EMS ➢ 3rd Party Network Elements ➢ Tejas Network Elements ➢ 3rd Party Software • MySQL

Figure 4: TOE application network diagram

2. Conformance Claims

2.1 CC Conformance Claim

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.

2.2 PP Claim

The TOE and ST do not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE and ST are claim conformance to the EAL2 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 5, April 2017.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3. Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not generated and reviewed, thus allowing an attacker to modify the behavior of TSF data without being detected.
T.COMINT	An unauthorized person may attempt to compromise the integrity of TOE data by bypassing a security mechanism.
T.LOSSOF	An unauthorized person may attempt to remove or destroy data from the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.OLDINF	An unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between a remotely located authorized administrator and the TOE.
T.REPLAY	An unauthorized person may replay valid identification and authentication data obtained while monitoring the TOE's network interface to access functions provided by the TOE.
T.USAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

Table 7 : Threats Addressed by the TOE

The IT Environment does not explicitly address any threats.

3.2 Organizational Security Policies

The Organizational Security Policies identified in the following table are addressed by the TOE and the Operational Environment.

THREAT	DESCRIPTION
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of activities.

Table 8: Policies Addressed by the TOE

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used.

The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PUBLIC	The TOE does not host public data.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.TEJAS	Administrators perform installation of the TOE in conjunction with TEJAS personnel.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

Table 9: Assumption

4. Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.MEDIAT	The TOE must mediate the flow of all information from users on an external network to resources on an internal network, and must ensure that residual information from a previous information flow is protected and not transmitted in any way.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.SECKEY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows.
O.SECSTA	Upon initial startup of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SIMUSE	The TOE must prevent the reuse of authenticate data for users attempting to authenticate at the TOE from a connected network.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.

Table 10: TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMTRA	Authorized administrators are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
OE.TEJAS	Administrators perform installation of the TOE in conjunction with TEJAS personnel.
OE.GENPUR	There are no general-purpose computing capabilities (e.g. the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PHYSEC	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PUBLIC	The TOE does not host public data.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 11: Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.COMINT	T.AUDACC	T.LOSSOF	T.PRIVIL	T.OLDINF	T.MEDIAT	T.PROCOM	T.REPLAY	T.USAGE	T.NOAUTH	A.TEJAS	A.GENPUR	A.LOCATE	A.PUBLIC	A.NOEVIL	A.PROTECT	A.MANAGE	A.SINGEN	P.ACCACT	P.MANAGE	P.PROTCT
O.ACCOUN		✓																	✓		
O.ACCESS	✓																			✓	✓
O.AUDITS		✓																			
O.EADMIN										✓											
O.IDAUTH										✓										✓	✓
O.SECFUN			✓																		✓
O.MEDIAT					✓	✓															
O.PROTCT			✓	✓																	✓
O.SECKEY							✓														
O.SECSTA	✓																				
O.SIMUSE								✓													
O.TOECOM							✓														
OE.TEJAS											✓									✓	
OE.ADMTRA									✓				✓							✓	✓
OE.GENPUR												✓									
OE.CREDEN															✓						✓
OE.INSTAL															✓		✓				
OE.PHYSEC													✓			✓					✓
OE.PUBLIC														✓							
OE.SINGEN																		✓			

Table 12 : Mapping of Assumption, Threats and OSPs to Security Objectives

4.3.1 Rationale for Security Threats to the TOE

SFR	RATIONALE
T.AUDACC	This is countered by ➢ O.ACCOUN provides user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit. ➢ O.AUDITS records audit records for data accesses and use of the TOE functions.
T.COMINT	This is countered by ➢ O.ACCESS allows authorized users to access only appropriate TOE functions and data. ➢ O.SECSTA provides the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows

T.LOSSOF	This is countered by ➢ O.SECFUN provides functionality that enables an authorized administrator to use the TOE security functions, and ensure that only authorized administrators are able to access such functionality. ➢ O.PROTCT protects itself from unauthorized modifications and access to its functions and data.
T.PRIVIL	This is countered by ➢ O.PROTCT protects itself from unauthorized modifications and access to its functions and data.
T.MEDIAT	This is countered by ➢ O.MEDIAT mediates the flow of all information from users on an external network to resources on an internal network and ensure that residual information from a previous information flow is protected and not transmitted in any way.
T.NOAUTH	This is countered by ➢ O.EADMIN includes a set of functions that allow effective management of its functions and data. ➢ O.IDAUTH identifies and authenticates authorized users prior to allowing access to TOE functions and data.
T.OLDINF	This is countered by ➢ O.MEDIAT mediates the flow of all information from users on an external network to resources on an internal network and ensure that residual information from a previous information flow is protected and not transmitted in any way.
T.PROCOM	This is countered by ➢ O.SECKEY provides the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows. ➢ O.TOECOM protects the confidentiality of its dialogue between distributed components.
T.REPLAY	This is countered by ➢ O.SIMUSE prevents the reuse of authenticate data for users attempting to authenticate at the TOE from a connected network.

T.USAGE	This is countered by ➢ OE.ADMTRA authorized administrators are trained to appropriately install, configure and maintains the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.

5. Extended Components Definition

5.1 Definition of Extended Components

There are no extended components in this Security Target.

6. Security Functional Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.2	Guarantees of audit data availability
	FAU_STG.3	Action in case of possible audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
	FDP_RIP.1	Subset Residual Information Protection
Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_SAE.1	Time-limited authorization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
	FMT_SMR.2	Restrictions on security roles
Protection of the TSF	FPT_STM.1	Reliable Time Stamps
TOE Access	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
Trusted Path/Channels	FTP_TRP.1	Trusted Path

Table 13: TOE Security Functional Requirements

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

6.2 Security Audit (FAU)

6.2.1 FAU_GEN.1 – Audit Data Generation

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

(Note: Audit function gets on / off along with the TOE startup/shutdown)

a. All auditable events for the [not specified] level of audit; and

b. [*The events in column two of Table – Auditable Events*]

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

a) Date and time of the event, type of event, subject identity (if applicable), 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, [*information specified below table*].

SFR	EVENT	DETAILS
FMT_SMR.1	Modification to the profile of users that are part of a role.	The identity of the User Manager performing modification and user identity being associated with a profile.
FIA_UID.2	All use of user identification mechanism	User Name and System IP from which operation got triggered.
FIA_UAU.2	Any use of user authentication mechanism	User Name and System IP from which operation got triggered.
FDP_IFF.1	All decisions on requests for information flow	The presumed address of the source and destination subject.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit with exception for viewing information flow security policy rules (FMT_MOF.1b), user attribute values (FMT_MOF.1 c)	The identity of the Administrator performing the Operation

Table 14: TJ5500 Auditable Events

EVENTS	DETAILS
NE (or NE component) added, deleted, or modified	NE Details along with Occurrence Time and Changes made
Any changes Made on NE	NE Details along with Occurrence Time and Changes made
All use of user identification mechanism	User Name and System IP from which operation got triggered.
Any use of user authentication mechanism	User Name and System IP from which operation got triggered.

Table 15: TJ5100 Auditable Events

6.2.2 FAU_GEN.2 – User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.3 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [TJ5500: *Administrator, Viewer and Operator roles, TJ5100: Admin*] 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.

6.2.4 FAU_SAR.2 – Restricted Audit Review

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

6.2.5 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [100000] stored audit records will be maintained when the following condition occur; [audit storage exhaustion].

6.2.6 FAU_STG.3 – Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall [*an authorized user can configure the Auto-purge option]* if the audit trail exceeds *[user defined limit (recommended is 100000 records)].*

6.3 Cryptographic Support (FCS)

6.3.1 FCS_CKM.1 – Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm:

RSA schemes using cryptographic key sizes of 2048-bit or greater3072 and 4096 bit that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3.

6.3.2 FCS_CKM.2 – Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *[as described in table 16]* that meets the following: *[as described in table 16].*

6.3.3 FCS_CKM.4 – Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroize] that meets the following: *[none].*

6.3.4 FCS_COP.1 – Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [the operations described in Table 16 – Cryptographic Operations] in accordance with a specified cryptographic algorithm *[multiple algorithms in the modes of operation described in Table 16 – Cryptographic Operations]* and cryptographic key sizes *[multiple key sizes described in Table 16 – Cryptographic Operations]* that meet the following: *[multiple standards described in Table – Cryptographic Operations].*

Protocol	Cipher suite	Respective Standards
TLS V1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA	rfc5289 rfc5289 rfc5289 rfc8422 rfc8422 rfc5288 rfc5288 rfc5246 rfc5246 rfc5246 rfc5246
TLS V1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256	rfc8446 rfc8446

Table 16: Cryptographic Operations

6.4 Information Flow Control (FDP)

6.4.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [*Flow control SFP*] based on the following types of subject, information and operation: [

Subject: Remote network systems sending and receiving data / packet through ports on two different NEs.

Information: Data /packet and

Operation: Forwarding of received data / packets]

6.4.2 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the data /traffic filtering SFP based on the following types of subject and information security attributes: [

Subject attributes: Receiving network element IP address, port and configured ACL;

Information attributes: Presumed source and destination IP addresses and ports.]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *[If an ACL is configured for the receiving IP address and port, Data /packet are forwarded if the presumed source or destination IP address and port is explicitly included in the ACL*.]

FDP_IFF.1.3 The TSF shall enforce the [*No additional rules*].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [*No additional rules*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*No additional rules*].

6.4.3 FDP_RIP.1 – Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to*] the following objects: [*Destination*].

6.5 Identification and Authentication (FIA)

6.5.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an User Manager configurable positive integer within the range 1-15 unsuccessful authentication attempts occur related to consecutive login failure attempts of an individual User Account. The default no of unsuccessful authentication attempts is 5.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall lock the User Account until unlocked by the User Manager.

6.5.2 FIA_ATD.1 – User Attribute Definition

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

- Username
- Password
- Associated user profile
- Password expiration value
- Inactive Timer Value
- Consecutive unsuccessful login count].

6.5.3 FIA_SOS.1 – Verification of secrets

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

1. *Minimum of eight (8) characters,*
2. *Maximum 110 allowed characters,*
3. *Minimum of one (1) numeric characters,*
4. *Minimum of one (1) special character,*
5. *Combination of both uppercase and lowercase alphabetic characters].*

6.5.4 FIA_UAU.2 – User Authentication before Any Action

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.

6.5.5 FIA_UID.2 User identification before any action

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

6.6 Security Management (FMT)

6.6.1 FMT_MOF.1 – Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behavior of, disable, enable and modify the behavior of]* the functions[

1. *Create, delete, and modify custom profiles; to [the User Manager]*
2. *Association and modification of user profiles; to [the User Manager]*
3. *Creation or deletion of temporary users; to [the User Manager]*
4. *Enable and disable external IT entities from communicating to the TOE; to [the Administrator profile]*
5. *Archive and clear the audit trail; to [the Administrator profile].*

]

6.6.2 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*flow control SFP*] to restrict the ability to [create & delete] the security attributes [*information flow security policy rules that permit or deny information flows*] to [*as defined in the FMT_MTD.1*].

6.6.3 FMT_MSA.2 – Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [*security attributes listed as per the Information flow control*].

6.6.4 FMT_MSA.3 – Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [*Information flow control SFR*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

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

6.6.5 FMT_SAE.1 – Time-limited Authorization

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [*passwords*] to [*the* User manager *profile / role*].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [*prompt the authenticated entity to change their password before allowing access to the User or Administrator interfaces of the TOE*] after the expiration time for the indicated security attribute has passed.

6.6.6 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*change default, modify, delete] the* [*data described in Table 17 –Management of TSF data*] to [*as per the table*]:

TOE	User Profiles / Roles	Management of TSF Data					
		Audit log		management sessions	Flow control SFP	User Account Attributes	User security attributes modification
		Viewing	Purge				
TJ5500	Administrator	✓	✓	✓	✓	×	×
	User Manager	×	×	×	×	✓	✓
	Operator	✓	×	×	×	×	×
	Viewer	✓	×	×	×	×	×
TJ5100	Admin	✓	NA	NA	NA	✓	✓
	Operators	×	×	×	NA	×	×
	Users	×	×	×	NA	×	×

Note: - *TJ5100 Operators and Users are default profiles which are used for two different purposes like user associated with profile "users" will have only view access and will not have permission to modify any data but users associated with profile "operators" will have permission to set some attributes value on Network Element.*

Table 17: Management of TSF data

6.6.7 FMT_SMF.1 - Specification of Management Functions

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

a) Create, delete, and modify custom profiles;
b) Create, delete, modify, and view user attribute values defined in FIA_ATD.1;
c) Creation or deletion of temporary users;
d) Enable and disable external IT entities from communicating to the TOE;
e) Archive, clear, and review the audit trail].

6.6.8 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the profiles / roles [

- *TJ5500*: *Viewer, Operator, User Manager and Administrator*
- *TJ5100: Admin, Operator and User]*.

Note: TJ5500: Except default profiles like Viewer, Operator, User Manager and Administrator, User manager has privilege to create custom profile as per requirement.

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

6.6.9 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles [*Viewer, Operator, User Manager and Administrator]*.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall govern the following profile/role assignment

- An account of TJ5500 with Viewer profile can only play role of viewer and cannot play other role.
- An account of TJ5500 with Operator profile can play role of both Operator and Viewer but cannot play role of Administrator and Manager.
- An account of TJ5500 with User Manager Profile can only play role of User Manager and cannot play other roles.
- An account of TJ5500 with administrator profile can play role of Viewer, Operator and Administrator but cannot play role of User Manager.

6.7 Protection of the TSF (FPT)

6.7.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.8 TOE Access (FTA)

6.8.1 FTA_SSL.3 – TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*30 minute (default) period of inactivity or maximum configured session inactivity period has been reached. Maximum allowed time period is 120 minutes*].

6.8.2 FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.8.3 FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [assignment: 1 number] sessions per user.

6.9 Trusted Path/Channels (FTP)

6.9.1 FTP_TRP.1 –Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification or disclosure].

FTP_TRP.1.2 The TSF shall permit [r*emote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*initial user authentication and all further communication after authentication*].

6.10 Security Functional Requirements for the IT Environment

There are no Security Functional Requirements for the IT Environment.

6.11 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.12.3 – Security Assurance

Requirements.

6.12 Security Requirements Rationale

6.12.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

THREATS/ ASSUMPTIONS / OBJECTIVES	O.ACCOUN	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.SECFUN	O.MEDIAT	O.PROTCT	O.SECKEY	O.SECSTA	O.SIMUSE	O.TOECOM
FAU_GEN.1	✓		✓									
FAU_GEN.2	✓		✓									
FAU_SAR.1			✓	✓								
FAU_SAR.2		✓	✓		✓							
FAU_STG.2		✓			✓	✓		✓				
FAU_STG.3						✓		✓				
FCS_CKM.1									✓			
FCS_CKM.2									✓			
FCS_CKM.4									✓			
FCS_COP.1									✓			
FDP_IFC.1							✓					
FDP_IFF.1							✓					
FDP_RIP.1							✓					
FIA_AFL.1		✓			✓							
FIA_ATD.1					✓						✓	
FIA_SOS.1					✓							
FIA_UAU.2		✓			✓							
FIA_UID.2	✓	✓			✓							
FMT_MOF.1						✓				✓		
FMT_MSA.1						✓	✓			✓		
FMT_MSA.2						✓	✓			✓		
FMT_MSA.3						✓	✓			✓		
FMT_SAE.1						✓						
FMT_MTD.1		✓			✓	✓	✓	✓		✓		
FMT_SMF.1				✓		✓						
FMT_SMR.1					✓	✓						
FMT_SMR.2						✓						
FPT_STM.1			✓									
FTA_MCS.1		✓										
FTA_SSL.3								✓				
FTA_SSL.4								✓				
FTP_TRP.1												✓

Table 18: Security Functional Requirements

6.12.2 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

SFR	RATIONALE
FAU_GEN.1	This component outlines what data must be included in audit records and what event must be audited. This component traces This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the objectives: O.AUDITS and O.ACCOUN.
FAU_GEN.2	This component addresses the requirement of accountability of auditable events at the level of individual user identity. It is used in addition to FAU_GEN.1
FAU_SAR.1	This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDITS and O.EADMIN
FAU_SAR.2	This component specifies that any users not identified in FAU_SAR.1 Audit review will not be able to read the audit records and aids in meeting the following objective: O.AUDIT, O.EADMIN and O.IDAUTH
FAU_STG.2	This component allows specifying to which metrics the audit trail should conform. This component traces back to and aids in meeting the following objectives: O.ACCESS, O.IDAUTH, O.PROTCT and O.SECFUN.
FAU_STG.3	This component ensures that the authorized administrator will be able to save data contained in the audit trail if the storage space should become full. It also ensures that no current audit events are lost. This component traces back to and aids in meeting the following objectives: O.PROTCT and O.SECFUN.
FCS_CKM.1	This component ensures that cryptographic keys and parameters are generated with standards-based algorithms and aids in meeting the following objective: O.SECKEY
FCS_CKM.2	This component provides secure key distribution to remote trusted IT products (users or other instances of TOE). The TOE to perform authentication using digital certificates, ensuring the source is trusted and aids in meeting the following objective: O.SECKEY
FCS_CKM.4	This component ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the Administrator forces generation of new keys. Keys are zeroized in accordance with FIPS 140-2 specifications and aids in meeting the following objective: O.SECKEY
FCS_COP.1	This component ensures that when all users communicate with the TOE remotely from an internal or external network that robust algorithms are used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.SECKEY
FDP_IFC.1	This component identifies the ports involved in the flow control SFP (i.e., forwarding / sending information to one port to another port). This component traces back to and aids in meeting the following objective: O.MEDIAT.
FDP_IFF.1	This component identifies the type of subject and information attributes and permits information flow between the source and destination ports. Then the policy is defined by saying where information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FDP_RIP.1	This component ensures that any residual information content pertaining to a resource accessible by a user, such as access to a file server, is not made available upon the allocation of that resource to another user. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FIA_AFL.1	This component addresses unsuccessful authentication and as such aids in meeting the following objectives: O.ACCESS, O.IDAUTH
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SIMUSE.
FIA_SOS.1	This component exists to ensure that passwords generated by users can be verified to meet the defined minimum password strength requirements. This component traces back to and aids in meeting the following objective: O.IDAUTH.
FIA_UAU.2	This component requires successful authentication of a role before having access to the TSF and as such aids in meeting O.ACCESS and O.IDAUTH.
FIA_UID.2	This component requires successful identification of a role before having access to the TSF and as such aids in meeting O.ACCESS, O.IDAUTH and O.ACCOUN.
FMT_MOF.1	This component was chosen to consolidate all TOE management / administration / security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.SECSTA.
FMT_MSA.1	This component restricts the ability to create, delete, modify and view the parameters for the flow control SFP as per the defined user's privilege / role and ensure that residual information from a previous information flow is protected and not transmitted in any way and as such aids in meeting O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_MSA.2	This component restricts the ability to create, delete and view the parameters for the Information flow control SFP as per the defined user's privilege / role and ensure that residual information from a previous information flow is protected and not transmitted in any way and as such aids in meeting O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_MSA.3	This component restricts the ability to create, delete and view the parameters for the Information flow control SFP as per the defined user's privilege / role and ensure that residual information from a previous information flow is protected and not transmitted in any way and as such aids in meeting: O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_SAE.1	The component provides the capability for an User manager to specify an expiration time on a user's password. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_MTD.1	This component restricts the ability to modify the flow control SFP, and as such aids in meeting O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.IDAUTH, O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to delete audit logs, and as such contributes to meeting O.MEDIAT, O.SECSTA, O.PROTCT and O.SECFUN. This component restricts the ability to modify the date and time, and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts unauthorized users to access appropriate TOE functions and data to meet O.ACCESS.

FMT_SMF.1	This component allows a set of functions that allow effective management of its functions and data to meeting the objective: O.EADMIN. This component was chosen in an attempt to consolidate all TOE Management / administration / security functions. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SMR.1	This component identifies and authenticates authorized users prior to allowing access to TOE functions and data to meeting the objective: O.IDAUTH. This component ensures that roles are available to allow for varying levels of administration capabilities and restricts access to perform TSF relevant functionality depending on the role assigned to an authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SMR.2	This component specifies the different roles that the TSF should recognize, and conditions on how those roles could be managed. and aids in meeting the following objective: O.SECFUN
FPT_STM.1	FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDITS.
FTA_MCS.1	This component allows the system to limit the number of sessions in order to effectively use the resources of the TOE. This component traces back to and aids in meeting the following objective: O.ACCESS
FTA_SSL.3	This component protects the TOE's communication path by terminating sessions idled for longer than 30 minutes and maximum of 120 minutes. This component traces back to and aids in meeting the following objective: O. O.PROTCT
FTA_SSL.4	This component provides the capability for an authorized user to terminate his/her interactive session. This component traces back to and aids in meeting the following objective: O.PROTCT
FTP_TRP.1	This component ensures about trusted communication between a user and the TSF. This component traces back to and aids in meeting the following objective: O.TOECOM

Table 19: Rationale for TOE SFRs to Objectives

The following table presents a mapping of the rationale of TOE Objectives to Security Requirements:

OBJECTIVE	RATIONALE
O.ACCOUN	This objective is completely satisfied by • FAU_GEN.1 - which outlines what events must be audited FAU_GEN.2 - which ensures about association of each auditable event with the identity of the user caused the event. • FIA_UID.2 - ensures that users are identified to the TOE
O.ACCESS	This objective is completely satisfy by

	• FAU_SAR.2 - The TOE is required to restrict the review of audit data to those granted with explicit read-access • FAU_STG.2 -The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack. • FIA_UID.2 & FIA_UAU.2- Users authorized to access the TOE are validated using an identification and authentication process. • FIA_AFL.1 - This process is supported by defined actions when repeated invalid credentials are supplied. • FMT_MTD.1 - Only authorized users of the TOE may access TSF data and functions according to their permissions. • FTA_MCS.1 – This shall restrict the maximum number of concurrent sessions that belong to the same user and shall enforce, by default, a limit of sessions per user.
O.AUDITS	This objective is completely satisfy by • FAU_GEN.1 - Security-relevant events must be defined and auditable for the TOE • FAU_GEN.2 – ensures the identity of the user that caused the event. • FAU_SAR.1 – which ensures that the audit trail/log can be read • FAU_SAR.2- Which ensures that the audit log can only be read by authorized users • FPT_STM.1 ensures that reliable time stamps are provided for audit records.
O.EADMIN	The objective is completely satisfy by • FAU_SAR.1 – which ensures the ability to review the audit trail/log • FMT_SMF.1 – ensures the ability of authorized users (Usermanager / Administrator) to effectively manage the TOE functions and data.
O.IDAUTH	The objective is completely satisfy by • FAU_SAR.2 - The TOE is required to restrict the review of audit data to those granted with explicit read-access. • FAU_STG.2 - The TOE is required to protect the stored audit records from unauthorized deletion. • FIA_ATD.1 - Security attributes of subjects use to enforce the authentication policy of the TOE must be defined. • FIA_UID.2 & FIA_UAU.2 - Users authorized to access the TOE are validated using an identification and authentication process • FIA_AFL.1 - The process includes defined actions when repeated invalid

	credentials are supplied • FIA_SOS.1 – which specifies metrics for authentication, and aids in meeting objectives to restrict access • FMT_MTD.1- Only authorized users may access TSF data and functions according to their permissions • FMT_SMR.1 - The TOE must be able to recognize the different roles that exist for the TOE
O.SECFUN	This objective is completely satisfied by • FAU_STG.2 which ensures that log /audit data protected and can be stored. • FAU_STG.3 which ensures the TOE overwrites the oldest stored audit data with any further audit data generated when the audit trail/log become full. • FMT_MOF.1 which ensures the ability to perform security management functions is restricted to administrator or User Manager. • FMT_MSA.1 which restricts the ability to create, modify, delete and view the parameters for the information flow control to user roles as defined in the FMT_MTD.1 • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Information flow control • FMT_MSA.3 which ensures that there is a default denies policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations • FMT_SAE.1 which allows Usermanager to set expiration times for user passwords • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 & FMT_SMR.2 defines the roles on which access decisions are based.
O.MEDIAT	This objective is completely satisfied by • FDP_IFC.1 which ensures the TOE supports an user information flow policy that controls which port can send and receive network traffic • FDP_IFF.1 which ensures the information flow control SFP based on the subject and information attributes and permits an information flow between controlled subject and information via a controlled operation.

	• FDP_RIP.1 which ensures the TOE tracks all packet information including packet length and ensures that no residual data is exposed to users. • FMT_MSA.1 which restricts the ability to create, modify, delete and view the parameters for the information flow control to user roles as defined in the FMT_MTD.1 • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Information flow control • FMT_MSA.3 which ensures that restricts the ability to modify, delete and view the parameters for the Information flow control SFP as per the defined user's privilege / role and ensure that residual information from a previous information flow is protected and not transmitted in any way. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations
O.PROTCT	This objective is completely satisfy by • FAU_STG.2 The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack. • FAU_STG.3 which ensures the TOE overwrites the oldest stored audit data with any further audit data generated when the audit trail/log become full. • FMT_MTD.1 Only authorized users may access TSF data and functions according to their permissions • FTA_SSL.3 ensure termination of an interactive session after a [30 minute period of inactivity (default) or a configured inactivity (maximum 120 minutes) inactivity period has been reached]. • FTA_SSL.4 allows user-initiated termination of the user's own interactive session.
O.SECKEY	This objective is completely satisfy by • FCS_CKM.1 which ensures that cryptographic keys and parameters are generated with standards-based algorithms • FCS_CKM.2 which provides secure key distribution to remote trusted IT products • FCS_CKM.4 which ensures that the cryptographic keys and parameters are safely destroyed. • FCS_COP.1 ensures that when all users communicate with the TOE remotely from an internal or external network that robust algorithms are used to encrypt such traffic.

O.SECSTA	This objective is completely satisfy by • FMT_MOF.1 which ensures the ability to perform security management functions is restricted to an authorized Administrator • FMT_MSA.1 which restricts the ability to create, modify, delete and view the parameters for the information flow control to user roles as defined in the FMT_MTD.1 • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Information flow control. • FMT_MSA.3 which ensures that there is a default denies policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations.
O.SIMUSE	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users.
O.TOECOM	This objective is completely satisfied by • FPT_TRP.1 ensures about trusted communication between a user and the TSF.

Table 20: Rationale for TOE Objectives to SFRs

6.12.3 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description.
	ADV_FSP.2	Security – enforcing functional specification.
	ADV_TDS.1	Operational User Guidance and Preparative Procedures Supplement.
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance.
	AGD_PRE.1	Preparative Procedures.
ALC: Lifecycle Support	ALC_CMC.2	Use of CM System.
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition

	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirement
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis.

Table 21: Security Assurance Requirements at EAL2

6.12.5 Security Assurance Requirements Rationale

The EAL-2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. 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.

6.12.6 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	TJ5500 / TJ5100 Design and Architecture document
ADV_FSP.2 Functional Specification with Complete Summary	TJ5500 / TJ5100 functional Specification document.
ADV_TDS.1 Basic Design	TJ5500 / TJ5100 Design and Architecture document
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Tejas Networks TJ5500
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Tejas Networks TJ5500
ALC_CMC.2 Use of a CM system	Life cycle Support process document.
ALC_CMS.2 Parts of the TOE CM coverage.	Life cycle Support process document.
ALC_DEL.1 Delivery Procedures	Delivery Procedures document
ASE_CCL.1 Conformance claims	TJ5500 / TJ5100 Security Target
ASE_ECD.1 Extended components Definition	TJ5500 / TJ5100 Security Target
ASE_INT.1 ST introduction	TJ5500 / TJ5100 Security Target
ASE_OBJ.2 Security objectives	TJ5500 / TJ5100 Security Target
ASE_REQ.2 Derived security Requirements	TJ5500 / TJ5100 Security Target
ASE_SPD.1 Security problem definition	TJ5500 / TJ5100 Security Target
ASE_TSS.1 TOE summary specification	TJ5500 / TJ5100 Security Target
ATE_COV.1 Evidence of coverage	Testing Evidence: Functional and test coverage document
ATE_FUN.1 Functional Testing	Test report: Functional and test coverage document
ATE_IND.2 Independent testing	
AVA_VAN.2 Vulnerability analysis	Nessus scan report: Tejas Networks TJ5500

Table 22: Security Assurance Rationale and Measures

7. TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Operations
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

7.2 Security Audit

TOE generates a set of AUDIT records which are stored in database tables. Each records of database contain the following parameters:

TOE	ATTRIBUTE	DESCRIPTION
TJ5500	User Name	Displays the name of the user.
	App Name	Displays the name of the application
	Time of Action	Displays the date and time of action
	Module Name	Displays the module name.
	Action	Displays the action performed.
	Audited Object	Displays the audited object. This attribute contains the information about the object that is modified and Entity who initiated the activity : [initiating IP] initiator username if applicable, (user type if applicable), [user role if applicable]
	Audit Status	Displays Event outcome (success or failure)
	Additional Info	Displays the additional information if any. This contains information about any new object creation. For example, the circuit creation information is displayed in the Additional Info field.
TJ5100	Changes	Displays the action performed.
	Table Name	Details about actual table modification.
	User	Displays the name of the user.
	Time	Displays the time of action.

	Operation	Displays the type of action
	IP Address	Displays the IP address of system from where action is performed.
	Occurrence Time	Displays the date and time of the performed action.
	Result	Displays event outcome (true/false)

The TOE generates logs for the following list of events:

- Modifications to the group of users that are part of a role, which includes the identity of the User Manager (TJ5500) / Admin (TJ5100) performing the modification and the user identity being associated with a role in each related log;
- All use of the user identification mechanism, which includes the user identities provided to the TOE in each related log;
- Any use of the authentication mechanism, which includes the user identities provided to the TOE in each related log;
- All decisions on requests for information flow with the exception for permitted access to a Windows file resource, which includes the presumed addresses of the source and destination subject in each related log;
- Changes to the time, which includes the identity of the Administrator performing the operation in each related log;
- Use of the functions listed in this requirement pertaining to audit with the exception for viewing information flow security policy rules, user attribute values, and audit trail data, which includes the identity of the Administrator performing the operation in each related log.

The logs are only accessible through the Web-Based administrative interface, which only authenticated Administrators are authorized access. Administrator can view, filter, purge and save the logs. When logs are saved from the TOE, they are transferred to the PC connected to the Web-Based administrative. The administrator also has the ability to change the log setting example: configuration of Auto-purge.

Audit Filter: Filtering audit provides set of attributes on which authorized user can filter audit logs. Combination of any of following attributes can be used as filter criteria.

User Name: User name drop-box displays list of user names. Authorized user may select one of the name from drop-box or you can type user name in drop-box
App Name: Name of the application from where operation is done.

Action: Action drop-box contains set of predefined actions, which can used to filter audit logs of specific action. Example: Login Action.

Status: Status of operation performed i.e., Success or Failure

Date from & Date to: Calendar button to select a date, to filter audit logs of particular date range specify date in Date From and Date To.

TOE has backup and purge facilities to maintain circular buffer for audit records. After the audit log records reached to maximum configured limit for logs in database, The oldest audit log records are overwritten by new records (If Auto-purge configured with backup option then backup will be taken before overwriting the records).

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

- FAU_GEN.1 and FAU_GEN.2: TJ5500 / TJ5100 generate all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details.
- FAU_SAR.1: The Administrator / Admin, operator and viewer have the ability to read all of the audit logs.
- FAU_SAR.2: TOE protects the unauthorized viewing of audit log. Any users not identified in FAU_SAR.1 Audit review will not be able to read the audit records.
- FAU_STG.2: Administrator, operator and viewer have access to view logs. Oldest audit record can be saved and purge once it reaches to maximum configured limit only by Administrator profile. Other user profile doesn't have privilege to purge the logs.
- FAU_STG.3: An authorized user can configure the Auto-purge option with required audit limit [the recommended limit is 100000], backup for old records, date and time log records in database to avoid the audit data loss.

7.3 Cryptographic Operations

TOE provides and encrypted path between users and TOE. Users connect to TOE using a secure connection using AES encryption algorithms supported by TJ5500. The secure connection ensures that user passwords and data are protected from modification and disclosure.

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

- FCS_CKM.1: This component ensures that cryptographic keys and parameters are generated with RSA schemes using cryptographic key sizes of 2048-bit or greater3072 and 4096 bit that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS
- FCS_CKM.2: This component provides secure key distribution through RSA that meets the TLS_ECDHE_RSA with AES_128/256 and TLS_DHE_RSA with AES_128/ 256.
- FCS_CKM.4: This component ensures that the non-persistent cryptographic keys are zeroized as the session terminates.
- FCS_COP.1: Robust algorithms as listed in table 16 are used to support encrypted communications.

7.4 User Data Protection

TOE enforces flow control policy between source and destination IP address and ports of two different network elements as per standard architecture. Before any access is granted, users must log into TJ5500. Each user account is associated with one user profile. Only the Administrator profile has privilege to set the flow control SFP.

TOE ensures that all packets that are delivered to a user do not contain residual information.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE supports a user information flow policy that controls which network element

can send and receive network traffic as per the standard architecture.

- FDP_IFF.1: Flow control SFP based on the subject and information attributes and permits an information flow between a controlled subject and controlled information via a controlled operation.
- FDP_RIP.1: Circuit created from TOE will create connection in participating nodes and deletion of circuit from TOE will delete connection from nodes and there will not be any residual information.

  The circuit between source and destination in TOE made as per the standard frame format. There won't be any residual information data exposed to non-designated destination.

7.5 Identification and Authentication

TOE performs identification and authentication of all users and administrators. TOE has the ability to authenticate users locally using a password or can integrate with a remote authentication server. In the evaluated configuration, TOE will perform the authentication locally. Users enter a username and password, which is validated by TOE against the user information stored by the TOE. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

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

- FIA_AFL.1: TOE shall detect unsuccessful attempts as configured by User Manager for an individual accounts. The default no. of unsuccessful authentication attempts is 5. When the defined number of unsuccessful authentication attempts has been met, the TSF shall lock the User Account till the user manager unlock that account.
- FIA_ATD.1: For each registered user, the TOE stores the following information: user identity, user name, user profiles, and password.
- FIA_SOS.1: Secrets are configured by the User Manager to ensuring their strength. The following are the default parameters of authentication secrets:
  - Minimum of eight (8) characters,
  - Maximum 110 allowed characters,
  - Minimum of one (1) numeric character,
  - Minimum of one (1) special character,
  - Combination of both uppercase and lowercase alphabetic characters
- FIA_UAU.2: The TOE requires a valid password associated with a user name before providing access to the TOE. Passwords must conform to the requirements in FIA_SOS.1
- FIA_UID.2: The TOE requires a user name during the identification and authentication process. The username is entered, then a password. If the password is valid, the user will be associated with a role and set of privileges based on the username.

AAA Server:

- AAA Server provides security for system. Authentication, Authorization and Auditing request/response for Web client (web GUI) and Applet
- AAA Server communicates with the NMS Server using RMI. AAA for the Security and NMS server to perform business logic.

- It also updated cache through JMS object sent by NMS server.
- It converts the xml request data to POJO using JAXB and vice versa.
- It provides the view (jsp) to client using webfwk. It our own web frame work similar to STRUTS.

7.6 Security Management

TJ5500

The security feature in NMS is designed on a RBAC (Role Based Access Control) model. Each profile has a set of allowed actions associated with the profile. Each user is associated with a profile. The system by default provides four non-modifiable profiles.

- Administrator: The user assigned with this profile setting will have permissions like, to view and purge audit logs, managing of EMS, topology, TL, nodes, alarms, circuits, service and tunnels function.
- Operator: The user assigned with this profile has the permission to view audit logs and make changes in configuration, manage circuits and acknowledge alarms.
- Viewer: The user assigned with this profile has only the permission to view audit logs, alarms and configuration data.
- User Manager: The user assigned with this profile has permission to create, delete and modify the user account and security attributes. Also has privilege to create custom profile as per requirement.

TJ5100

Security management controls access to the network resources to ensure the reliability of the network. The security feature in EMS is designed on a user based security module. Different users are assigned different permissions (read, write, delete) on the tasks that they are authorized to perform. EMS defines certain terms such as actions, action table permissions, profiles, and groups that are associated with security.

The actions include viewing, configuring and modifying the network attributes. Each action has a certain set of tables associated with it. The user will have access to these tables with the permissions (read, write, and/or delete) based on the action table permissions defined.

The profiles consist of a set of pre-defined actions. User is authorized to assign a profile with the permissions associated. The group consists of authorized users. The users in a group have access to all the objects that the group is assigned to and their access levels are defined by their profiles.

- EMS_Admin: The user assigned with this profile setting will have permissions like, to view audit logs and create, delete and modify the user account and security attributes.
- EMS_Operator: The user assigned with this profile has the permission to make changes in configuration and acknowledge alarms and doesn't have privilege to access to TSF data.
- EMS_User: The user assigned with this profile has only the permission to view alarms and configuration data and doesn't have privilege to access to TSF data.

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

- FMT_MOF.1: User Manager able to create, delete, modify and association of user profile. Also able to create and delete a temporary user. Administrator able to archive and clear the audit trail and enable / disable the external IT entities from communicating to the TOE.
- FMT_MSA.1: User privilege / roles as per FMT_MTD.1 ensure the ability to create, delete and view the parameters for the information flow policy rule (circuit).
- FMT_MSA.2: This component ensures that only secure values are accepted for the configuration parameters associated with the information flow control SFP.
- FMT_MSA.3: Restrictive access by default but the Administrator can assign more restrictive permissions.
- FMT_MTD.1: The TOE restricts the management of TSF data as per FMT_MTD.1FMT_SAE.1: User Manager able to set passwords expiry period. When password expired, user is prompted to change their password before being allowed additional access to the TOE.
- FMT_SMF.1: User Manager able to create, delete, modify and association of user profile. Also able to create and delete a temporary user. Administrator able to archive and clear the audit trail and enable / disable the external IT entities from communicating to the TOE.
- FMT_SMR.1: User Manager, Operator, Viewer and Administrator are the default profiles to manage the security roles / permission of an user. Customs profile can also be created by user manager to define the custom roles.
- FMT_SMR.2: An account with Viewer profile can only play role of viewer and cannot play other role, an account with Operator profile can play role of both Operator and Viewer but cannot play role of Administrator and Manager, an account with User Manager Profile can only play role of User Manager and cannot play other roles and an account with administrator profile can play role of Viewer, Operator and Administrator but cannot play role of User Manager.

7.7 Protection of the TSF

TOE provides a timestamp for its own use. The timestamp is used from the clock provided in the TOE environment hardware. The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_STM.1: The TOE provides a reliable timestamp for its own use.

7.8 TOE Access

TOE provides a limitation on multiple concurrent graphical user interface session. Maximum of sessions depends on the license. Also TOE protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 30 minutes or reaches a maximum lifetime of 120 minutes, the session times out and is deleted from the session table. Session timeouts are enforceable on sessions initiated on both the administrator and user interfaces of the TOE.

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

- FTA_MCS.1: Restrict the maximum number of concurrent sessions that belong to the same user as per license agreement.
- FTA_SSL.3: Protects existing encrypted sessions from becoming compromised by enforcing a session timeout after a session has been idle for more than 30 minutes (default) or configured session inactivity (maximum120 minutes) has been reached.
- FTA_SSL.4: User can terminate their own session through logout option.

7.9 Trusted Path

The TOE client is a web based graphical user interface, which enables the operator or the user to visualize the network and perform management operations. The user-interface facilitates the various FCAPS functionality as well as allows a graphical user interface cut through to the underlying TOE. Also communications among all service are secure via SSL over CORBA or JMS.

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

- FTP_TRP.1: A trusted path “HTTPS” is being used by remote user to connect to the TOE and both end points are identified by their IP addresses (TJ5500/TJ5100 provides whitelisting of Client IP address) and all communication (initial user authentication and all communication afterwards) follow HTTPS over TLSv1.2, TLSv1.3 path.

-- End of document --