Security Target
For
C-DOT CRAT-100/CRDT-100 Router
Running
CROS-1.8.22-S01 Software

Released on: 06.02.2020

Any hard copy unless authorized or a soft copy in a directory other than the central repository is an Uncontrolled Copy.

This hard copy of the document is a Controlled Copy only when signed by an authorized signatory.

Issued to: ____________________________

Signature and Date

CENTRE FOR DEVELOPMENT OF TELEMATICS
MANDI ROAD, MEHRAULI, NEW DELHI 110030, INDIA
ELECTRONICS CITY (PHASE I), HOSUR ROAD, BANGALORE 560100, INDIA

Approval Block

Organizational responsibility	Name	Signature	Date
PMT coordinator	Manish Sharma	**[signed]**	**[06.02.2020]**

Revision Chart

This document replaces

Document code : CDOT-NGN-ST-CROS-v07d03
Document name : Security Target for C-DOT CRAT-100/CRDT-100 Router running CROS-1.8.22-S01 Software

Version/ Draft no.	Submitted on	Summary of changes	Reference Sections	Reason of change
v01 d01	21.02.2014	N.A.	All Sections	1st Draft
v01d02	19.03.2014	Acronyms updated. TOE description updated. CC reference updated.	Sec 1.2 Sec 1.4 Sec 2	Review feedback
v01	27.03.2014	N.A	N.A.	Released as version 01
v02d01	28.04.2015	TOE summary specifications aligned with SFRs	Sec 6 and Sec 7	Feedback during CCS workshop.
v02d02	04.06.2015	Definition of users updated.	Sec 6.2.4	Review feedback.
v02d03	30.07.2015	Rationale for Security Objectives updated	Sec 8.1	Review feedback
v02d04	03.09.2015	SRFs updated (FAU_SAR updated and FTA_TAB.1 removed)	Sec 6.2.1.5 Sec 6.2.1.6 Sec 7.1.5	Review Feedback
v02	15.10.2015	N.A.	N.A.	Released as v02
v03d01	02.03.2016	ST version and Publication Date is updated. Major security features updated. Extended Component Definition included. Threat description detailed out.	Sec 1.1 Sec 1.3.2, 1.5.2 Sec 5 Sec 3.2	Review Feedback from STQC Kolkata
v03d02	11.04.2016	Table 8 is updated. Table 10 is updated. Cryptographic Support included. Table 11 updated. Table 12 updated and OE.CRYPTO removed. Table 13 updated. FAU_SAR.3 is removed.	Sec 6.2 Sec 6.3 Sec 7.1.7 Sec 8.1.1 Sec 8.1.2 Sec 8.2 Sec 8.2.1	Review feedback

Version/ Draft no.	Submitted on	Summary of changes	Reference Sections	Reason of change
v03d03	15.05.2016	Table 4 is updated. Table 6 is updated. Table 7 is updated. Security Management Functions updated	Sec 3.1.3 Sec 4.1 Sec 4.2 Sec 6.2.4.9	Review feedback
v03d04	09.07.2016	FAU_SAR.3 component removed Updated users of TOE Sec 1.3.2.1 to 1.3.2.7 removed. TOE Access Function is updated CC Conformance for Extended components updated. Table 9 Auditable Events added	Sec 6.2.1 Sec 1.5.2 Sec 1.3.2 Sec 1.5.2 Sec 2. Sec 6.2.1.2	Review feedback
v03	19.08.2016	None	N.A.	Released as version v03
v04d01	09.12.2016	TOE reference updated to CROS1_1_8.4_1 Non-TOE hardware requirement is updated in the TOE overview ST/TOE Conformance claim along with extended components updated Users in Table 10 are made consistent as defined in entire document Table no reference is updated in section 6.3 SAR components description and rationale is described References of FIPS standards mentioned in TSS for the crypto algorithms Consistency between SFR and TSS maintained w.r.t. configuration of RADIUS/ TACACS server and by [System-Admin, Root-Admin] Consistency between SFR and TSS maintained w.r.t. configuration of system date/time and NTP server. Functions described in SFR part 6.2.4.9 are updated in TSS Part. Consistency between SFR and TSS maintained w.r.t. capability to configure the session of TOE is updated. Self-Testing is included in Protection of TSF (FPT) class as extended component (FPT_TST_EXT.1).	Sec 1.1 Sec 1.3.2 Sec 2 Sec 6.2.4 Sec 6.3 Sec 8.3 Sec 7.1.9 Sec 7.1.2 Sec 7.1.6 Sec 7.1.3 Sec 6.2.6.3 Sec 5.3, Table 8, Sec 6.2.5.2	Review Feedback from STQC (OR_ASE_CDOT _24112016)

Version/ Draft no.	Submitted on	Summary of changes	Reference Sections	Reason of change
v04d02	10.01.2017	Acronyms of 3DES, AES, DSA, ECDSA, HMAC-SHA, RSA included Auditable events for Self Test included in Table 9 Fail Secure (FPT_FLS.1) included Table no reference is updated in section 8.2 Serial Number to be assigned in Table 15	Sec 1.2 Sec 6.2.1.2 Sec 6.2.5.3 Sec 8.2 Sec 8.3	Internal review feedback
v04	31.01.2017	N.A.	N.A.	Release as v04 version
v05d01	05.11.2018	TOE Reference updated User Privileges updated Rollback FDP_ROL.1 updated Multiple Authentication Mechanism FIA_UAU.1 updated Management of TSF Data (User Attributes) updated Management of TSF Data (Sessions) updated Security Roles FMT_SMR.1 updated Session Termination on Inactivity FTA_SSL.3 updated Verification of Secrets FIA_SOS.1 updated Audit Data Generation FAU_GEN.1 updated	Entire Document Sec 1.5.2.3 Sec 6.2.2.3, 7.1.1 Sec 6.2.3.6, 7.1.2 Sec 6.2.4.3, 7.1.3 Sec 6.2.4.6, 7.1.3 Sec 6.2.4.8, 7.1.3 Sec 6.2.6.3, 7.1.5 Sec 7.1.2 Sec 7.1.4	Review feedback
v05d02	12.11.2018	Table 15 updated	Sec 8.3	Review Feedback
v05	12.11.2018	None	N.A.	Release as v05 version
v06d01	18.04.2019	Summary of items out of the TOE boundary FAU_ARP.1.1 updated Crypto Algorithms used updated in FCS_CKM.4, FCS_COP.1 FCS_SSHC_EXT.1 updated, FCS_SSHS_EXT.1 updated FMT_MSA.3 updated FAU_STG.1.2 updated Summary of Cryptographic Support for Protection of Management Interface Sessions is updated	Sec 1.5.3 Sec 6.2.1.1 Sec 6.2.7.1, 6.2.7.3 Sec 6.2.7.4 Sec 6.2.7.5 Sec 7.1.3 Sec 7.1.4 Sec 7.1.9	Review Feedback from STQC

Version/ Draft no.	Submitted on	Summary of changes	Reference Sections	Reason of change
v06d02	27.07.2019	FCS_SSHC_EXT.1.5 updated, FCS_SSHS_EXT.1.5 updated TOE Reference updated	Sec 6.2.7.4 Sec 6.2.7.5 Entire Document	Review feedback
v06d03	19.08.2019	FAU_ARP.1 updated Auditable events updated Table 9 FIA_SOS.1.1 updated FMT_MSA.3.1 updated DSA Algorithm information updated in FCS_SSHC_EXT.1.5 updated & FCS_SSHS_EXT.1.5 updated FMT_MSA.3 updated FAU_STG.1 updated	Sec 6.2.1.1 Sec 6.2.1.2 Sec 6.2.3.2 Sec 6.2.4.1 Sec 6.2.7.4 Sec 6.2.7.5 Sec 7.1.3 Sec 7.1.4	Review feedback
v06	10.09.2019	None	N.A.	Release as v06 version
v07d01	10.01.2020	TOE Reference updated Table 9 FDP_IFF.1, FPT_TST_EXT.1, FPT_FLS.1, FCS_SSHC_EXT.1 : SSH updated in Auditable events	Entire Document Sec 6.2.1.2	Feedback from STQC
v07d02	27.01.2020	Table 10 FMT_SMR.1.1 Security Roles updated for rootsystem user	Sec 6.2.4.8	Review feedback
v07d03	06.02.2020	CRDT-100 Router model mentioned along with CRAT-100 CC Conformance reference updated Details of CRAT-100 and CRDT-100 updated TOE deliverables to users included Summary of item out of the scope of evaluation is updated FAU_SIG.1 summary updated	Entire document Sec 2 Sec 1.4 Sec 1.5.3 Sec 7.1.4	Review feedback
v07	06.02.2020	None	NA	Released as v07 version

Participation

This document has been authored/modified by

NGN Team
C-DOT Delhi

Table of Contents

List of Tables

List of Figures

1. ST INTRODUCTION

1.1 ST and TOE Reference Identification

ST reference	Security Target for C-DOT CRAT-100/CRDT-100 Router running CROS-1.8.22-S01 Software
ST Version	Version 7.0
Publication Date	06.Feb.2020
ST Author	NGN Team, C-DOT Delhi
Developer of the TOE	C-DOT
TOE Reference	CROS-1.8.22-S01 Software running on C-DOT CRAT-100/CRDT-100 Router
TOE Hardware Models	C-DOT CRAT-100/CRDT-100 Routing Platform
TOE Software Version	CROS-1.8.22-S01
Keywords	IP, MPLS, Routing, Switching

1.2 Acronyms

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ARP	Address Resolution Protocol
AES	Advanced Encryption Standard
BGP	Border Gateway Protocol
CC	Common Criteria
CRAT	C-DOT Router AC powered Terabit
CRDT	C-DOT Router DC powered Terabit
CROS	CDOT Routing Operating System
CLI	Command Line Interface
CM	Configuration Management
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standard
FM	Fault Management
FTP	File Transfer Protocol
HA	High Availability
HMAC-SHA	Hash Message Authentication Code - Secure Hash Algorithm
I/O	Input/Output
IP	Internet Protocol
IT	Information Technology
MPLS	Multi-Protocol Label Switching

NGN	Next Generation Network
NTP	Network Time Protocol
OAM	Operation Administration and Management
OS	Operating System
OSPF	Open Shortest Path First
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RIB	Routing Information Base
RIP	Routing Information Protocol
RSA	Rivest-Shamir-Adleman Algorithm
SF	Security Functions
SFR	Security Functional Requirements
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSHv2	Secure Shell Version 2
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

Table 1: Acronyms list

1.3 TOE Overview

1.3.1 Usage and major features of the TOE

The TOE is CROS-1.8.22-S01 software running on C-DOT CRAT-100/CRDT-100 routing platform. C-DOT CRAT-100/CRDT-100 routing platform is designed to operate in Core and Edge layer of IP/MPLS network. The TOE analyzes the incoming IP traffic/packets and routes them to the required destination as per the information contained in the IP packet and defined routing procedures.

1.3.2 Major security features of the TOE

The TOE is comprised of several security features which consist of following security functionalities.

- User Data Protection Function
- Identification and Authentication Function
- Security Management Function
- Audit Function
- TOE Access Function
- Protection of TOE Security Functions (TSF)
- Cryptographic Support

None of the above mentioned security features are implemented in CRAT-100/CRDT-100 hardware. However, TOE runs on CRAT-100/CRDT-100 hardware based routing platform.

1.4 TOE Description

TOE is software running on C-DOT CRAT-100/CRDT-100 system. The CRAT-100/CRDT-100 system is based upon innovative hardware solution and software exploits the innovative hardware features for line rate performance. It is designed to address Core and Edge layer of typical IP/MPLS network deployment. This system can be used as routing solution for a broad range of applications in the datacenter and in service provider environments. CRAT-100/CRDT-100 system can act as a standalone L2-L4 switching and routing system for converged Ethernet datacenters, as well as broadband aggregation systems. The system supports both routing and switching functionality. The required features on devices can be configured using software driven management interface. So, same device can work as an L2 switch, L3 Switch or router, as required by the user. It implements industry standard compliant OAM features to manage the network. It provides standard compliant software/hardware interfaces for interoperability.

TOE has distributed architecture with clear separation of Forwarding Plane processing from the Control Plane processing. Similarly, both the Forwarding Plane and the Control plane are decoupled from the management plane ensuring TOE protection. During startup, TOE performs a series of self-tests which checks the integrity of the TOE. In case of fault, TOE fault management (FM) feature handles and recovers the fault, providing the uninterrupted services of system.

CRAT-100 and CRDT-100 platform are equivalent in terms of their hardware except their power supply. CRAT-100 is an AC powered (220V) system whereas CRDT-100 is powered through DC power (-48V) supply. The AC and DC power supply modules are interchangeable in the system. The hardware functionality and the CROS software functionality run on these platforms is independent of the AC or DC power supplies.

Following are the parts/items delivered to the TOE user:

S.N	Part/Item Description	Delivery method
1.	CRAT-100/CRDT-100 Router Hardware along with 2 set of power cable, one USB to Serial Cable and Hardware Release Note	Packed in a box and shipped by post
2.	CROS-1.8.22-S01 with Software Release Note	In a CD and shipped by post
3.	Installation Manual-v05	In a CD and shipped by post
4.	User Manual-v04	In a CD and shipped by post

1.4.1 TOE Type

TOE is C-DOT Routing Operation System software (CROS-1.8.22-S01) running on CRAT-100/CRDT-100 routing platform providing routing/switching functionality in IP/MPLS network.

1.5 TOE Boundaries

The TOE physical and logical boundaries are as follows:

1.5.1 Physical Boundary

The TOE is CROS-1.8.22-S01 software running within the physical boundary of CRAT-100/CRDT-100 system which is a single card routing platform having network data and management interfaces. The TOE can be configured through Command Line Interface (CLI) over SSH connection. It can be synchronized with NTP server. The user authentication for remote login can also be done through external RADIUS/TACACS server. The system logs can be transferred to external syslog server from time to time. The architectural block diagram of the TOE is shown below in figure 1.

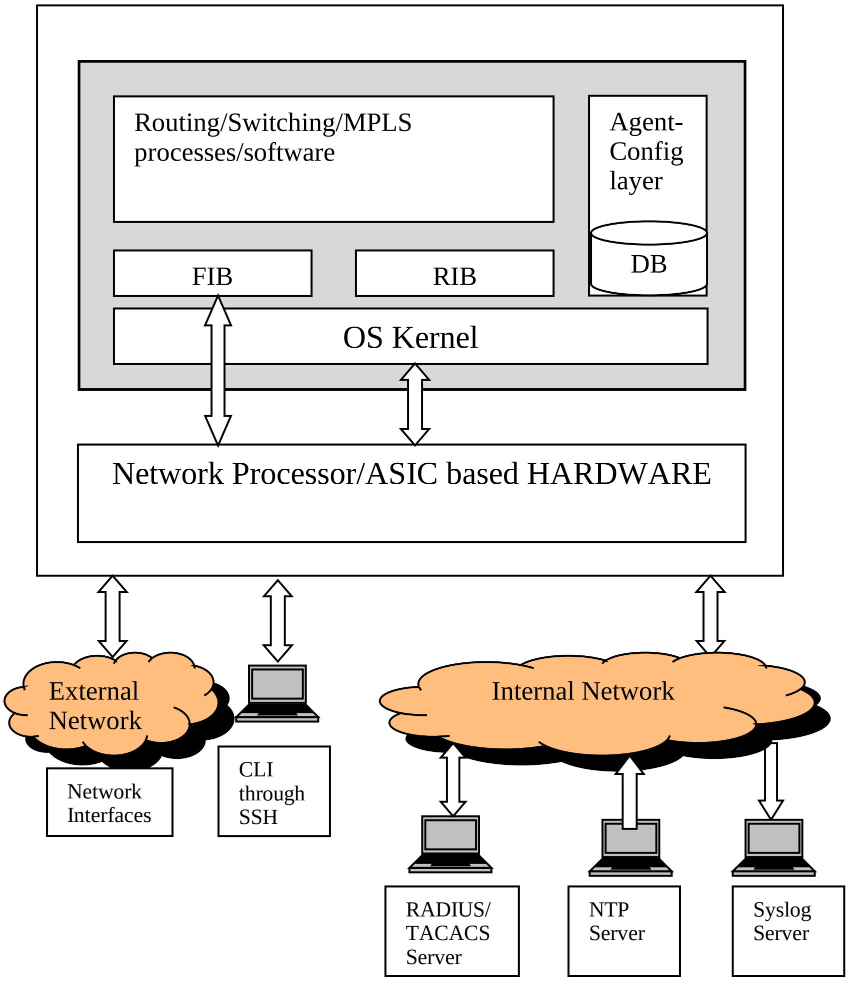


Figure 1: TOE Architecture Block Diagram

1.5.2 Logical Boundaries

TOE provides following security features:

- User Data Protection
- Identification and Authentication
- Security Management
- Audit
- TOE Access Function
- Protection of TOE Security Functions (TSF)
- Cryptographic Support

1.5.2.1 User Data Protection

The TOE receives network packets from source network nodes to its physical ports, processes them and forwards them to destination port based on available routing information. This routing information is either dynamically calculated by TOE or configured by TOE users.

1.5.2.2 Identification and Authentication

The TOE performs identification and authentication of TOE users before granting access to the system by providing user name and password. The TOE authenticates users through its local database (user name, passwords) or through a remote RADIUS/TACACS authentication server (external authentication server is outside the scope of TOE).

Applications exchanging information with TOE through management interface needs to be successfully authenticated prior to any exchange via SSH.

1.5.2.3 Security Management

The router is configured and managed through a Command Line Interface (CLI) protected by SSH. The TOE users are Operator, System-Admin and Root-System. The Operator user can only view different settings and attributes of the system. The TOE allows authorized System-Admin to create, modify and delete configurations or date and time. The Root-System can perform all the configurations done by System-Admin and user management functions, including creating and deleting users of TOE.

1.5.2.4 Audit

The TOE maintains a syslog where TOE auditable events are stored which can be sent to external log server (external syslog server is outside the scope of TOE). The audit events include authentication and configuration change activities. User name, date and time associated with each event is maintained. The audit syslog can only be viewed by Root-System and System-Admin user.

1.5.2.5 TOE Access Function

TOE access requires authentication before any administrative action. Administrative access is restricted to specific functions related to user account management and configuration of TOE. Inactive sessions both local and remote can be terminated by TOE after a time-period which can be configured by an administrator. Once a session is terminated the user is required to re-establish a new session.

1.5.2.6 Protection of TOE Security Functions (TSF)

The TOE protects its security functions through various mechanisms. The TOE performs self-test during start-up and brings the system to secure state. In case of Self Test failure, TOE remains in secure state. The TOE provides accurate date and time from internal clock. The system clock can also be synchronized with an NTP server (NTP server is outside the scope of TOE). The TOE routing functions operate in an isolated environment thus protecting any accidental or intentional interference by others.

1.5.2.7 Cryptographic Support (TSF)

The TOE supports cryptography for secure communication and protection of information on Management interface. The TOE uses SSHv2 protocol for allowing remote clients for logging through CLI. SSHv2 provides encryption methods to create a secure channel of communication. SSHv2 encrypts the data flowing through the session with the help of a shared secret key.

1.5.3 Summary of items out of the TOE boundary

The following items are out of the scope of the evaluation:

- All hardware
- External servers (NTP, RADIUS, TACACS, SNMP, Syslog servers)
- Use of the serial port.
- Use of SNMP.
- Telnet is a filtered service. Use of Telnet by default it is disabled.
- FTP is a filtered service. Use of FTP by default it is disabled.
- Non-security features like IPv4/IPv6, MPLS, Routing Protocols, Layer 2, QoS.

2. CC CONFORMANCE

CC identification:

[CC1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model April 2017 Version 3.1 Revision 5 Final CCMB-2017-04-001

[CC2] Common Criteria for Information Technology Security Evaluation Part 2: Introduction and general model April 2017 Version 3.1 Revision 5 Final CCMB-2017-04-002

CC Part 2 (Version 3.1, Revision 5, April 2017) extended due to the use of the components FPT_TST_EXT, FCS_SSHC_EXT and FCS_SSHS_EXT

[CC3] Common Criteria for Information Technology Security Evaluation Part 3: Introduction and general model April 2017 Version 3.1 Revision 5 Final CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation, April 2017 Version 3.1, Revision 5, Final CCMB-2017-04-004.

This ST does not claim conformance to any PPs.

This ST and the TOE described is CC Part 2, CC Part 3 (version 3.1 Revision 5) conformant and meet EAL 3 certification requirements.

This ST and the TOE described is also conformant to the following extended components:
CC Part 2 (version 3.1 Revision 5) extended due to the use of the components FPT_TST_EXT, FCS_SSHC_EXT and FCS_SSHS_EXT.

3. SECURITY PROBLEM DEFINITION

Security Problem Definition describes:

- Assumptions related to TOE's operational environment to provide security functionality.
- Threats countered by TOE to protect itself and the environment in which it operates.
- Organizational policies that TOE must enforce.

3.1 Assumptions

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

3.1.1 Physical Assumptions

Assumption (Physical)	Assumption Description
A.ACCESS	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access to TOE.

Table 2: TOE Physical Assumption

3.1.2 Personnel Assumptions

Assumption (Personnel)	Assumption Description
A.COMP_NOEVIL	The authorized users of TOE will be trained and competent to use TOE, and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Table 3: TOE Personal Assumption

3.1.3 IT Environment Assumptions

Assumption (Operations)	Assumption Description
A.EXTAUTH	External authentication services will be available via RADIUS.
A.TIME	External NTP services will be available.
A.NWCOMP	The network components that access the management interface of the TOE will be located within a controlled and secure environment. The authorized users of the components will not be willfully negligent or hostile.
A.LIMITED_FUNCTIONALITY	The TOE is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).

Assumption (Operations)	Assumption Description
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the TOE to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the TOE, destined for another network entity, is not covered by this ST. It is assumed that this protection will be covered by for particular types of network devices (e.g, firewall).

Table 4: TOE IT Environment Assumption

3.2 Threats

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset. Threat agents are entities that can adversely act on assets – the threat agents in the threats below are unauthorized user, network attacker, and authorized user. Assets are entities that can be user’s data or TOE data which provides network services to the users. Adverse actions are unauthorized changes to configuration; both network routing configuration and management configuration resulting into loss of user data or disruption in the services provided to the users.

The TOE communicates with other network devices and other network entities. The endpoints of this communication can be geographically and logically distant and may pass through a variety of other systems. The intermediate systems may be un-trusted providing an opportunity for unauthorized communication with the network device or for authorized communication to be compromised. In a network, IP packets are exposed to incorrect routing caused by unauthorized changes to the TOE configuration. The security functionality of the network device must be able to protect any critical network traffic (administration traffic, authentication traffic, etc.).

The primary threats to TOE communications addressed in this ST document focus on an external, unauthorized entity attempting to access, modify, or otherwise disclose the critical network traffic. A poor choice of cryptographic algorithms along with weak administrator credentials, such as an easily guessable password or use of a default password, will allow a threat agent unauthorized access to the TOE. Weak or no cryptography provides little to no protection of the traffic allowing a threat agent to read, manipulate and/or control the critical data with little effort.

Lack of secure storage and improper handling of credentials and data, such as unencrypted credentials inside configuration files or access to secure channel session keys, can allow an attacker to not only gain access to the TOE, but also compromise the security of the network through seemingly authorized modifications to configuration. These attacks allow an unauthorized entity to gain access and perform administrative functions using the Security Administrator’s credentials and to intercept all traffic as an authorized endpoint. This results in difficulty in detection of security compromise and in reconstruction of the network, potentially allowing continued unauthorized access to administrator and device data.

Auditing of TOE activities is a valuable tool for administrators to monitor the status of the device. It provides the means for administrator accountability, security functionality activity reporting, reconstruction of events, and problem analysis. Processing performed in response to TOE activities may give indications of a failure or compromise of the security functionality. When indications of activity that impact the security functionality are not generated and monitored, it is possible for such activities to occur without administrator awareness. Further, if records are not generated and retained, reconstruction of the network and the ability to understand the extent of any compromise could be negatively affected. Additional concerns are the protection of the audit data that is recorded from alteration or unauthorized deletion.

TOE Failures could result in a compromise to the security functionality of the device. The TOE must ensure the reliability of the device’s security functionality in case it fails during start-up or during operations and recovers the TOE configuration on re-start.

Following are the threats addressed by TOE and its operational environment. The assumed level of expertise of the attacker for all the identified threats is BASIC.

Threat Name	Threat Description
T.NETWORK_DATA_FLOW	An unauthorized entity may disrupt the TOE operation or hamper its security mechanism, so that it can interrupt the network data flow.
T.UNAUTH_ACCESS	An unauthorized user may get access to TOE security functions and data to disrupt the security function of TOE by changing the configuration data.
T.UNAUTH_APPL	An unauthorized process or application may get access to TOE security functions and data to disrupt the security function of TOE by changing the configuration data.
T.INTERCEPT	Network traffic may be intercepted and unauthorized changes to management traffic from or to the TOE may be done.
T.CONFIG_LOSS	Failure of network components may lead to loss of configuration data which may not be restored immediately.
T.UNIDENTIFIED_ACTIONS	Unauthorized changes to the TOE configurations and other management information may not be detected.

Table 5: Threat Description addressed by TOE

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.

Objective Name	Objective Definition
O.NW_PKT_ROUTE	The TOE must ensure that network packets from source are routed to destination as per the routing procedures and available routing information.
O.PROTECT	The TOE must check integrity of its security function during start-up through self test procedure. The TOE must protect against unauthorized accesses and disruptions of TOE security functions and data – by isolating user and control data planes.
O.EADMIN	The TOE must provide services that allow effective management of its functions and data.
O.ACCESS_CONTROL	The TOE must restrict access to TOE security functions and data to authorized users and processes (applications).
O.ROLBAK	The TOE must enable rollback of router configurations to a known state.
O.AUDIT	The TOE must generate audit records providing the identity of users performing the event and its time.
O.CONN	The TOE must limit the IP addresses from which an administrator is able to manage the TOE and from which control data is accepted.
O.ENCRYPT	The TOE must provide Encryption of management data in a remote management session.

Table 6: Security Objectives Description for TOE

4.2 Security Objectives for the Environment

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

Environmental Objective Name	Environmental Objective Definition
OE.EXT_AUTH	External authentication services must be available via a RADIUS server within internal trusted network.
OE.TIME_SYNC	NTP server must be available within internal trusted network to provide accurate/synchronized time services to the router.
OE.PHYSICAL	The TOE must be protected from any physical attack.
OE.ADMIN	Authorized users must be trained and follow all administrator guidance.
OE.NWCOMP	The IT environment network components that have access to the management interface of the TOE must be protected.

Environmental Objective Name	Environmental Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

Table 7: Security Objectives for Environment Description for TOE

5. Extended Component Definition

TOE supports extended components which are not part of existing CC Part 2. The extended component is part of TOE Security Functional Requirement (SFR) with an extension "_EXT" to TOE SFR name. The extended SFR is modeled using SFR included in CC Part 2.

In this ST, the extended SRF is part of the identified class of requirements FCS and FPT. The extended SFR dependencies on other SRF, Management requirements, and Audit requirements are identified in 5.1.2 section.

5.1Requirement for Extended Components

Class of Requirement FPT

In order to check the integrity of security function of the TOE, the TOE performs self-test at time of start-up.

Class of Requirement FCS

In order to have a secure communication channel between TOE and remote terminals for administration, SSH protocol is used. SSH uses two way authentications between TOE and remote terminal to provide secure communication channel so that it can prevent any attack to disrupt the management interface information or TOE configurations.

5.2Definition

This SFR is taken from collaborated Protection Profile for Network Devices version 1.0. It is defined as a requirement specific to SSH protocol supported by the TOE.

5.3 FPT_TST_EXT.1 Self Test

Family Behavior

The component in this family addresses the requirements for self-testing the TSF for selected correct operation.

Component Leveling

FPT_TST_EXT: Self Test
1

FPT_TST_EXT.1 The TSF shall run a suite of self-tests during initial start-up to demonstrate the correct operation of the TSF therefore ensuring TOE integrity.

Management: FPT_TST_EXT.1

None

Audit: FPT_TST_EXT.1

The following action should be auditable if FAU_GEN Security audit data generation is included in ST:

a) Self-Tests results.

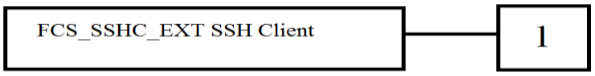
Hierarchical to:	No other components
Dependencies:	None

5.4 FCS_SSHC_EXT.1 SSH Client

Family Behavior

The component in this family addresses the ability for a client to use SSH to protect data between the client and a server using the SSH protocol.

Component Leveling



FCS_SSHC_EXT.1 SSH Client requires that the client side of SSH be implemented as specified.

Management: FCS_SSHC_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_SSHC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of SSH session establishment.
b) SSH session establishment
c) SSH session termination

FCS_SSHC_EXT.1 SSH Client Protocol

Hierarchical to:	No other components
Dependencies:	FCS_COP.1.1 Cryptographic operation (AES Data Encryption/Decryption; Signature Verification; Hash Algorithm)

5.5 FCS_SSHS_EXT.1 SSH Server Protocol

Family Behavior

The component in this family addresses the ability for a server to offer SSH to protect data between the client and a server using the SSH protocol.

Component Leveling

FCS_SSHS_EXT.1 SSH Server requires that the server side of SSH be implemented as specified.

Management: FCS_SSHC_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_SSHS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of SSH session establishment.
b) SSH session establishment
c) SSH session termination

FCS_SSHS_EXT.1	**SSH Server Protocol**

Hierarchical to:	No other components
Dependencies:	FCS_COP.1.1 Cryptographic operation (AES Data Encryption/Decryption; Signature Verification; Hash Algorithm)

6. IT SECURITY REQUIREMENTS

6.1 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**.

- 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 within square brackets*].

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

- The **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.

6.2 Security Functional Requirements

This section describes the Security Functional Requirements (SFRs) for the TOE, organised by CC class. SFRs implemented by the TOE are identified in the Table No 8 below. In the subsequent sections, they are further described in details.

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)
	Audit review (FAU_SAR.1)
	Restricted Audit review (FAU_SAR.2)
	Potential violation analysis (FAU_SAA.1)
	Protected audit trail storage (FAU_STG.1)

Security Functional Class	Security Functional Components
User data protection (FDP)	Subset information flow control (FDP_IFC.1)
	Simple security attributes (FDP_IFF.1)
	Rollback (FDP_ROL.1)
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Specification of secrets (FIA_SOS.1)
	User authentication before any action (FIA_UAU.2)
	User identification before any action (FIA_UID.2)
	Authentication failure (FIA_AFL.1)
	Multiple authentication mechanisms (FIA_UAU.5)
Security management (FMT)	Static attribute initialisation (FMT_MSA.3)
	Management of TSF data (Router configuration) (FMT_MTD.1a)
	Management of TSF data (User attributes) (FMT_MTD.1b)
	Management of TSF data (Audit logs) (FMT_MTD.1c)
	Management of TSF data (Date/time) (FMT_MTD.1d)
	Management of TSF data (Sessions) (FMT_MTD.1e)
	Management of TSF data (Router routing) (FMT_MTD.1f)
	Specification of Management Functions (FMT_SMF.1)
	Specification Management Roles (FMT_SMR.1)
Protection of the TSF (FPT)	Time stamps (FPT_STM.1)
	Self Test (FPT_TST_EXT.1)
	Fail Secure (FPT_FLS.1)
TOE access (FTA)	TOE session establishment (FTA_TSE.1)
	Limit multiple concurrent sessions (FTA_MCS.1)
	Session Termination on Inactivity (FTA_SSL.3)
Cryptographic support (FCS)	Cryptographic key generation (FCS_CKM.1)
	Cryptographic key destruction (FCS_CKM.4)
	Cryptographic operation (FCS_COP.1)
	FCS_SSHC_EXT.1 : SSH
	FCS_SSHS_EXT.1 : SSH

Table 8: Security Function Requirement for TOE

6.2.1 Audit (FAU)

6.2.1.1 Security alarms (FAU_ARP.1)

FAU_ARP.1.1

The TSF shall take [the following actions: generate an alarm, create a log entry and lock user account for a specified time] upon detection of a potential security violation.

6.2.1.2 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~~ Note: start up and shut down of the audit function will not be captured in Audit Log as Audit function will always be on;
b) All auditable events for the [not specified] level of audit specified in Table 9; and
c) [User login/logout;
d) Login failures;
e) Committing the TOE configuration;
f) Alarms generated during any operation].

S.N.	SFR Family	Description	Auditable Event
1.	FAU_ARP.1	Security alarms	Actions taken due to potential security violations.
2.	FAU_GEN.1	Audit data generation	None (CC Part-2, Page 31)
3.	FAU_GEN.2	User identity association	None (CC Part-2, Page 31)
4.	FAU_SAR.1	Security Audit review	Reading of information from the audit records.
5.	FAU_SAR.2	Restricted Audit review	None
6.	FAU_SAA.1	Potential violation analysis	a) Enabling and disabling of any of the analysis mechanisms; b) Automated responses performed by the tool.
7.	FAU_STG.1	Protected audit trail storage	None (CC Part-2, Page 41)
8.	FDP_IFC.1	Subset information flow control	None (CC Part-2, Page 65)
9.	FDP_IFF.1	Simple security attributes	None
10.	FDP_ROL.1	Rollback	All successful rollback operations.
11.	FIA_ATD.1	User attribute definition	None. (CC Part-2, Page 91)
12.	FIA_SOS.1	Specification of secrets	Change of any tested secret (password).

S.N.	SFR Family	Description	Auditable Event
13.	FIA_UAU.2	User authentication before any action	Unsuccessful use of the authentication mechanism.
14.	FIA_UID.2	User identification before any action	Unsuccessful use of the user identification mechanism, including the user identity provided.
15.	FIA_AFL.1	Authentication failure	a) Detect 3 consecutive unsuccessful authentication attempts of the same user account and the actions taken (lock the user account).
16.	FIA_UAU.5	Multiple authentication mechanisms	The final decision on authentication.
17.	FMT_MSA.3	Static attribute initialization	a) Modifications of the default setting of permissive or restrictive rules. b) All modifications of the initial values of security attribute.
18.	FMT_MTD.1a	Management of TSF data (Router configuration)	All modifications to the values of Router configuration data.
19.	FMT_MTD.1b	Management of TSF data (User attributes)	All modifications to the values of User attribute data.
20.	FMT_MTD.1c	Management of TSF data (Audit logs)	All attempts to modify or delete to the values of Audit logs data.
21.	FMT_MTD.1d	Management of TSF data (Date/time)	All modifications to the values of NPT server address and System clock data.
22.	FMT_MTD.1e	Management of TSF data (Sessions)	All modifications to the rules to establish management sessions.
23.	FMT_MTD.1f	Management of TSF data (Router routing)	All modifications to the values of Router's routing table data.
24.	FMT_SMF.1	Specification of Management Functions	Use of the management functions.
25.	FMT_SMR.1	Specification Management Roles	Modifications to the group of users that are part of a role.
26.	FPT_STM.1	Time stamps	Changes to the time.
27.	FPT_TST_EXT.1	Self Test	Self Test successful results.
28.	FPT_FLS.1	Fail Secure	None
29.	FTA_TSE.1	TOE session establishment	Denial of a session establishment due to the session establishment mechanism.
30.	FTA_MCS.1	Limit multiple concurrent sessions	Rejection of a new session based on the limitation of multiple concurrent sessions.
31.	FTA_SSL.3	Session Termination on Inactivity	Termination of an interactive session due to user inactivity.

S.N.	SFR Family	Description	Auditable Event
32.	FCS_CKM.1	Cryptographic key generation	None
33.	FCS_CKM.4	Cryptographic key destruction	None
34.	FCS_COP.1	Cryptographic operation	None
35.	FCS_SSHC_EXT.1 : SSH	SSH Client Protocol	CLI command to initiate SSH session along with user identity and timestamp.
36.	FCS_SSHS_EXT.1 : SSH	SSH Server Protocol	a) Failure to establish an SSH Session. b) Establishment and Termination of SSH Session.

Table 9: Auditable Events

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, event and subject identity (if applicable);
b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP~~/ST [no additional information].

6.2.1.3 User identity association (FAU_GEN.2)

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.

6.2.1.4 Audit review (FAU_SAR.1)

FAU_SAR.1.1

The TSF shall provide [System-Admin, Root-System] 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.

6.2.1.5 Restricted Audit review (FAU_SAR.2)

FAU_SAR.2.1

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

6.2.1.6 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 enforcement of the SFRs.

FAU_SAA.1.2

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

a) Accumulation or combination of [failed authentication attempt events] known to indicate a potential security violation;
b) [No other events].

6.2.1.7 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1

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

FAU_STG.1.2

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

6.2.2 User data protection (FDP)

6.2.2.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1

The TSF shall enforce the [ACL SFP] on

a) [subjects: Unauthenticated external IT entities that send and receive packets through the TOE to one another;
b) Information (IP packets): Network packets sent through the TOE from one subject to another;
c) operation: Route packets or drop packets].

6.2.2.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1

The TSF shall enforce the [ACL SFP] based on the following types of subject and information security attributes: [

a) subject security attributes:

- presumed address

b) information security attributes:
   - presumed address of source subject
   - presumed address of destination subject
   - transport layer protocol
   - network layer protocol
   - TOE interface on which packet arrives and departs]

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) [subjects on a network can cause packets to flow through the TOE to another connected network if:

- all the packet security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the packet security attributes, created by the authorized user;
- the presumed address of the source subject, in the packet, is consistent with the network interface it arrives on;
- and the presumed address of the destination subject, in the packet, can be mapped to a configured next hop].

FDP_IFF.1.3

The TSF shall enforce the [no additional ACL SFP rules].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules that explicitly authorize information flows].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [no additional rules that explicitly deny information flows].

6.2.2.3 Basic Rollback (FDP_ROL.1)

FDP_ROL.1.1

The TSF shall enforce [the management function to modify router configuration as specified under (FMT_SMF.1)] to permit the rollback of the [committed configuration change] on the [Router].

FDP_ROL.1.2

The TSF shall permit operations to be rolled back within the [selected any of the saved configuration].

6.2.3 Identification and authentication (FIA)

6.2.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:
[For interactive users:

a) User identity
b) Privilege levels
c) Password

For neighbour routers:

a) IP address
b) Password]

6.2.3.2 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [password length of 8-16 characters with at least one change of character set (upper, lower, numeric, special character) for interactive users].

6.2.3.3 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.

6.2.3.4 User identification before any action (FIA_UID.2)

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.

6.2.3.5 Authentication failure (FIA_AFL.1)

FIA_AFL.1.1

The TSF shall detect when [3] unsuccessful authentication events occur related to [login of users].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [lock the user account for a specified period which can be un-locked by the Root-System; never lock Root-System account].

6.2.3.6 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1

The TSF shall provide [internal password mechanism and external server (RADIUS/TACACS) mechanism to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [authentication mechanism specified by System-Admin, Root-System].

6.2.4 Security management (FMT)

6.2.4.1 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1
The TSF shall enforce the [ACL SFP] to provide [permissive] default values for security attributes that are used to enforce the SFP.

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

6.2.4.2 Management of TSF data (Router configuration) FMT_MTD.1a

FMT_MTD.1.1a

The TSF shall restrict the ability to [modify] the [router configuration data] to [System-Admin, Root-System].

6.2.4.3 Management of TSF data (User attributes) (FMT_MTD.1b)

FMT_MTD.1.1b

The TSF shall restrict the ability to [modify] the [user account attributes] to [Root-System].

6.2.4.4 Management of TSF data (Audit logs) (FMT_MTD.1c)

FMT_MTD.1.1c

The TSF shall restrict the ability to [modify or delete] the [audit logs] to [None].

6.2.4.5 Management of TSF data (Date/time) (FMT_MTD.1d)

FMT_MTD.1.1d

The TSF shall restrict the ability to [modify] the [NTP Server address and system clock] to [System-Admin, Root-System].

6.2.4.6 Management of TSF data (Sessions) (FMT_MTD.1e)

FMT_MTD.1.1e

The TSF shall restrict the ability to [modify, delete] the [rules that restrict the ability to establish management sessions] to [Root-System].

6.2.4.7 Management of TSF data (Router routing data) (FMT_MTD.1f)

FMT_MTD.1.1f

The TSF shall restrict the ability to [modify, delete] the [router's routing data] to [System-Admin, Root-System].

6.2.4.8 Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the privilege levels to differentiate [Root-System, System-Admin and Operator]

S.N.	Privilege Level	User Role	User Privileges/Functions Performed
1.	1	operator	User with "operator" role privileges can perform following functions: • View router configurations only. • Change own password.
2.	2	sysadmin	User with "sysadmin" role privileges can perform following functions: • View router configurations. • Change own password. • View audit logs.

S.N.	Privilege Level	User Role	User Privileges/Functions Performed
			• Configure and modify router interfaces and routing protocols, hence manage routing tables. • Configure RADIUS/TACACS for user authentication. • Configure external syslog server information on the Router. • Configure, modify system date and time. • Configure NTP client. • Configure, modify and apply information flow control attributes (ACL Filter and Rules) on TOE interfaces. • Configure or modify time limit of user inactivity. • Save Router configurations to a configuration file.
3.	3	rootsystem	User with “rootsystem” role can perform following functions: • View router configurations. • Change own password. • View audit logs. • Configure and modify router interfaces and routing protocols, hence manage routing tables. • Configure RADIUS/TACACS for user authentication. • Configure external syslog server information on the Router. • Configure, modify system date and time. • Configure NTP client and server. • Configure, modify and apply information flow

S.N.	Privilege Level	User Role	User Privileges/Functions Performed
			control attributes (ACL Filter and Rules) on TOE interfaces. • Configure or modify time limit of user inactivity. • Save Router configurations to a configuration file. • Can reset router to factory setting. • Can load/rollback a saved configuration file. • FTP configuration files to/from external machine. • Create, modify and delete users and its roles (*sysadmin,operator*) /privileges/passwords. Can not create a user with *rootsystem* role. • Configure or modify the number of concurrent session of a user. • Configure or modify the number of concurrent session of a user. • Configure Management ACL white-list to control management sessions.

Table 10: TOE user's privileges and roles

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.4.9 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

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

- Configure, modify, save Router configuration data including rollback of router configurations.
- Configure or modify date and time.
- Configure or modify information flow control attributes (ACL Filter and Rules).

- Create, modify and delete user attributes and privileges to authenticate and identification of users before providing access to the system.
- Configuring User Login control (identification and authentication mechanism through local, or RADIUS/TACACS).
- Configure or modify time limit of user inactivity.
- Configure or modify the number of concurrent session of a user.
- Configure or modify number of unsuccessful consecutive login attempts before locking the user account.
- Configure external authentication server (RADIUS/TACACS).
- Configuring NTP client/server.
- Configuring external Syslog server.
- Manage routing tables.
- Manage the audit logs.
- Controlling management sessions.]

The user privilege/role to perform the above mentioned security function is defined in table 10 of section 6.2.4.8

6.2.5 Protection of the TOE security functions (FPT)

6.2.5.1 Time stamps (FPT_STM.1)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.2.5.2 Self Test (FPT_TST_EXT.1)

FPT_TST_EXT.1.1

The TSF shall run a suite of self tests [during start-up] to demonstrate the correct operation of TSF [

- Routing Software Integrity checks by verifying Data Plane, Control Plane, Management Plane binaries for any tampering or corruption.

].

6.2.5.3 Fail Secure (FPT_FLS.1)

FPT_FLS.1

The TSF shall preserve a secure state when the following types of failures occur: [

- Self Test failure – During start-up if software integrity checks are failed then the further software start-up is prevented and system does not provide any services. In this situation, System Administrator intervention is required to re-install the Routing software files.

].

6.2.6 TOE access (FTA)

6.2.6.1 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1

The TSF shall be able to deny session establishment based on [presumed origin of the request].

6.2.6.2 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

FTA_MCS.1.1

The TSF shall restrict the maximum number of concurrent sessions of the same user.

FTA_MCS.1.2

The TSF shall enforce by default, a limit of [10 total maximum number of sessions per user who is not Root-System, which is configurable. The Root-System can have only one session.]

6.2.6.3 Session Termination on Inactivity (FTA_SSL.3)

FTA_SSL.3.1

The TSF shall terminate an interactive session after [30 minutes of user inactivity, inactive duration can be configured by System-Admin or Root-System].

6.2.7 Cryptographic Support (FCS)

6.2.7.1 Cryptographic key management (FCS_CKM.1)

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:

- DSA (Digital Signature Algorithm) schemes using cryptographic key sizes of 1024-bit that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”,
- RSA (Rivest-Shamir-Adleman Algorithm) schemes using cryptographic key sizes of 2048-bit that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”,]

~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].~~

6.2.7.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1

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

6.2.7.3 Cryptographic key operation (FCS_COP.1)

Remote administration by SSH

FCS_COP.1.1

The TSF shall perform [encryption/decryption of remotely authorized user sessions] in accordance with a specified cryptographic algorithm [for host key generation: Digital Signature Standard as specified in FIPS PUB 186-4 with key length 1024 bits; for asymmetric encryption: RSA as specified in FIPS PUB 186-4 with key length 2048 bits; for key exchange: diffie-hellman-group-exchange-sha256 as per RFC 4419; for user authentication: Digital Signature Algorithm (DSA) as specified in FIPS PUB 186-4;for symmetric encryption: Advanced Encryption Standard (AES) used in [CTR] mode with key lengths 128, 192 or 256 bits that meet the following: AES as specified in ISO 18033-3, [CTR as specified in ISO 10116]; for data integrity check: Hash Message Authentication Code - Secure Hash Algorithm 2 (HMAC-SHA 2) with block size 256/512 as specified in FIPS PUB 180-4.] ~~and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.

6.2.7.4 SSH Client Protocol (FCS_SSHC_EXT.1)

FCS_SSHC_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254].

FCS_SSHC_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: password- based.

FCS_SSHC_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [AES-128-CTR, AES-192-CTR and AES-256-CTR].

FCS_SSHC_EXT.1.5

The TSF shall ensure that the SSH transport implementation uses [RSA-2048, DSA-1024] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [HMAC-SHA 2 256/512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7

The TSF shall ensure that [diffie-hellman-group-exchange-sha256] are the only allowed key exchange methods used for the SSH protocol.

6.2.7.5 SSH Server Protocol (FCS_SSHS_EXT.1)

FCS_SSHS_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253 and 4254].

FCS_SSHS_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: password- based.

FCS_SSHS_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [AES-128-CTR, AES-192-CTR and AES-256-CTR].

FCS_SSHS_EXT.1.5

The TSF shall ensure that the SSH transport implementation uses [RSA-2048, DSA-1024] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [HMAC-SHA 2 256/512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7

The TSF shall ensure that [diffie-hellman-group-exchange-sha256] are the only allowed key exchange methods used for the SSH protocol.

6.3 Security Assurance Requirements

The following Table No 11 describes the TOE security assurance requirements drawn from Part 3 of the CC.

Assurance Class	**Assurance Components**
Security Target (ASE)	*ST introduction (ASE_INT.1)*
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Conformance Claim (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	*Security architecture description (ADV_ARC.1)*
	Functional specification with complete summary (ADV_FSP.3)
	Architectural design (ADV_TDS.2)
Guidance documents (AGD)	*Operational user guidance (AGD_OPE.1)*
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	*Authorisation controls (ALC_CMC.3)*
	Implementation representation CM coverage (ALC_CMS.3)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
Tests (ATE)	*Analysis of coverage (ATE_COV.2)*
	Testing: basic design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	*Vulnerability analysis (AVA_VAN.2)*

Table 11: TOE Security Assurance Requirement

7. TOE SUMMARY SPECIFICATION

7.1 TOE Security Functions

7.1.1 Information Flow Function

FDP_IFC.1 Subset information flow control and FDP_IFF.1 Simple security attributes

The TOE processes the network traffic on incoming port and forwards them to destination port based on available routing information. Network traffic represents packet flows between source and destination network elements. The specific routing of traffic is based on the routing information data that has been created by the TOE users (static) or has been collected (e.g., ARP, BGP) dynamically from neighbouring routers as defined by the TOE users. The routing decision is based on the routing table database along with source and destination IP address of the packet. The TOE accepts routing information only from trusted routers with IP configured by the administrators.

The TOE controls the information flow by filtering and applying a set of rules based on source IP address, destination IP address, source port, destination port, type of protocol used defined by ACL SFP policy on ingress as well as egress ports. It allows the packets coming from defined IP address entities and going to identified IP address entities in the network based on the policy. IP packets which do not match any configuration entries defined in ACL will be dropped. In this way, an unauthorised entity is prevented from communicating with other entities in the network through TOE.

FDP_ROL.1 Basic rollback

CROS configuration can be saved locally in a configuration files and can be rolled back to any of them on request.

When the system boots up, it loads its primary configuration. The system can be brought to factory setting default by Root-System. Root-System can also load/rollback a saved configuration file to bring the TOE to a known configuration.

7.1.2 Identification and Authentication Function

FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes: user name, authentication data (password) and privilege (Level). The System-Admin or Root-System can configure TOE to handover the authentication process to a RADIUS/TACACS server.

For neighbor routers, which cannot access the admin interface, the attributes maintained are IP address and password, which are used to authenticate the remote router for exchange of routing table information.

FIA_SOS.1 Verification of secrets

Locally stored authentication data for password authentication is a case-sensitive, alphanumeric value. The password has a minimum length of 8 ASCII characters with at least one change of character set (upper, lower, numeric, special character), and can be up to 16 ASCII characters in length.

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 CROS software supports three methods of user authentication: local password authentication and external authentication server Remote Authentication Dial In User Service (RADIUS) or TACACS.

With local password authentication, a password is configured for each user allowed to log into the Router. RADIUS is an authentication method for validating users who attempt to access the router. Both are distributed client/server systems—the RADIUS clients run on the appliance, and the server runs on a remote network system in the IT environment.

If the user identity specified is defined locally, the TOE can successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Alternately, if the TOE is configured to work with a RADIUS/TACACS (by System-Admin, Root-System), the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless user authentication mechanisms, no administrative actions are allowed until successful authentication is done as an authorized administrator.

FIA_AFL.1 Authentication failure

After 3 (configurable by Root-System) consecutive login failures for a particular user, the account will be locked for a specified period and Root-System can unlock the account.

7.1.3 Security Management Function

FMT_MSA.3 Static attribute initialisation

The TOE boots up with default security attributes, some of which can only be configured by Root-System user by configuring an ACL rule to restrict/allow network access to the TOE. As default, allows SSH connection to access the TOE from serial port or a predefined subnet. The TOE allows only authorized administrators (Root-System, System-Admin) depending on their privileges to create alternative policy over and above default attributes/policy to access TOE.

FMT_MTD.1a Management of TSF Data (Router Information)

The TOE restricts the ability to administer the router configuration data based on the privilege level of users. The CLI provides a text-based interface from which the router configuration can be managed and maintained. From this interface all TOE functions, such as BGP, OSPF and MPLS protocols can be managed and including date/time. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

FMT_MTD.1b Management of TSF Data (User Data)

The TOE restricts the ability to administer user data to Root-System. The CLI provides Root-Admin users with a text based interface from which all user data can be managed. From this interface new accounts can be created, and existing accounts can be modified or deleted. This interface also provides administrator an ability to configure an external authentication server, such as a RADIUS/TACACS server. When this is assigned, a user can be authenticated to the external server instead of directly to the TOE.

FMT_MTD.1c Management of TSF Data (Audit logs)

The TOE can be configured to transfer audit logs automatically to external syslog server by System-Admin or Root-System. Audit logs can not be modified or deleted by any of the administrator or user.

FMT_MTD.1d Management of TSF Data (Date/time)

The TOE will allow System-Admin or Root-System to modify/update the date/time setting on the device.

FMT_MTD.1e Management of TSF Data (Sessions)

The TOE will allow Root-System to create, delete or modify the policy which controls the presumed address from which management sessions can be established.

FMT_MTD.1f Management of TSF Data (Router routing data)

The TBR shall restrict the ability to modify and delete the routing data to System-Admin or Root-System.

FMT_SMF.1 Management of Security Functions

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

a) Create, modify and delete User attributes and privileges;

b) Configure User login control (Local or RADIUS/TACACS);

c) User authentication (authentication data, roles);

d) Router configuration (date/time, configuration rollback, ACL filter/Rules, and update/management of routing tables and deletion of routing information learned from the network);

e) Configure time limit for user inactivity.

f) Session establishment management/restrictions which depends on number of concurrent sessions of types of users and their privileges.

g) Configure the limit on unsuccessful consecutive login failures after which the login account is locked.

h) Configure NTP client/server and external RADIUS/TACACS, Syslog servers.

i) Audit management and review;

FMT_SMR.1 Security Roles

The TOE has privilege levels defined per user role. When a new user account is created, it must be assigned one of the user roles.

Operator Role: this role can view TOE status and statistics only in addition to change its own password.

System-Admin Roles:

a) create, modify, delete, save and view TOE configuration.

b) Change own password

c) modify date/time;

d) create or delete static routes and routing protocols

e) configure external authentication server (RADIUS/TACACS)

f) configure external syslog server

g) configure NTP client

h) configure and apply ACL rules

i) configure time limit of user inactivity

j) Can review the audit records

Root-System Roles:

Root-System has permission to all commands for System-Admin. In addition to that Root-System can perform configuration of Management ACL white-list, TOE user administration, reset router to factory setting, ftp configuration files and load a saved configuration file.

7.1.4 Audit Function

FAU_GEN.1 Audit data generation

CROS creates and stores audit records for the following events:

1. User login/logout;

2. Login failures;

3. SSH session establishment and termination;
4. Failure to set up SSH session;
5. Configuration is committed;
6. Configuration is changed.
7. Modification of date/time;
8. Alarms generated during any operation.

CROS shall also record Date and time of the above auditable event, event and subject identity (if applicable).

FAU_GEN.2 User identity association

CROS will associate Date and time of the event, event and subject identity causing the event.

FAU_SAR.1 Audit review

CROS provides System-Admin, Root-System users with the ability to display audit data from the CLI. CROS provides the ability to display audit records as complete files, or selective records based on user-defined filters.

FAU_SAR.2 Restricted Audit review

Audit log view shall be restricted to any other user except those who have been given the privilege to review.

FAU_STG.1 Protected audit trail storage

Audit records will be saved in files. The Root-System and System-Admin user may display the content of Audit logs on screen using CLI commands. There is no CLI command to edit or delete the Audit log files. Hence, they are protected from any modification or deletion.

FAU_ARP.1 Security alarms

While authenticating a user, an audit log message is generated and the user account is locked after 3 successive login failures and alarm is generated.

FAU_SAA.1 Potential violation analysis

CROS shall analyse the failed authentication attempts to identify activity indicating a potential violation. The potential violation is defined as 3 successive login failures, and the action taken is that the user account is locked for a specified period.

7.1.5 TOE Access Function

FTA_TSE.1 TOE session establishment

The TOE can be configured by Root-System such that users can only gain access from specific management networks/stations at specific IP addresses.

FTA_MCS.1 Maximum number of concurrent sessions

The TOE allows a maximum of 10 concurrent sessions for every user by default, which is configurable up to 32 for users who are not Root-System and a single session each for Root-System.

FTA_SSL.3 Session termination on user inactivity

The TOE will terminate a session after 30 minutes (configurable by System-Admin or Root-System) of inactivity.

7.1.6 Clock function

FPT_STM.1 Time stamps

The clock function of the TOE provides a source of date and time information, used in audit timestamps. The clock function is reliant on the system clock.

For better accuracy of timestamp and synchronization of time across devices in the IT environment, an external NTP server can be deployed. In such deployments the audit timestamps will be synchronized with external NTP servers, if configured (by Root-System).

7.1.7 TOE Self Test

FPT_TST_EXT.1 Self Test

At start-up, TOE performs the integrity check of Routing software executables to check the correct operation of the TOE. The TOE maintains a list of critical executable files along with their fingerprints. Any mismatch in fingerprints of these executable images and files is an indication of corruption or compromise. These files consist of control plane, data plane and management plane binaries. The TOE will compute the fingerprints of these files using MD5 and match them with the respective stored fingerprints before they are executed. Any mismatch in the fingerprints will trigger a failure and will prevent further software startup. In such a scenario, TOE does not provide any access or services.

7.1.8 Fail Secure

FPT_FLS.1 Fail Secure

The TOE remains in a secure state in case of Self Test failure during start-up and does not provide any services. The system can be rebooted or re-installed by TOE user to recover it.

7.1.9 Cryptographic Support for Protection of Management Interface Sessions

FCS_CKM.1 Cryptographic key management, FCS_CKM.4 Cryptographic key destruction, FCS_COP.1 Cryptographic key operation, FCS_SSHC_EXT.1 SSH Client Protocol, FCS_SSHS_EXT.1 SSH Server Protocol

The TOE protects remote user sessions over management interface from any cryptographic attack. The TOE uses Open SSHv2 protocol for allowing remote clients for logging through CLI. SSHv2 uses DSA/RSA key generation (conformant to FIPS PUB 186-4), session key using Diffie-Hellman Exchange Algorithm (diffie-hellman-group-exchange-sha256) and 128, 192 or 256 bits AES (CTR mode) for encryption. HMAC-SHA 2 256/512 is used for Data Integrity as specified in FIPS PUB 180-4. The keys are overwritten when new keys are generated.

8. 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

8.1 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.

8.1.1 Rationale for Security Objectives for the TOE

	T.NETWORK_DATA_FLOW	T.UNAUTH_ACCESS	T.UNAUTH_APPL	T.INTERCEPT	T.CONFIG_LOSS	T.UNIDENTIFIED_ACTIONS	A.ACCESS	A.COMP_NOEVIL	A.TIME	A.EXTAUTH	A.NWCOMP	A.LIMITED_FUNCTIONALITY	A.NO_THRU_TRAFFIC_PROTECTION
O.NW_PKT_ROUTE	✓												
O.PROTECT	✓	✓	✓										
O.EADMIN	✓				✓								
O.ACCESS_CONTROL	✓	✓	✓										
O.ROLBAK	✓	✓	✓		✓								
O.AUDIT	✓	✓	✓	✓		✓							
O.CONN		✓	✓	✓									
O.ENCRYPT		✓	✓	✓									

Table 12: TOE Security Objective Rationale

O.NW_PKT_ROUTE: This objective helps to counters the threat of disrupting TOE operation (T.NETWORK_DATA_FLOW) by malicious entity in the network.

O.PROTECT: This objective contributes to correct routing of information (T.NETWORK_DATA_FLOW) and prevention of disruption to TOE functions by users (T.UNAUTH_ACCESS) or processes (T.UNAUTH_APPL).

O.EADMIN: This objective is to provide effective management tools that assist in the correct routing of packets (T.NETWORK_DATA_FLOW) and to provide effective management tools that help to recover from failures (T.CONFIG_LOSS).

O.ACCESS_CONTROL: This objective addresses the need to protect the TOE's operations and data. This helps counter the threats of incorrect routing (T.NETWORK_DATA_FLOW), unauthorised access (T.UNAUTH_ACCESS and T.UNAUTH_APPL).

O.ROLBAK: The objective to restore previously saved configurations helps ensure correct routing of data (T.NETWORK_DATA_FLOW), and helps recover from loss of configuration data (T.CONFIG_LOSS) and helps recover from unauthorised changes (T.UNAUTH_ACCESS, T.UNAUTH_APPL).

O.AUDIT: This objective serves to discourage and detect inappropriate use of the TOE (T.UNIDENTIFIED_ACTIONS), and as such helps counter T.NETWORK_DATA_FLOW, T.UNAUTH_ACCESS, T.UNAUTH_APPL and T.INTERCEPT, which relate to inappropriate (deliberate or accidental) use of the TOE.

O.CONN: This objective helps to counter the threats relating to unauthorised modification by an attacker to the TOE configuration (T.UNAUTH_ACCESS & T.UNAUTH_APPL) by limiting the IP addresses from which the TOE accepts management and control traffic connections (T.INTERCEPT).

O.ENCRYPT: This objective helps to counter the interception of management data by encrypting the remote management data (T.INTERCEPT) and prevent the unauthorised access (T.UNAUTH_ACCESS, T.UNAUTH_APPL) to TOE.

8.1.2 Rationale for Security Objectives for the Environment

	T.NETWORK_DATA_FLOW	T.UNAUTH_ACCESS	T.UNAUTH_APPL	T.INTERCEPT	T.CONFIG_LOSS	T.UNIDENTIFIED_ACTIONS	A.ACCESS	A.COMP_NOEVIL	A.TIME	A.EXTAUTH	A.NWCOMP	A.LIMITED_FUNCTIONALITY	A.NO_THRU_TRAFFIC_PROTECTION
OE.EXT_AUTH		✓								✓			
OE.TIME_SYNC									✓				
OE.PHYSICAL							✓						
OE.ADMIN								✓					
OE.NWCOMP											✓		
OE.NO_GENERAL_PURPOSE												✓	
OE.NO_THRU_TRAFFIC_PROTECTION													✓

Table 13: TOE Security Objectives for Environment Rationale

OE.EXT_AUTH The objective to have an authentication server in the TOE environment which helps to counter the threat of unauthorised access enforcing authentication of users attempting to access to TOE security functions and data (T.UNAUTH_ACCESS), and supports the assumption that such a server is present (A.EXTAUTH).

OE.TIME_SYNC The objective to have an NTP server in the TOE environment which supports the assumption (A.TIME) that time services are available to provide the appliance with accurate/synchronised time information.

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

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

OE.NWCOMP The objective to protect those network components with access to the management interface of the TOE supports the assumption that these network components will be protected (A.NWCOMP).

OE.NO_GENERAL_PURPOSE The objective protects the TOE from performing any other function other than its intended operation, administration and its support functions (A.LIMITED_FUNCTIONALITY).

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not protect the traffic that traverse through it. It protects the traffic which is generated on or destined for the TOE, like management data, audit data, configuration data, etc. (A.NO_THRU_TRAFFIC_PROTECTION).

8.2 Rationale for Security 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. The functional requirements are mutually supportive, and their combination meets the security objectives. Table 12 demonstrate the relationship between the threats (T), assumptions (A) and the security objectives (O). Table 13 identifies relationship between the threats (T), assumptions (A) and the environmental objectives (OE). Table 14 illustrates the mapping between security functional requirements (SFRs) and security objectives (O) for the TOE. Together these tables demonstrate the completeness and sufficiency of the requirements.

	O.NW_PKT_ROUTE	O.PROTECT	O.EADMIN	O.ACCESS_CONTROL	O.ROLBAK	O.AUDIT	O.CONN	O.ENCRYPT
FAU_ARP.1		✓				✓		
FAU_GEN.1						✓		
FAU_GEN.2						✓		
FAU_SAA.1		✓				✓		
FAU_SAR.1						✓		
FAU_SAR.2						✓		
FAU_STG.1						✓		
FDP_IFC.1	✓							
FDP_IFF.1	✓							
FDP_ROL.1					✓			
FIA_ATD.1		✓		✓		✓		
FIA_AFL.1				✓				
FIA_SOS.1				✓				
FIA_UAU.2		✓		✓		✓		
FIA_UAU.5		✓		✓		✓		
FIA_UID.2		✓		✓		✓		
FMT_MSA.3	✓		✓	✓				

	O.NW_PKT_ROUTE	O.PROTECT	O.EADMIN	O.ACCESS_CONTROL	O.ROLBAK	O.AUDIT	O.CONN	O.ENCRYPT
FMT_MTD.1a	✓	✓						
FMT_MTD.1b		✓		✓				
FMT_MTD.1c						✓		
FMT_MTD.1d						✓		
FMT_MTD.1e				✓				
FMT_MTD.1f	✓							
FMT_SMF.1	✓	✓	✓	✓		✓		
FMT_SMR.1	✓	✓	✓	✓		✓		
FPT_TST_EXT.1		✓						
FPT_FLS.1		✓						
FPT_STM.1						✓		
FTA_TSE.1				✓			✓	
FTA_MCS.1				✓				
FTA_SSL.3				✓				
FCS_CKM.1				✓				✓
FCS_CKM.4				✓				✓
FCS_COP.1				✓				✓
FCS_SSHS_EXT.1				✓				✓
FCS_SSHC_EXT.1				✓				✓

Table 14: TOE Security Requirements Rationale

8.2.1 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. The functional requirements are mutually supportive, and their combination meets the security objectives. Table 10 and Table 11 demonstrate the relationship between the threats and assumptions and the security objectives. Table 12 illustrates the mapping between security functional requirements and security objectives for the TOE. Together these tables demonstrate the completeness and sufficiency of the requirements.

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

FAU_GEN.1 This component outlines what events must be audited, and aids in meeting O.AUDIT.

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.PROTECT and O.AUDIT.

FAU_SAR.1 This component requires that the audit trail can be read, and aids in meeting O.AUDIT.

FAU_SAR.2 This component requires that the audit trail can be read, and aids in meeting O.AUDIT.

FAU_STG.1 This component requires that unauthorized deletion of audit records does not occur, and thus helps to maintain accountability for actions, as required by O.AUDIT.

FDP_IFC.1 This component identifies the entities involved in the UNAUTHENTICATED information flow SFP (i.e. external IT entities sending packets), and aids in meeting O.NW_PKT_ROUTE.

FDP_IFF.1 This component identifies the conditions under which information is permitted to flow between entities (the UNAUTHENTICATED SFP), and aids in meeting O.NW_PKT_ROUTE.

FDP_ROL.1 This component allows previously saved router configurations to be restored, if primary configuration is corrupt, and aids in meeting O.ROLBAK.

FIA_ATD.1 This component specifies that individual user attributes are to be maintained and aids in meeting O.PROTECT, O.ACCESS_CONTROL and O.AUDIT.

FIA_AFL.1 This component protects against repeated unauthorized access attempts and hence helps meeting O.ACCESS_CONTROL.

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

FIA_UAU.2 This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access and aids in meeting O.PROTECT, O.ACCESS_CONTROL, and O.AUDIT.

FIA_UAU.5 This component was selected to ensure that appropriate authentication mechanisms can be selected. As such it aids in meeting objectives to restrict access O.PROTECT, O.ACCESS_CONTROL.AND O.AUDIT

FIA_UID.2 This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access O.PROTECT, O.ACCESS_CONTROL and O.AUDIT.

FMT_MSA.3 This component ensures that there is a default deny policy for the information flow control security rules. As such it aids in meeting O.NW_PKT_ROUTE. It also assists in effective management, and as such aids in meeting O.EADMIN AND O.ACCESS_CONTROL.

FMT_MTD.1a This component restricts the ability to modify routing configuration details, and as such aids in meeting O.NW_PKT_ROUTE, O.PROTECT.

FMT_MTD.1b This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.ACCESS_CONTROL and O.PROTECT.

FMT_MTD.1c This component restricts the ability to delete audit logs, and as such contributes to meeting O.AUDIT.

FMT_MTD.1d This component restricts the ability to modify the date and time, and as such contributes to meeting O.AUDIT.

FMT_MTD.1e This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.ACCESS_CONTROL.

FMT_MTD.1f This component restricts the ability to delete the routing data, and as such contributes to meeting O.NW_PKT_ROUTE.

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

FMT_SMR.1 Each of the components in the FMT class listed above relies on this component (apart from FMT_MSA.3). It defines the roles on which access decisions are based. As such it aids in meeting O. NW_PKT_ROUTE, O.PROTECT, O.EADMIN, O.ACCESS_CONTROL and O.AUDIT.

FPT_STM.1 This component ensures that reliable time stamps are provided for audit records and aids in meeting O.AUDIT.

FPT_TST_EXT.1 This component ensures that reliable self test are performed to ensure the integrity of TSF and aids in meeting O.PROTECT.

FPT_FLS.1 This component ensures that TOE remains in secure state in case self test fails and aids in meeting O.PROTECT.

FTA_TSE.1 This component limits the range of locations from which a user session can be established, and hence reduces the chance of unauthorized access. It aids in meeting O.ACCESS_CONTROL. It also aids in meeting O.CONN.

FTA_MCS.1 This component limits the number of sessions a user can establish, and hence reduces the chance of unauthorized access. It aids in meeting O.ACCESS_CONTROL.

FTA_SSL.3 This self-terminates idle sessions after a timeout, and hence reduces the chances of unauthorized access via unattended sessions. This helps meeting O.ACCESS_CONTROL.

FCS_CKM.1 This component defines cryptographic key management functions, namely the generation of keys. This key management secures the cryptographic operations. This helps in meeting O.ENCRYPT and O.ACCESS_CONTROL.

FCS_CKM.4 This Defines cryptographic key management functions, namely the destruction of keys. This key management secures the cryptographic operations. This helps in meeting O.ENCRYPT and O.ACCESS_CONTROL.

FCS_COP.1 This Defines the actual cryptographic operation, that secures the communication between TOE and users. This helps in meeting O.ENCRYPT and O.ACCESS_CONTROL.

FCS_SSHS_EXT.1 and FCS_SSHC_EXT.1: The SSH protocol is used to secure communications between the TOE and the endpoints; authentication of users; mainly for remote administration. Securing the communication channel provides interoperability and resistance to cryptographic attack by means of two-way authentication of each end-point. This helps in meeting O.ENCRYPT and O.ACCESS_CONTROL.

8.3 Rationale for Security Assurance Requirements (SAR)

Following are the Security Assurance Requirements selected for EAL3 assurance:

S.N.	Security Assurance Requirement/Components	Description/Rationale
1.	ADV_ARC.1 Security architecture description	*Security Architecture for CROS Software for CRAT-100/CRDT-100 Router* document describes the Security Architecture of TSF which can be analysed to assure that self-protection, domain separation and non-bypass-ability properties of TSF are achieved by the design and its correct implementation. Also, it describes that the Security Architecture design is consistent with TSF.
2.	ADV_FSP.3 Functional specification with complete summary	*Function Specification for CROS Software for CRAT-100/CRDT-100 Router* document provides the characteristics of all external TSF Interfaces (TSFI), such as, TSFI’s purpose, method of use, parameters, parameter descriptions, actions and error message descriptions. This document provides understanding and assurance how TSF meets the claimed SFRs with summary.
3.	ADV_TDS.2 Architectural design	*TOE Security Design for CROS Software for CRAT-100/CRDT-100 Router* document provides sufficient information to determine the TSF boundary, and to describe how the TSF implements the SFRs. It describes TOE at both Sub-system level as well as Module level details. It describes the Sub-system interfaces, Module Interfaces and communication between them. The level of assurance increases, as the design description details are provided from the general (subsystem level) to more (module level) detail.
4.	AGD_OPE.1 Operational user guidance	*User Manual for C-DOT CRAT-100/CRDT-100 Router* document provides guidelines to understand the TSF’s security functionality, instructions including warnings for its users to operate, configure, maintain and administrate TOE in a secure manner. It also specifies for each user their roles, user-accessible functions and privileges as per their group, such as, operator, System-Admin and Root-System. The main objective is to minimize the risk of human or other errors in operation that may deactivate, disable, or lead the TOE into an undetected insecure state.
5.	AGD_PRE.1 Preparative procedures	*Installation Manual for C-DOT CRAT-100/CRDT-100 Router* document describes all necessary steps for secure installation of the TOE. It also provides TOE administrator with all information for preparing an intended operational environment necessary to meet the security objectives of the

S.N.	Security Assurance Requirement/Components	Description/Rationale
		TOE.
6.	ALC_CMC.3 Authorisation controls	*Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router* document describes the Authorisation controls to propagate Configuration Items (CIs), changes to CIs and release of CIs into TOE. The CM manager ensures Authorisation Control is in place into the CM system to develop and maintain the TOE throughout its life cycle.
7.	ALC_CMS.3 Implementation representation CM coverage	*Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router* document describes the CM system to be followed to develop and maintain the TOE. The CM plan describes the convention followed to uniquely identify the TOE, Configuration Items (CIs) and Non Configuration Items (Non-CIs). The CM manager ensures that the CM system is in place to develop and maintain the TOE throughout its life cycle.
8.	ALC_DEL.1 Delivery procedures	*Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router* document describes the delivery procedure to be followed by developer to ensure delivery of TOE (New Released version or patches) to its consumer in a secure way. The necessary documents are part of delivery procedure, such as, Installation manual, Release Note so that the administrator has sufficient and necessary information to install the correct version of the TOE and bring it to in a secure state.
9.	ALC_DVS.1 Identification of security measures	The TOE development environment security measures and procedures to be followed to maintain the confidentiality and integrity of the TOE design and development is documented in *Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router* document. The Configuration Management (CM) manager ensures that the said procedures are followed and maintains the TOE development environment.
10.	ALC_LCD.1 Developer defined life-cycle model	The Life-Cycle-Model (LCM) to develop and maintain the TOE is documented in *Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router* document. The LCM assures that the TOE is developed and maintained throughout its life cycle in controlled and secured way.
11.	ATE_COV.2 Analysis of coverage	The analysis of the test coverage documented in *Test Case Document for CROS Software for CRAT-100/CRDT-100 Router* shall demonstrate that all the functional test cases corresponding to each of the TSFIs in the functional specification have been executed and all the TSFIs are successfully tested.
12.	ATE_DPT.1 Testing: basic design	The analysis of the depth of testing documented in *Test Case Document for CROS Software for CRAT-100/CRDT-100 Router* shall demonstrate that all the functional test cases corresponding to each of the TSF Sub-systems have been executed and all the TSF Sub-systems in the TOE design are successfully tested.

S.N.	Security Assurance Requirement/Components	Description/Rationale
13.	ATE_FUN.1 Functional testing	*Test Case Document for CROS Software for CRAT-100/CRDT-100 Router* document will provide test procedure for each of the test scenarios along with test environment, test condition, test data parameters and values so that one can perform an independent testing of each of the TSFIs and TSF Sub-systems. The test scenarios also capture any ordering dependencies on the results of other tests. In the Functional Test Report, each of the Test Cases has an expected result and actual result. These results are used for independently verifying the testing of TSFIs and TSF Sub-systems along with the test coverage analysis and depth of testing.
14.	ATE_IND.2 Independent testing – sample	The assurance gained through Function Testing, Test Coverage and Depth analysis is independently verified by executing a set of functional test cases by evaluator to confirm TSF operates as specified in design documents and as per guidance documents. For this, evaluator may create a new test case and execute apart from test cases provided by developer in *Test Case Document for CROS Software for CRAT-100/CRDT-100 Router*.
15.	AVA_VAN.2 Vulnerability analysis	The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE. The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Table 15: TOE SAR Rationale

Based on the threats defined according to the TOE environment, EAL3 assurance is selected as per CC Part 1 and CC Part 3 (Version 3.1, Revision 4) to establish a sufficient level of confidence in the security offered by the TOE. The TOE will be subject to independent vulnerability analysis for attack potential basic.

8.3.1 Dependencies Rationale

All functional and assurance requirements dependencies indicated in [CC2] and [CC3] have been satisfied, with the exception of the dependency of FMT_MSA.3 on FMT_MSA.1. The requirement for FMT_MSA.3 is included as a dependency from FDP_IFF.1, to specify how the security attributes associated with the information flow rules are initialised. The subsequent dependency from FMT_MSA.3 on FMT_MSA.1 allows for the specification of the management of the security attributes. However, for this TOE the management of the information flow security attributes is specified using FMT_MTD.1a. Therefore, there is no need to include FMT_MSA.1 as FMT_MTD.1a has satisfied the intent of the dependency. The extended component defined for SSH Server and Client Protocol (FCS_SSHS_EXT.1 and FCS_SSHC_EXT.1) has dependency on FCS_COP.1 for cryptographic algorithms and their operation to protect the management sessions. No additional dependencies have been identified.

[END OF DOCUMENT]