NOKIA IXR SERVICE ROUTER LINUX (SR LINUX) FAMILY V24.10.4 SECURITY TARGET

Evaluated Assurance Level: 3

Document No. 2233-002-D102
Version: 1.0, 25 November 2025

Prepared for:
Nokia
520 Almanor Ave
Sunnyvale, CA
USA, 94085

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

and

Saffire Systems
1061 W 136TH ST
Carmel, IN 46032

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Nokia IXR Service Router Linux (SR Linux) 24.10.4 Family, hereafter referred to generically as SR Linux, the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the SR Linux satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

This document is structured as follows:

- Section 1 - Introduction provides the ST reference, the TOE reference, the TOE overview, and the TOE description.
- Section 2 - Conformance Claims describes how this ST conforms to the Common Criteria and Packages. This ST does not conform to a Protection Profile.
- Section 3 - Security Problem Definition describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.
- Section 4 - Security Objectives defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition
- Section 5 - Extended Components Definition defines the extended components which are then detailed in Section 6.
- Section 6 - Security Requirements specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.
- Section 7 - TOE Summary Specification describes the security functions and assurance measures that are included in the TOE to enable it to meet the IT security functional and assurance requirements.
- Section 8 - Other References identifies reference documents beyond the TOE guidance documentation listed in Section 1.6.6 that are either referred to directly in this Security Target or aid in better understanding the TOE and the application of its technology.

1.2 SECURITY TARGET REFERENCE

This Security Target is uniquely identified as depicted in Table 1.

Table 1: Security Target Reference

Title	Nokia IXR Service Router Linux (SR Linux) Family v24.10.4 Security Target
Version Number	Version 1.0
Publication Date	25 November 2025
Author	Electronic Warfare Associates – Canada Ltd. (EWA-Canada) Saffire Systems

1.3 TARGET OF EVALUATION REFERENCE

The Target of Evaluation (TOE) for this Security Target (ST) is the Nokia IXR Service Router Linux (SR Linux), v24.10.4 (build number is 244-g5c0afd1a61) running on any of the router platforms and models listed in Table 2.

Table 2: Platforms Supported by SR Linux

Platform	Model(s)	Operating System	Collective Reference Terms
7220 Interconnect Routers (IXR)	7220 IXR-D1 7220 IXR-D2 7220 IXR-D2L 7220 IXR-D3 7220 IXR-D3L 7220 IXR-D4 7220 IXR-D5 7220 IXR-H2 7220 IXR-H3 7220 IXR-H4	SR Linux v24.10.4	72x0 or IXR
7250 Interconnect Routers (IXR)	7250 IXR-6e 7250 IXR-10e 7250 IXR-X1b 7250 IXR-X3b		

1.4 TERMINOLOGY AND ACRONYMS

The following terms and acronyms as used within this Security Target have the meanings defined herein.

1.4.1 Terminology

The following terminology is used in this ST:

72x0	A collective term used in this document to refer to Nokia 7250 IXR service switches and 7220 IXR Ethernet services switches. Refer to Table 2 for additional information.
Access Control List	An Access Control List (ACL) is filter policy applied on a packet-by-packet basis on ingress or egress to a routing device on an interface. ACLs are used to filter and restrict traffic access.
Nokia IXR Service Router Linux (SR Linux) 24.10.4 Family	The Nokia IXR Service Router Linux (SR Linux) 24.10.4 Family is the Target of Evaluation (TOE). The SR Linux consists of the following software configuration items (CIs): a. Nokia IXR Service Router Linux, v24.10.4; These software CIs operate on the routers and switches listed in Table 2.
Border Gateway Protocol	The Border Gateway Protocol (BGP) is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional IGP metrics, but makes routing decisions based on path, network policies and/or rule sets.
Central Processing Unit	All traffic destined to the CPM and CSM and that will be processed by its CPU
Command Line Interface	The Command Line Interface (CLI) is a terminal-based administrator interface used to configure a 72x0 IXR.

Control Processor Module	The Control Processor Module (CPM) is a module with the IXR devices.
Coordinated Universal Time	Coordinated Universal Time (UTC) is the definitive reference time scale. Time zones around the world may be expressed as positive or negative offsets from UTC. UTC is derived from International Atomic Time (TAI).
CPM Filter	SR routers and switches use separate CPM modules that have traffic management and queuing hardware on the CPM modules dedicated to protecting the control plane. CPM filters can be created on this hardware. These filters can be used to drop or accept packets, as well as allocate dedicated hardware shaping queues for traffic directed to the control processors. On the IXR-6, 6e, 10 & 10e the CPM filters are applied on a line card separate to the CPM.
Intermediate System to Intermediate System	Intermediate system to intermediate system (IS-IS) is a protocol used by network devices (routers) to determine the best way to forward datagrams through a packet-switched network, a process called routing.
Internet Engineering Task Force	The Internet Engineering Task Force (IETF) develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standards bodies and dealing in particular with standards of the TCP/IP and Internet protocol suite. It is an open standards organization.
Internet Protocol	The Internet Protocol (IP) is a network layer protocol underlying the Internet, which provides an unreliable, connectionless, packet delivery service. IP allows large, geographically-diverse networks of computers to communicate with each other quickly and economically over a variety of physical links.
IXR	Interconnect Routers (IXR) is a collective term used in this document to refer to the 7220 & 7250 IXR router models listed in Table 2.
Local Area Network	A Local Area Network (LAN) is a system designed to interconnect computing devices over a restricted geographical area (usually not more than a couple of kilometres).
CPM Filter	A CPM Filter controls all traffic in and out of the CPM. This can be used to restrict management of the IXR device by other nodes outside either specific (sub)networks or through designated ports.
Media Access Control	Media Access Control (MAC) is a media-specific access control protocol within IEEE 802 specifications. The protocol is for medium sharing, packet formatting, addressing, and error detection.
Quality of Service	Quality of Service (QoS) is a set of performance parameters that characterize the traffic over a given connection
Remote Authentication Dial-In User Service	Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize access to the requested system or service.
Request for Comments	A Request for Comments (RFC) is an Internet Engineering Task Force (IETF) memorandum on Internet systems and standards
RS-232	RS-232 is a serial communications protocol currently defined by **[TIA-232-F]**

Service Router	Service Router (SR) is a collective term used in this document to refer to the seven 7750 SR router models listed in Table 2.
Terminal Access Controller Access Control System Plus	Terminal Access Controller Access Control System Plus (TACACS+) is an authentication protocol that allows a remote access server to forward an administrator's logon password to an authentication server to determine whether access is allowed to a given system.
Transmission Control Protocol	The Transmission Control Protocol (TCP) enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and guarantees that packets will be delivered in the same order in which they were sent.
User Datagram Protocol	The User Datagram Protocol (UDP) is a is transport layer protocol which do not guarantee delivery of data.
Virtual Private Network	A Virtual Private Network (VPN) is a way to provide secure and dedicated communications between a group of private servers over public Internet.
VPN Routing and Forwarding	VPN Routing and Forwarding (VRF) is a technology used in computer networks that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses are used without conflicting with each other.

1.4.2 Acronyms

The following acronyms are used in this ST:

ACL	Access Control List
ANSI	American National Standards Institute
AS	Autonomous System(s)
BGP	Border Gateway Protocol
CC	Common Criteria for Information Technology Security Evaluation (Common Criteria)
CEM	Common Evaluation Methodology (Common Criteria)
CLI	Command Line Interface
CPM	Control Plane Module
CPU	Central Processing Unit
D/DoS	Distributed Denial of Service
DoS	Denial of Service
EAL	Evaluation Assurance Level (Common Criteria)
EAL 3+	Evaluation Assurance Level 3, Augmented (Common Criteria)
FC	Forwarding Class
FTP	File Transfer Protocol
GUI	Graphical User Interface
I&A	Identification and Authentication
I/O	Input / Output
ID	Identification (or Identity)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers

IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
ISO	International Organization for Standardization
IT	Information Technology
IXR	Interconnect Routers
LAN	Local Area Network
LDP	Label Distribution Protocol
LSR	Label Switch Router
MAC	Media Access Control
NTP	Network Time Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RS-232	Serial protocol
SFP	Security Function Policy (Common Criteria)
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SR Linux	Service Router Operating System Refer to the definition of “Nokia IXR Service Router Linux (SR Linux) 24.10.4 Family” on page 2 for more information.
SSD	Solid-state drive
SSH	Secure Shell (protocol)
ST	Security Target (Common Criteria)
TACACS+	Terminal Access Controller Access Control System Plus
TAI	International Atomic Time
tar	File format used for archiving data (derived from “tape archive”)
TCP	Transmission Control Protocol
TCP/IP	Transport Control Protocol over Internet Protocol
TOE	Target of Evaluation (Common Criteria)
TSF	TOE Security Functionality (Common Criteria)
TSFI	TOE Security Functionality Interface (Common Criteria)
TTL	Time to Live
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
VRF	VPN Routing and Forwarding
W3C	World Wide Web Consortium
XML	Extensible Mark-up Language

1.5 TOE OVERVIEW

The TOE is a network operating system (NOS) router/switch providing network operating system functionality. The TOE is the Nokia IXR Service Router Linux (SR Linux) 24.10.4 Family running on the Nokia 7250 IXR series or 7220 IXR series platforms and models identified in Table 2. The physical boundary of the TOE is the hardware platform and operating system (i.e., SR Linux v24.10.4).

The 7220 & 7250 IXR offer modular, high-scale interconnectivity. SR Linux is located on a non-removable solid-state drive (SSD). For the various hardware models there are only performance (number of I/O modules, thru-put, redundancy, capacity) differences and no security related differences. Security features defined in the evaluated configuration, their behaviours, and the way they are configured are the same in the 72x0 IXR routers and switches.

SR Linux is intended to be used in data centers to improve scalability and automation. SR Linux monitors, routes, and manipulates network traffic to facilitate the traffic data delivery to the proper destination on a network or between networks. SR Linux forwards data packets between networks and must have physical access to at least two distinct networks or network segments to pass data between.

All TOE interfaces, except the network traffic/data interfaces, SSH and gNMI protocol interfaces, are attached to the internal trusted protected network that is only accessibly by the infrastructure devices and trusted administrators. The network traffic/data interfaces are attached to both internal and external networks. The Console Access via RS-232 interface is a direct local connection which provides the CLI.

1.5.1 Security Features

SR Linux offer security features to address the security requirements in both network infrastructure and service layer. SR Linux generates audit records for security-relevant actions that occur on the system. Administrative users and external trusted products must be authenticated to interact with SR Linux. SR Linux also provides user session controls, such as session locking. Local and remote management capabilities are available for administrators. SR Linux enforces router information flow control rules configured by the administrator to control the network packets transmitted through the router. Trusted communications are implemented for all communications between SR Linux and other trusted products. Remote management traffic (to/from the TOE) is protected from unauthorized modification and disclosure. The SR Linux also provides protection against the Denial of Service (DoS) attacks. The deployed configuration of the TOE uses quality of service mechanisms, Access Control Lists (ACLs) to protect against Distributed and other DoS (D/DoS) attacks.

1.5.2 Operational Environment

This section identifies any non-TOE hardware, software, and firmware that is required by the TOE to operate in accordance with this certification.

The local Console used to interface with the Command Line Interface (CLI) is outside the TOE boundary. In the deployed configuration of the TOE in its intended environment, the primary means of administering the TOE during normal operations will be via the CLI accessed using SSH.

The operational environment requires a local Console for installation and initial setup only and that the following local systems are attached to the internal trusted protected network that is only accessible by infrastructure devices and trusted administrators:

- a RADIUS or TACACS+ server for authentication / authorization services;
- Syslog servers for logging; and
- a Network Time Protocol (NTP) server for external time synchronization.

Minimum hardware and operating system requirements for the external IT entities connected to the TOE are:

- RADIUS/TACACS+ server: Any combined hardware and operating system platform that supports RFC 2865 (Authentication & Authorization) and RFC 2866 (Accounting) for RADIUS. Any combined hardware and operating system platform that supports RFC 8907 for TACACS+;
- SSH/remote CLI: Any combined hardware and operating system platform that supports the operation of the Secure Shell protocol;
- gNMI: Any combined hardware and operating system platform that supports a gNMI client;
- Syslog server: Any combined hardware and operating system platform that supports RFC 5424 The Syslog Protocol;
- Local Console: A direct connection via a RS-232 interface providing CLI access for installation and initial setup only
- NTP server: Any combined hardware and operating system platform that supports RFC 1305 for Network Time Protocol.

1.6 TOE DESCRIPTION

1.6.1 Introduction

Nokia Service Router Linux (SR Linux) is a network operating system (NOS) router/switch providing network operating system functionality. It is intended to be used in modern IP and data center networks and across hybrid- and multi-cloud environments. SR Linux provides more control and flexibility to allow customers to design and operate their networks as needed. The TOE monitors, routes, and manipulates network traffic to facilitate the traffic data delivery to the proper destination on a network or between networks.

1.6.2 Architectural Overview

SR Linux is comprised of three subsystems: Linux kernel, an operating system (OS), and a suite of modular applications that each support a protocol or function. The Linux® kernel within SR Linux handles all interactions between the OS and hardware, and serves as the foundation on which to build network applications.

SR Linux is a suite of applications running in a Linux environment. The SR Linux applications communicate with the impart database (IDB) to process configuration and state information. Messaging between SR Linux applications is controlled by the IDB. The routing functions and protocols on SR Linux execute as modular, lightweight applications that are isolated into their own domains. These applications use gRPC and APIs to communicate with each other and external systems over TCP.

In the evaluated configuration, an administrator can configure Access Control List policies to filter IPv4 traffic. The Nokia-supplied applications can be augmented by third-party developed applications, which plug into the SR Linux framework. These third-party applications are outside the scope of the TOE.

System configuration is controlled by the management server application. SR Linux includes model-driven management interfaces (SR Linux CLI and gNMI server) based on a common infrastructure. The CLI can be accessed using a console or an SSH connection. SR Linux offers the ability to configure an SSH server to establish secure connection to/from the SR Linux to access the CLI. The SR Linux family also offers the ability to manage the devices using gRPC Network Management Interface (gNMI) that is transmitted over HTTPS. SR Linux also provides gNOI, gNSI, JSON, and SNMPv2 interfaces, but these interfaces will be disabled in the evaluated configuration.

The SR Linux software uses a base Linux operating system (OS). The primary copy of SR Linux software is located on a solid-state drive or solid-state memory card installed in the hardware platforms that are shipped with each model.

The TOE controls of three distinct network planes: management plane, control plane, and data plane. The management plane provides management access to SR Linux. The Management Plane subsystem includes the CLI over SSH and gNMI over HTTPS/TLS. The Control Plane consists of all software modules that interact with or control how traffic is forwarded through an individual node or the entire network. This includes routing and services protocols. The Data Plane handles the forwarding of user data traffic. It also provides other planes with statistics and state information and receives configuration information for services and forwarding information for the handling of data.

Using Quality of Service (QoS) and Access Control List (ACL) filter capabilities of the SR Linux, DoS activity can be mitigated. ACLs are used to protect against DoS attacks on traffic passing through the routers and on against traffic "to" the TOE.

1.6.3 Physical Scope

1.6.3.1 TOE Boundary

Figure 1 shows the TOE in its deployment configuration.

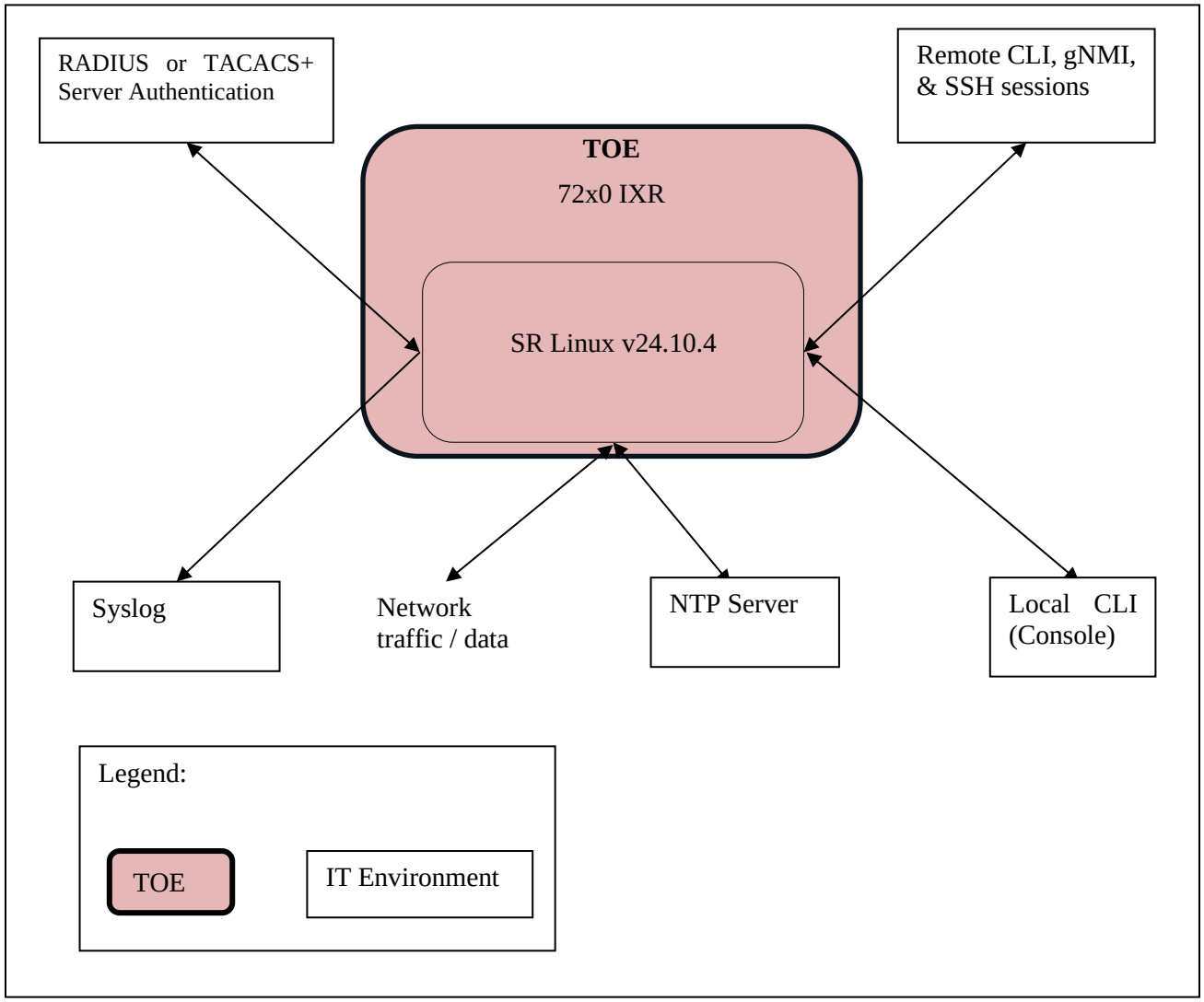

Figure 1: TOE Boundary

Note to Figure 1 *The physical boundary is the SR Linux operating system (i.e., SR Linux v24.10.4) running on the IXR platforms. The TOE's operational environment requires the following systems be on an internal trusted protected network: a RADIUS or TACACS+ server for authentication/authorization services, local Console access for installation and initial setup, Syslog servers for logging, and a Network Time Protocol (NTP) server for external time synchronization.*

1.6.3.2 TOE Guidance Documentation

The guidance documentation that accompanies the TOE is listed in the following table.

Table 3: TOE Guidance Documentation

Guidance Name	Document Number	Edition	Date
Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 ACL and Policy-based Routing Guide	3HE 20968 AAAA TQZZA	01	November 2024
Nokia Service Router Linux, 7220 Interconnect Router, 7250 Interconnect Router, Release 24.10 Advanced Solutions Guide	3HE 20952 AAAA TQZZA	01	November 2024
Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Configuration Basics Guide	3HE 20951 AAAA TQZZA	01	November 2024
Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Data Model Reference	3HE 20958 AAAA TQZZA	01	November 2024
Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Log Events Guide	3HE 20957 AAAA TQZZA	01	November 2024
Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Product Overview	3HE 20948 AAAA TQZZA	01	November 2024
Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Routing Protocol Guide	3HE 20966 AAAA TQZZA	01	November 2024
Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Software Installation Guide	3HE 20953 AAAA TQZZA	01	November 2024

Guidance Name	Document Number	Edition	Date
Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 System Management Guide	3HE 20949 AAAA TQZZA	01	November 2024
Nokia IXR Service Router Linux (SR Linux) Family v24.10.4 Supplemental Common Criteria Guidance	2233-002-D105	1.0	25 November 2025

1.6.4 Logical Scope

The logical boundaries of the TOE are defined by the functions that are carried out by the TOE at the TOE external interfaces. The TOE addresses the security relevant features described in the following subsections.

1.6.4.1 Audit

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system.

Audit also keeps track of the activity of an administrator who has accessed the network. The type of audit information recorded includes a history of the commands executed during the session.

1.6.4.2 Cryptography

The cryptographic operations in SR Linux are provided by OpenSSL 3.0.15.

Trusted path communications between the TOE and the Administrator are protected by HTTPS and SSH protocols that utilize the cryptographic mechanisms.

1.6.4.3 Identification & Authentication (I&A)

SR Linux identifies and authenticates individual users by validating an administrator's username and password. Administrators are identified and authenticated via local authentication, RADIUS or TACACS+. All authentication methods are available on each management interface. SR Linux also provides authentication failure handling and the ability for the administrator to define password security (complexity) requirements.

1.6.4.4 Security Management

SR Linux implements authorization features using role-based access control. Each authenticated user is assigned one or more predefined roles that specify the functions the user is allowed to perform. SR Linux can be managed using a CLI over console and SSH and gNMI server over HTTPS. The Administrator configures system security and access functions, configuration settings, and logging features.

1.6.4.5 TOE Access

Local and remote Administrator's sessions are dropped after an Administrator-defined time period of inactivity. SR Linux can be configured to display a login banner before a user is authenticated and a message of the day banner after the user is authenticated.

1.6.4.6 User data protection (Information flow control)

The SR Linux enforces a Traffic Filtering policies whereby the network packets sent through the TOE are subject to router information flow control rules setup by the administrator. The Quality of Service (QoS) and Access Control List (ACL) filter capabilities of the SR Linux can mitigate DoS activity.

1.6.5 Evaluated Configuration

The evaluated configuration for the TOE must include the following enabled/disabled/configured settings (all other services, protocols and settings are excluded from the evaluated configuration):

a. Enable SR Linux (CLIENT-side) for:

   (1) RADIUS or TACACS+ server authentication/ authorization services;

   (2) Local Console access for installation and initial setup;

   (3) Network Time Protocol (NTP) server for external time synchronization;

   (4) GNMI over TLS

b. Ensure FTP remains disabled;

c. gNOI, JSON, and SNMPv2 interfaces remain disabled;

d. Use of gNSI is disabled.

e. Configure CPM filters on IXR devices for protection of the CPM by restricting traffic;

f. Disable sending events to a console destination. The console device is not be used as an event log destination. A log created with the console type destination displays events to the physical console device. Events are displayed to the console screen whether an administrator is logged into the console or not; and

g. Use of Netconf server is disabled.

h. Use of Linux users is disabled except during initial installation, setup and troubleshooting.

i. The use of IPv6 Interface filters, IPv6 CPM filters, System filters, and MAC ACLs are excluded from the evaluated configuration.

j. The use of secondary actions (i.e., policer and log actions) in ACLs is excluded from the evaluated configuration.

k. Use of Zero Touch Provisioning (ZTP) is disabled.

l. SR Linux offers service providers and enterprises differentiated services, from Internet access to Ethernet Virtual Private Network (EVPN) with Virtual eXtensible LAN (VXLAN) deployments. VPN is a capability of the SR Linux; however, it is defined outside the TOE and was not evaluated. The use of Ethernet Virtual Private Network (EVPN) and VXLAN (EVPN-VXLAN) are excluded from the evaluated configuration.

1.6.6 Non-evaluated Functions/Features

The following features of the SR Linux product family are outside the evaluated configuration. Their use is allowed in the evaluated configuration, but the features have not been tested.

1. The high availability (HA) feature is not in the scope of the evaluated configuration.
2. The following protocols and technologies are not in the scope of the evaluated configuration.
   a. Border Gateway Protocol (BGP)

b. MAC-VRF

c. Multiprotocol Label Switching (MPLS)

d. Label Distribution Protocol (LDP)

3. Third-party developed applications that plug into the SR Linux framework.
    a. CLI Plug-Ins
4. gRPC Routing Information Base Interface (gRIBI) – a gRPC-based protocol that allows external applications to change routes in a device's routing information base (RIB).
5. Packet capture filters that copy and extract packets for inspection by tools outside the TOE to protect against Distributed and other DoS (D/DoS) attacks.
6. Filtering based on IP Differentiated Services Code Point (DSCP).

1.6.7 Delivery

The customer is responsible for acquiring the Nokia IXR hardware required for SR Linux 24.10.4 to execute on in the evaluated configuration. The IXR hardware is shipped to the customer directly from the Nokia inventory warehouse. The Nokia IXR hardware and SR Linux software can be purchased together or separately. All new systems require the purchase of an appropriate software license. The CC Guidance Supplement instructs the customer to download SR Linux 24.10.4 binary images from the Nokia Support Portal.

The SR Linux software is distributed in the following ways:

- Shipment of the new license with an SD card containing the binary image(s)
- Shipment of the system preloaded with the binary image in the SSD
- Software delivery via web interface.

When a new system is first ordered, SR Linux image is typically delivered either via shipment of the new license with an SD card or preloaded in the SDD. When the Nokia IXR hardware and SR Linux software are ordered together, the 7250 IXR-X and 7220 IXS will ship with a version of the SR Linux operating system (OS) already installed in the SSD. For the other hardware models, the system comes preloaded with the binary image, allowing it to boot directly into the version of SR Linux it was shipped with.

For delivery via the web, SR Linux is delivered to the user via download from the Nokia Support Portal over an HTTPS connection. Downloading a product from the Nokia Support Portal requires that the user have a valid login account and completed the PO process. Only products purchased by the customer are available for download. The software is provided as multiple images. The integrity of the SR Linux installation image downloads can be verified using a checksum.

Bonded shipping carriers, such as FedEx and UPS, are used to transport the IXR hardware and the SD card. Upon receiving the shipment(s), the customer is instructed to inspect the packaging for signs of tampering or other issues. This includes checking that the box label and product label match the ordered product.

The standard SR Linux documentation is available from the Nokia Doc Center (https://documentation.nokia.com/srlinux/). The documentation is publicly available over an HTTPS connection. The CC Guidance Supplement is only accessible to customers and is available through the Nokia Support Portal.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST is conformant with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, Revision 5, April 2017:

a. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017;

b. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017; and

c. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.

The Target of Evaluation (TOE) for this ST is:

- CC Part 2 conformant; and
- CC Part 3 conformant.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE described by this ST does not claim conformance with any Protection Profile (PP).

2.3 EVALUATION ASSURANCE LEVEL (EAL)

This Security Target claims conformance to EAL3, augmented with ALC_FLR.1 (Basic Flaw Remediation).

3 SECURITY PROBLEM DEFINITION

The security problem definition shows the threats, Organizational security policies (OSPs) and assumptions that must be countered, enforced, and upheld by the TOE and its operational environment.

3.1 THREATS

The threats listed in Table 4 are addressed by the TOE. The threat agents consist of unauthorized persons or external IT entities that are not authorized to use the TOE as well as authorized administrators of the TOE who make errors in configuring the TOE.

The assumed level of expertise of the attacker for all the threats is unsophisticated. Both threat agents are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network.

Considering the possible attack scenarios for the deployed configuration of the TOE in its intended environment, the level of attack potential assumed for the attacker is BASIC[1] which is in keeping with the desired EAL 3 assurance level of this TOE, considering factors of attackers' expertise, resources, opportunity, and motivation.

Fully authorized administrators with access to data have low motivation to attempt to compromise the data because of other assumptions and organization security policies defined herein.

Table 4: Threats

Threat Identifier	Description
T.AUDIT	Management actions may not be known to administrators due to actions not being recorded (and time stamped), or the audit records not being reviewed prior to the machine shutting down, or an unauthorized user modifies or destroys audit data.
T.MEDIATE	An unauthorized entity may send impermissible information through the TOE which results in the exploitation (e.g., destruction, modification, or removal of information and/or other resources), and/or exhaustion of resources on the network (e.g., bandwidth consumption or packet manipulation).
T.TSF_DATA	A malicious administrator may gain unauthorised access to inappropriately view, tamper, modify, or delete TOE Security Functionality (TSF) data.
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session and view and change the TOE security configuration.
T.UNAUTH_MGT_ACCESS	An unauthorized user gains management access to the TOE and views or changes the TOE security configuration.
T.UNTRUSTED_CHANNELS	An unauthorized user intercepts critical communication channels between the TOE and *remote administrators*, resulting in the loss of confidentiality and/or integrity of network traffic.

[1] Attack Potential is a function of expertise, resources, and motivation. Refer to Sections B.3 and B.4 of the "*Common Methodology for Information Technology Security Evaluation - Evaluation Methodology*", Document ID: CCMB-2017-04-004 for a detailed discussion of Attack Potential and how it is estimated.

T.WEAK_AUTH	An unauthorized entity masquerades as an authorized user or device inserting themselves in the network traffic, resulting in in the loss of confidentiality and/or integrity of network traffic.
T.WEAK_CRYPTO	A user uses weak cryptographic algorithms, modes and key sizes which allows attackers to gain unauthorized access to the system allowing them to read, modify and/or control traffic.

3.2 ORGANIZATIONAL SECURITY POLICIES

Table 5 defines the Organizational Security Policies (OSPs) that are to be enforced by the TOE, its operational environment, or a combination of the two.

Table 5: Organizational Security Policies

OSP Identifier	Description
P.DEPLOYED_CONFIG	The deployed configuration of the TOE in its intended environment shall be at least as restrictive as the baseline evaluated configuration defined herein and will be configured in accordance with guidance documentation.
P.USERS	The TOE is administered by two or more Administrators who have been granted rights to administer the TOE. All administrators are "vetted" to help ensure their trustworthiness, and administrator connectivity to the TOE is restricted. Non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.

3.3 ASSUMPTIONS

Table 6 identifies the assumptions made to ensure that the security functionality defined herein can be provided by the TOE in its intended operating environment. These include assumptions made on personnel, the physical environment, and operational conditions.

Table 6: Assumptions

Assumption Identifier	Description
A.ADMINISTRATOR	It is assumed that authorized Assumptions administrators are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance, and will periodically check the audit record; however, they are capable of error. It is further assumed that personnel will be trained in the appropriate use of the TOE to ensure security.
A.EXT_AUTH	It is assumed that external authentication services will be available to the TOE via either RADIUS, TACACS+, or both, based on defined Internet Engineering Task Force (IETF) standards.
A.INTEROPERABILITY	It is assumed that the TOE functions with the external IT entities shown in Figure 1 and with other vendors' routers on the network and meets Request for Comments (RFC) requirements for implemented protocols.
A.NO_GENPURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

Assumption Identifier	Description
A.PHYSICAL_PROT	It is assumed that the operational environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE. It is further assumed that the processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.
A.TIMESTAMP	It is assumed that the Operational Environment provides the TOE with the necessary reliable time stamp. External Network Time Protocol (NTP) services will also be available to provide external time synchronization.
A.TRUSTED_DEVICE	It is assumed that the trusted remote systems that communicate with the TOE, except for the network traffic/data interface, are attached to an internal trusted protected network that is only accessible by infrastructure devices and trusted administrators. This includes: (1) the RADIUS, TACACS+ server; (2) the Syslog servers; and (3) the NTP server. The Network traffic/data interface is attached to internal and external networks. Console Access is via RS-232, a direct local connection in the same physical location as the TOE.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means). Mappings of security objectives to assumptions, threats, and organizational security policies, along with supporting rationale, are found in Section 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

Table 7 defines the TOE security objectives that are to be addressed by the TOE.

Table 7: TOE Security Objectives

Identifier	Description
O.AUDIT	The TOE will generate audit records which will include the time that the event occurred and the identity of the administrator performing the event. The TOE will provide the privileged administrators the capability to review audit data and will restrict audit review to administrators who have been granted explicit read-access.
O.CRYPTO	The TOE will provide cryptographic functionality capable of maintaining confidentiality and integrity of data.
O.I&A	The TOE will uniquely identify and authenticate the claimed identity of all administrators before granting management access to control their actions.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must mediate the flow of all information between hosts located on disparate internal and external networks governed by the TOE. The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.
O.PROT_COMMS	The TOE provides communication channels for administrators. These communication channels authenticate the other endpoint and protect the data from unauthorized disclosure and modification during transmission to and from the TOE.
O.TOE_ACCESS	The TOE will provide mechanisms that control an administrator's logical access to the TOE and to explicitly deny access to specific administrators when appropriate.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

4.2.1 IT Security Objectives for the Operational Environment

The IT security objectives for the environment[2] listed in Table 8 are to be addressed by the Operational Environment via technical means.

[2] This ST addresses TOE (client-side) support of RADIUS and TACACS+ where external authentication services are available via either RADIUS, TACACS+, or both. RADIUS or TACACS+ authentication servers or NTP servers with which the SR Linux communicates are considered external IT entities that are part of the TOE's operational environment. The operational environment for the SR Linux requires a RADIUS or TACACS+ server and a Network Time Protocol (NTP) server for external time synchronization.

Table 8: IT Security Objectives for the Operational Environment

Security Objective for Operational Environment Identifier	Description
OE.DEPLOYED_CONFIG	The deployed configuration of the TOE in its intended environment is at least as restrictive as the baseline evaluated configuration defined herein and will be configured in accordance with a guidance documentation
OE.EXT_AUTHORIZATION	A RADIUS server, a TACACS+ server, or both is available for external authentication services.
OE.INTEROPERABILITY	The external IT entities shown in Figure 1 are able to function with the TOE and with other vendors' routers on the network and meet Request for Comments (RFC) requirements for implemented protocols.
OE.NO_GENPURPOSE	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities for the TOE in its operational environment.
OE.TIME	The operational environment supplies the TOE with a reliable time source.
OE.TRUSTED_DEVICE	All TOE external interfaces except for the network traffic/data interface are attached to an internal trusted protected network that is only accessible by infrastructure devices and trusted administrators. This includes: (1) the RADIUS, TACACS+ server interface; (2) the Syslog interface; and (3) the NTP interface. The Network traffic/data interface is attached to internal and external networks. Console Access is via RS-232, a direct local connection in the same physical location as the TOE.

4.2.2 Non-IT Security Objectives for the Operational Environment

The non-IT security objectives listed in Table 9 are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

Table 9: Non-IT Security Objectives for the Operational Environment

Identifier	Description
OE.ADMINISTRATOR	The authorized administrators are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance (e.g., procedures to review/manage audit records); however, they are capable of error. Personnel will be trained in the appropriate use of the TOE to ensure security.
OE.PHYSICAL_PROT	The processing resources of the TOE are located within controlled access facilities, which prevent unauthorized physical access. In addition, the operational environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE

Identifier	Description
OE.USERS	All administrators are "vetted" to help ensure their trustworthiness, and administrator connectivity to the TOE is restricted. Non administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Security Objectives Rationale Related to Threats

Table 10 provides a bi-directional mapping of Security Objectives to Threats. It shows that each of the threats is addressed by at least one of the security objectives, and that each of the TOE security objectives addresses at least one of the threats. Following this table is rationale that discusses how each threat is countered by one or more Security Objectives.

Table 10: Mapping Of Security Objectives to Threats

	O.AUDIT	O.CRYPTO	O.I&A	O.MANAGE	O.MEDIATE	O.PROT_COMMS	O.TOE_ACCESS	OE.ADMINISTRATOR	OE.TIME
T.AUDIT	X							X	X
T.MEDIATE					X				
T.TSF_DATA				X				X	
T.UNATTENDED_SESSION							X		
T.UNAUTH_MGT_ACCESS			X						
T.UNTRUSTED_CHANNELS						X			
T.WEAK_AUTH						X			
T.WEAK_CRYPTO		X				X			

T.AUDIT *Management actions may not be known to administrators due to actions not being recorded (and time stamped), or the audit records not being reviewed prior to the machine shutting down, or an unauthorized user modifies or destroys audit data.*

The O.AUDIT objective covers this threat by generating audit records. O.AUDIT requires the TOE provide the Authorized administrator with the capability to view Audit data. O.AUDIT requires that the TOE protect audit data and restrict audit review to administrators who have been granted explicit read-access.

The OE.ADMINISTRATOR objective on the environment assists in covering this threat on the TOE by requiring that the administrator abide by the instructions provided by the TOE documentation, including the administrator guidance to periodically check the audit record.

The OE.TIME objective on the environment assists in covering this threat by requiring that the OE provide accurate time to the TOE for use in the audit records.

These objectives provide complete coverage of the threat.

T.MEDIATE *An unauthorized entity may send impermissible information through the TOE which results in the exploitation (e.g., destruction, modification, or removal of information and/or other resources), and/or exhaustion of resources on the network (e.g., bandwidth consumption or packet manipulation).*

The O.MEDIATE security objective mitigates this threat by ensuring all information that passes through the network is mediated by the TOE and mediating the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.

This objective provides complete coverage of the threat.

T.TSF_DATA *A malicious administrator may gain unauthorised access to inappropriately view, tamper, modify, or delete TOE Security Functionality (TSF) data.*

The O.MANAGE objective mitigates this threat by providing all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. This objective provides complete TOE coverage of the threat.

The OE.ADMINISTRATOR objective on the environment assists in covering this threat on the TOE by requiring that the administrator abide by the instructions provided by the TOE documentation, including the administrator guidance to periodically check the audit record, reducing the possibility for error.

These objectives provide complete coverage of the threat.

T.UNATTENDED_SESSION *A user may gain unauthorized access to an unattended session and view and change the TOE security configuration.*

The O.TOE_ACCESS objective mitigates this threat by including mechanisms that place controls on administrator's sessions. Local and remote administrator's sessions are dropped after an Administrator-defined time period of inactivity. Dropping the connection of a local and remote session (after the specified time period) reduces the risk of someone accessing the local and remote machines where the session was established, thus gaining unauthorized access to the session.

This objective provides complete coverage of the threat.

T.UNAUTH_MGT_ACCESS *An unauthorized user gains management access to the TOE and views or changes the TOE security configuration.*

The O.I&A objective mitigates this threat by uniquely identifying and authenticating the claimed identity of all administrators before granting management access and to control their actions. O.I&A requires an administrator to enter a unique identifier and authentication before management access is granted.

This objective provides complete coverage of the threat.

T.UNTRUSTED_CHANNELS *An unauthorized user intercepts critical communication channels between the TOE and remote administrators, resulting in the loss of confidentiality and/or integrity of network traffic.*

The O.PROT_COMMS objective mitigate this threat by providing communication channels for administrators and external IT entities that are protected from unauthorized disclosure and modification during transmission to and from the TOE.

This objective provides complete coverage of the threat.

T.WEAK_AUTH *An unauthorized entity masquerades as an authorized user or device inserting themselves in the network traffic, resulting in in the loss of confidentiality and/or integrity of network traffic.*

The O.PROT_COMMS objective mitigate this threat by providing communication channels for administrators and external IT entities that authenticate the administrator or external IT entity.

This objective provides complete coverage of the threat.

T.WEAK_CRYPTO *A user uses weak cryptographic algorithms, modes and key sizes which allows attackers to gain unauthorized access to the system allowing them to read, modify and/or control traffic.*

The O.CRYPTO objective mitigates this threat by encrypting data transmitted to and from administrators and trusted IT entities.

The O.PROT_COMMS objective mitigate this threat by providing communication channels that protect data from unauthorized disclosure and modification.

These objectives provide complete coverage of the threat.

4.3.2 Environment Security Objectives Rationale Related to Assumptions and OSPs

Table 11 provides a bi-directional mapping of Assumptions and OSPs to Security Objectives for the Operational Environment. Since the Security Objectives for the Operational Environment were derived directly from the Assumptions and OSPs there is a one-to-one mapping between them.

It is also clear since the Security Objectives for the Operational Environment are simply a restatement of the applicable assumption or OSP, that each objective is suitable to meet its corresponding assumption or OSP.

Table 11: Mapping Of Environment Security Objectives to Assumptions and OSPs

	OE.ADMINISTRATOR	OE.DEPLOYED_CONFIG	OE.EXT_AUTHORIZATION	OE.INTEROPERABILITY	OE.NO_GENPURPOSE	OE.PHYSICAL_PROT	OE.TIME	OE.TRUSTED_DEVICE	OE.USERS
A.ADMINISTRATOR	X								
A.EXT_AUTH			X						
A.INTEROPERABILITY				X					

	OE.ADMINISTRATOR	OE.DEPLOYED_CONFIG	OE.EXT_AUTHORIZATION	OE.INTEROPERABILITY	OE.NO_GENPURPOSE	OE.PHYSICAL_PROT	OE.TIME	OE.TRUSTED_DEVICE	OE.USERS
A.NO_GENPURPOSE					X				
A.PHYSICAL_PORT						X			
A.TIMESTAMP							X		
A.TRUSTED_DEVICE								X	
P.DEPLOYED_CONFIG		X							
P.USERS									X

5 EXTENDED COMPONENTS DEFINITION

There are no extended SFRs for the TOE.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

The security requirements consist of two groups of requirements:

a. the security functional requirements (SFRs): a translation of the security objectives for the TOE into a standardised language; and

b. the security assurance requirements (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

6.1 SECURITY REQUIREMENTS PRESENTATION CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2 are identified in this ST in the following manner:

a. Selection: Indicated by italicized text, e.g., *selected item*;

b. Assignment: Indicated by bold text, e.g., **assigned item**;

c. Refinement: Refined components are identified by using underlining additional information, or ~~strikeout~~ for deleted text; and

d. Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_IFC.1(1), Subset Information Flow Control (VPN Policy)'.

The markings are relative to the requirement statements in the Common Criteria standard.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC as summarized in Table 12.

Table 12: Summary of Security Functional Requirements

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
Cryptographic Support (FCS)	FCS_COP.1	Cryptographic Operation
User Data Protection (FDP)	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication (FIA)	FIA_AFL.1	Authentication Failure Handling
	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UAU.5	Multiple Authentication Mechanisms

Class	Identifier	Name
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UID.2	User Identification Before Any Action
Security Management (FMT)	FMT_MOF.1	Management of Security Functions Behaviour
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable Time Stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User Initiated Termination
	FTA_TAB.1	Default TOE access banners
Trusted Path/Channels (FTP)	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

6.2.1 Security Audit (FAU)

6.2.1.1 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:

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

b) all auditable events for the *not specified* level of audit;

c) **Log all login attempts**

d) **Log successful configuration change activity of administrators;**

e) **Security breach logging**.

Application Note:

Log successful configuration change activity of administrators (generating audit records for viewing of audit logs and configuration settings are not claimed). The change activity event source is all events that directly affect the configuration or operation of the TOE as defined in the FMT_MOF.1, FMT_SMF.1, and FMT_SMR.1 SFRs).

Security breach logging. The security event source is all events that affect attempts to breach system security such as failed login attempts or attempts to access commands to which the administrator is not granted access. Security events are generated by the security application.

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

a) Date and time of the event, type of event, subject identify (if applicable), and the outcome (short text description 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, **none**.

6.2.1.2 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.

6.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide **authorized administrators** with the capability to read **all audit data** 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.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **the cryptographic operations identified in Table 13** in accordance with a specified cryptographic algorithm **the cryptographic algorithms identified in Table 13** and cryptographic key sizes **the cryptographic key sizes identified in Table 13** that meet the following: **standards identified in Table 13**.

Table 13: Cryptographic Specifications

Cryptographic Operation	Cryptographic Algorithm	Key Sizes	Standards	Uses
Encryption, Decryption	AES with GCM mode AES with CBC mode	128, 256 bits	AES as specified in ISO 18033-3, GCM as specified in ISO 19772 CBC as specified in ISO 10116	TLS HTTPS SSH
	AES with CTR mode	128, 256 bits	AES as specified in ISO 18033-3, CTR as specified in ISO 10116	SSH
	AES with CCM mode	128 bits	AES as specified in ISO 18033-3, CCM as specified in SP 800-38C	TLS HTTPS
Digital signature generation and verification	RSA Digital Signature Algorithm	3072 bits default for SSH 4096 bits for TLS	FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	TLS HTTPS SSH
	Elliptic Curve Digital Signature Algorithm (ECDSA)	256 bits	FIPS PUB 186-5 "Digital Signature Standard (DSS)", Section 6 and Appendix D ISO/IEC 14888-3 Section 6.4	SSH
Hashing Services	SHA-256	256 bits	ISO/IEC 10118-3:2004	TLS

Cryptographic Operation	Cryptographic Algorithm	Key Sizes	Standards	Uses
				HTTPS SSH
	SHA-512	512 bits	ISO/IEC 10118-3:2004	SSH
	SHA-384	384 bits	ISO/IEC 10118-3:2004	TLS HTTPS
Keyed-hash message authentication	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512	160, 256, 512 bits	*ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*	SSH

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the **Traffic Filtering SFP** on

a) **subjects: each IT entity that sends and receives information through the TOE to one another or each IT entity that sends and receives information to/from the TOE;**

b) **information: network packets sent through the TOE from one subject to another or network packets sent to/from the TOE; and**

c) **operations: accept (allow the packet to the next processing function) or drop network packets (discard the packet without ICMP generation)**.

6.2.3.2 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the **Traffic Filtering SFP** based on the following types of subject and information security attributes:

a) **security subject attributes:**

   i. IPv4 network address and port of source subject;

b) **information subject attributes:**

   i. IPv4 network address and port of source subject;

   ii. IPv4 network address and port of destination subject;

   iii. transport layer protocol and their flags and attributes (UDP, TCP);

   iv. network layer protocol (IP, ICMP);

   v. packet fragmentation;

   vi. **interface on which traffic 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) **Each ACL rule has a sequence ID. The rules within an ACL (an ordered set of rules) are evaluated starting with the rule with the lowest sequence ID,**

progressing to the rule with the highest sequence ID. ACL rule evaluation stops at the first matching ACL rule and the associated action is performed with no further evaluation

b) **IPv4 Interface filters (ACLs) and IPv4 CPM filters (ACLs) are logically attached to the physical network interfaces**

c) **IPv4 CPM filters (ACLs) are system wide filters**

d) **IPv4 Interface filters are processed before IPv4 CPM filters**

e) **If the packet does not match any ACL rules, the default action is to accept.**

f) **The match conditions that can be configured in an ACL rule are:**

i. source subject attributes are in the set of source subject ACL criteria:

(1) source prefix and prefix-length;

(2) source address and address-mask;

(3) TCP/UDP source port range

ii. destination entity attributes are in the set of destination entity criteria

(1) destination prefix and prefix-length;

(2) destination address and address-mask;

(3) TCP/UDP destination port range

iii. ICMP type/code

iv. IP protocol number

v. TCP flags: RST, SYN, ACK

vi. Packet fragmentation

(1) Whether the packet is a fragment;

(2) whether the packet is a first-fragment

FDP_IFF.1.3 The TSF shall enforce the **following additional information flow control rules: none.**

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **none**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

a) **The TOE shall reject requests for access or services where the source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;**

b) **The TSF shall drop requests in which the information received by the TOE does not correspond to an entry in the routing table;**

c) **The TSF shall deny information flows that do not conform to the layer 3 IP packet header specification;**

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within* ***a range of values 0[3] – 64***, within an administrator configurable period of time within a range of values 0 — 1440 minutes, unsuccessful authentication attempts occur related to **any claimed SR Linux administrator ID attempting to authenticate**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall **prevent SR Linux administrators from performing activities that require authentication until an action is taken by an SR Linux administrator, or until an administrator-defined time period (within a range of values 0 - 1440 minutes) has elapsed**.

6.2.4.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets (passwords) meet **for all local SR Linux users the password must meet the following:**

a) **minimum password length (8-12 characters);**

b) **maximum password length (8 - 1023 characters);**

c) **Complexity requirements:**

i. **at least one (1) numeric character must be present in the password;**

ii. **at least one (1) special character must be present in the password. Special characters include: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~;**

iii. **at least one (1) upper; and**

iv. **at least one (1) lower case character;**

d) **Password aging sets the number of days after which the user password expires and the user must update their password. The maximum number of days the password is valid shall be definable within a range of values of 1 – 500;**

e) **Force local users to change their password on the first login to the system; and**

f) **Configure the system to not allow the username in the password**.

6.2.4.3 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.

6.2.4.4 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide **client RADIUS, TACACS+, and local authentication mechanisms** to support SR Linux user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **authentication mechanism specified by the administrator**.

[3] A value of 0 indicates that unlimited unsuccessful authentication attempts is allowed.

6.2.4.5 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only **obscured feedback** to the administrative user while authentication is in progress.

6.2.4.6 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.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of, modify the behaviour of* the functions **listed in Table 14** to **the Administrator**.

Table 14: Security Functions

Security Functions
Configuring Banners
Configuring Management Access
Configuring ACLs
Configuring Password Management Parameters
Configuring Roles
Configuring Administrators
Configuring Remote administration
Configuring Inactivity Timeouts
Configuring RADIUS/TACACS+
Configuring Syslog
Configuring NTP

6.2.5.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the **Traffic Filtering SFP** to restrict the ability to *change_default, query, modify, delete* the security attributes **defined in FDP_IFF.1.1** to the **administrator with a role allowed to execute the corresponding commands**.

6.2.5.3 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the **Traffic Filtering 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 **administrators** to specify alternative initial values to override the default values when an object or information is created.

6.2.5.4 FMT_SMF.1 Specification of Management Functions

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

a) **reboot;**

b) **create, modify, or delete configuration parameters;**

c) **create, delete, empty, and review the audit trail;**

d) **create, delete, modify, and view filtering rules;**

e) **perform configuration backups;**

f) **password management; and**

g) **security management functions listed in Table 14: Security Functions**.

6.2.5.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the role~~s~~ **administrators**.

FMT_SMR.1.2 The TSF shall be able to associate users with role~~s~~.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable Time Stamps

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

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive CLI session after ~~a~~ an **administrator defined period of inactivity within a range of 0 to 4,294,967,295 seconds**.

6.2.7.2 FTA_SSL.4 User-initiated Termination

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

6.2.7.3 FTA_TAB.1 Default TOE access banners

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

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **audit server communications**.

6.2.8.2 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, disclosure*.

FTP_TRP.1.2 The TSF shall permit *remote 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*, ***all remote administrator actions***.

6.3 TOE SECURITY ASSURANCE REQUIREMENTS

The security assurance requirements for the TOE consist of the requirements corresponding to the EAL3 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Basic Flaw Remediation (ALC_FLR.1).

The assurance requirements for this evaluation are summarized in the following table.

Table 15: EAL 3+ Assurance Requirements

Assurance Class	Assurance Components	
	Identifier	**Name**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
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 requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.4 CC COMPONENT HIERARCHIES AND DEPENDENCIES

Table 16 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

Table 16: Functional Requirements Dependencies

SFR	Dependencies	Dependency Satisfied?
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes Yes - Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FAU_SAR.1	FAU_GEN.1	Yes
FCS_COP.1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Per Canadian Common Criteria program instructions v2.0, only CAVP certificates are required.
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes Yes
FIA_AFL.1	FIA_UAU.1	Yes - Satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_SOS.1	None	N/A
FIA_UAU.2	FIA_UID.1	Yes – Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FIA_UAU.5	None	N/A
FIA_UAU.7	FIA_UAU.1	Yes - Satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_UID.2	None	N/A
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Yes, via FDP_IFC.1 Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Yes – Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FPT_STM.1	None	N/A
FTA_SSL.3	None	N/A
FTA_SSL.4	None	N/A
FTA_TAB.1	None	N/A
FTP_ITC.1	None	N/A
FTP_TRP.1	None	N/A

6.5 SECURITY REQUIREMENTS RATIONALE

6.5.1 Security Functional Requirements Rationale

Table 17provides a bi-directional mapping of Security Functional Requirements to TOE Security Objectives. This table demonstrates that each of the applicable objectives for the TOE is addressed by at least one of the functional requirements and that each of the functional requirements address at least one of the objectives.

Following this table is rationale that discusses how each applicable TOE Security Objective is addressed by the corresponding Security Functional Requirements.

Table 17: Security Functional Requirements to TOE Security Objectives

Security Functional Requirement	O.AUDIT	O.CRYPTO	O.I&A	O.MANAGE	O.MEDIATE	O.PROT_COMMS	O.TOE_ACCESS
FAU_GEN.1 Audit Data Generation	X						
FAU_GEN.2 User Identity Association	X						
FAU_SAR.1 Audit Review	X						
FCS_COP.1 Cryptographic Operation		X				X	
FDP_IFC.1 Subset Information Flow Control					X		
FDP_IFF.1 Simple Security Attributes					X		
FIA_AFL.1 Authentication Failure Handling			X				
FIA_SOS.1 Verification of Secrets			X				
FIA_UAU.2 User Authentication Before Any Action			X				
FIA_UAU.5 Multiple Authentication Mechanisms			X				
FIA_UAU.7 Protected Authentication Feedback			X				
FIA_UID.2 User Identification Before Any Action			X				
FMT_MOF.1 Management of Security Functions Behaviour				X			
FMT_MSA.1 Management of Security Attributes				X			
FMT_MSA.3 Static Attribute Initialization				X	X		
FMT_SMF.1 Specification of Management Functions				X			
FMT_SMR.1 Security Roles				X			
FPT_STM.1 Reliable Time Stamps	X						
FTA_SSL.3 TSF-initiated Termination							X
FTA_SSL.4 User-initiated Termination							X
FTA_TAB.1 Default TOE access banners							X
FTP_ITC.1 Inter-TSF Trusted Channel						X	
FTP_TRP.1 Trusted Path						X	

The following subsections describe how each applicable TOE Security Objective is addressed by the corresponding Security Functional Requirements.

O.AUDIT *The TOE will generate audit records which will include the time that the event occurred and the identity of the administrator performing the event. The TOE will provide the privileged administrators the capability to review audit data and will restrict audit review to administrators who have been granted explicit read-access.*

The TOE generates audit records of security related events. The audit records include the time that the event occurred and the identity of the administrator performing the event. [FAU_GEN.1, FAU_GEN.2, and FPT_STM.1].

The TOE provides the privileged administrators the capability to review Audit data. [FAU_SAR.1].

O.CRYPTO *The TOE will provide cryptographic functionality capable of maintaining confidentiality and integrity of data.*

The TOE implements encryption, decryption, digital signature, and verification services, hashing services, and keyed-hash message authentication to provide confidentiality, integrity, and authentication services. The TOE implements the cryptographic operations defined in Table 13. [FCS_COP.1]

O.I&A *The TOE will uniquely identify and authenticate the claimed identity of all administrators before granting management access to control their actions.*

The TOE uniquely identifies and authenticates the claimed identity of all administrators before granting management access. Administrators authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. The interactive authentication data entered by the administrator is obscured from viewing as it is entered [FIA_UAU.7]. Before TOE allows any actions on behalf of the administrator, the administrator's identity is identified to the TOE [FIA_UID.2]. Multiple consecutive unsuccessful attempts to authenticate result in locking of the account until the administrator re-enables it or the administrator-configured length of time has passed [FIA_AFL.1]. The TOE checks passwords for aging, minimum length, login attempts, and complexity [FIA_SOS.1].

The TOE provides RADIUS, TACACS+, and local authentication mechanisms to support administrator authentication. [FIA_UAU.5]

O.MANAGE *The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.*

The TOE ensures that all administrator actions resulting in the access to TOE security functions and configuration data are controlled. The TOE provides the ability to restrict the use of TOE management/administration/security functions to authorized administrators of the TOE [FMT_MOF.1]. The TOE provides security management functions for use by authorized administrators, including reboot, and creating/modifying/deleting configuration parameters [FMT_SMF.1].

The TOE ensures that access to TOE security functions and configuration data is based on the assigned administrator role. [FMT_SMR.1].

The TOE restricts the ability to manage security attributes associated with the Traffic Filtering SFP to the administrator. [FMT_MSA.1]

The TOE allows the privileged administrator to specify alternate initial values when an object is created. [FMT_MSA.3].

O.MEDIATE *The TOE must mediate the flow of all information between hosts located on disparate internal and external networks governed by the TOE. The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.*

The TOE identifies the entities involved in the Traffic Filtering SFPs [FDP_IFC.1].

The Traffic Filtering SFPs defines the rules and conditions required for information to flow through/to the TOE. Information that is permitted to flow is then routed according to the information in the routing table [FDP_IFF.1].

The TOE implements a default accept policy for the information flow control security rules [FMT_MSA.3].

O.PROT_COMMS *The TOE provides communication channels for administrators. These communication channels authenticate the other endpoint and protect the data from unauthorized disclosure and modification during transmission to and from the TOE.*

The TOE provides a trusted communication channel between itself and an audit server. The connection provides assured identification of end points as well as confidentiality and integrity of data transmitted. [FTP_ITC.1]

The TOE implements trusted path channels to allow administrators to remotely connect to the TOE. Administrators are authenticated by the TOE before transmitting data or requests to and from the TOE. The trusted path channel provides confidentiality and integrity of the data transmitted between the administrator and the TOE. [FTP_TRP.1]

The TOE must implement encryption, decryption, digital signature, and verification services, hashing services, and keyed-hash message authentication in order to provide trusted communication and trusted path channels. [FCS_COP.1]

O.TOE_ACCESS *The TOE will provide mechanisms that control an administrator's logical access to the TOE and to explicitly deny access to specific administrators when appropriate.*

The TOE terminates an interactive Console or SSH sessions after an administrator defined time interval of administrator inactivity. [FTA_SSL.3]

The administrator is also able to terminate their own interactive session. [FTA_SSL.4]

The TOE displays an administrator-configurable message to users prior to session establishment using the CLI. [FTA_TAB.1]

6.5.2 Security Assurance Requirements Rationale

The TOE and this ST are EAL 3 conformant, augmented with basic flaw remediation (ALC_FLR.1). This combination is termed EAL 3+. This provides a level of independently assured security that is consistent with the postulated threat environment. Specification of EAL 3+ includes the vulnerability assessment component.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions (and supporting general technical mechanisms) of the TOE that meet the TOE security requirements defined in Section 6. The functions and functional requirements are cross-referenced in Section 7.2.

This section provides a description of the functions that are carried out by the TOE at the TOE external interfaces (TOE Security Functionality Interfaces (TSFI)).

7.1 TOE SECURITY FUNCTIONS

The TOE security functions that were previously introduced are described in more detail in this section.

7.1.1 Audit

7.1.1.1 Audit Data Generation

The SR Linux records the start-up of the audit functions and the reboot of the system which corresponds to the shutdown of the audit functions. It also generates an audit record of the following events:

a. *Log all login attempts.*

b. *Log successful configuration change activity of administrators*. The SR Linux logs the configuration change activity of the administrator in a security log (viewing of audit logs and configuration settings are not claimed). *The change activity event source is all events that directly affect the configuration or operation of the TOE as defined in the FMT_MOF.1, FMT_SMF.1, and FMT_SMR.1 SFRs)*;

c. *Security breach logging*. The security event source is all events that affect attempts to breach system security such as failed login attempts or attempts to access commands to which the administrator is not granted access. Security events are generated by the security application.

The SR Linux implements logging using the standard Linux syslog libraries, using rsyslog to filter logs and pass them on to remote servers. (Note: Sending logs to a remote server using rsyslog is not configured in the evaluated configuration.) The system is configured to specify a source for input log messages, filter the log messages, and specify an output destination for the log messages. Linux facilities and SR Linux subsystem are sources on which log messages can be filtered. The security-relevant records are generated from the audit, auth, authpriv, user facilities, as well as from the aaa, acl, app, and mgmt subsystems. SR Linux logs the activity of the administrator from the user facility. Filters can also be configured to control the generation of audit records at a specific priority.

The generating application, a unique event ID within the application, and a short text description is recorded for each applicable event in the audit log records. Audit log records are the means of recording system generated events for later analysis. Events are messages generated by applications or processes with the SR Linux.

Filters can also be used within the SR Linux to specify logging destinations for the audit log records. In the evaluated configuration, audit records must be sent to either a specified log file on disk, to a remote audit server or both. Audit log records can be sent to the following logging destinations:

- Specified Log file
    - Default directory: /var/log/srlinux/file/
    - Default maximum file size: 10 MB
    - Number of files to keep in rotation of files: four
- One or more remote audit servers (not allowed for use in the CC evaluated configuration as instructed in the CC guidance; SFTP can be used to manually transfer the logs to the syslog server)

- Memory buffer storage (not persistent across reboots; not allowed for use in the CC evaluated configuration as instructed in CC guidance)
- Console (/dev/console; not allowed for use in the CC evaluated configuration as instructed in CC guidance)

Log entries that are forwarded to a destination are formatted in a way appropriate for the specific destination, but log event entries have common elements or properties:

- Sequence number
- A time stamp in Universal Time Co-ordinated (UTC) or local time; and
- Severity
- The generating application:
  - A unique event ID within the application;
  - A subject identifying the affected object; and
  - A short text description (including outcome information).

The functionality described in this section implements FAU_GEN.1.

7.1.1.2 User Identity Association

For audit events resulting from actions of identified administrators, the SR Linux associates each auditable event with the identity of the administrator that caused the event.

The functionality described in this section implements FAU_GEN.2.

7.1.1.3 Audit Review

Authenticated administrators are able to read all the information in the specified log files using the CLI.

The administrator uses the CLI commands to determine the destination for the audit records. Audit records can be written to a specified filename located within the specified directory (default directory is /var/log/srlinux/file/).

The functionality described in this section implements FAU_SAR.1.

7.1.1.4 Reliable Time Stamps

The SR Linux synchronizes its local time with an NTP server in the operational environment. The SR Linux includes the date and time (using either UTC or local time as configured by the Administrator) within each audit record that it generates.

The functionality described in this section implements FPT_STM.1.

7.1.2 Cryptography

SR Linux utilizes OpenSSL 3.0.15 to implement encryption, decryption, digital signature, and verification services, hashing services, and keyed-hash message authentication in order to provide confidentiality, integrity, and authentication services. In the evaluated configuration, the TOE will be in FIPS mode. The TOE implements the cryptographic operations specified in Table 13.

Higher level network protocols utilize OpenSSL to implement SSH, TLS, and HTTPS for the purposes of:

- Transferring audit log files to the remote audit server using SFTP
- SSH session for CLI access
- gNMI management over HTTPS/TLS

The TOE implements an SFTP client to provide a trusted communication channel between itself and an audit server. The SFTP connection provides assured identification of end points as well as confidentiality and integrity of audit data transmitted from the TOE to the remote audit server. The SR Linux local and remote users of the TOE initiate all transmissions to the remote audit server. The TOE is configured to require mutual authentication with the remote audit server.

In the evaluated configuration, the following local systems must be attached to an internal trusted protected network that is only accessible by infrastructure devices and trusted administrators:

- a RADIUS or TACACS+ server for authentication / authorization services;
- Syslog servers for logging; and
- a Network Time Protocol (NTP) server for external time synchronization.

The TOE implements SSH, TLS and HTTPS to allow remote administrators to connect to the TOE over a trusted path channel. Administrators are authenticated using password-based authentication either locally or via RADIUS or TACACS+. The following trusted path channels are distinct communication paths provided by the TOE:

- TLS / HTTPS connections to the TOE from a gNMI management client. HTTP over TLS (HTTPS) utilizes cryptographic mechanisms to provide the ability to authenticate the endpoints and protect the data transmitted from modification and disclosure.
- SSH connections to the SR Linux CLI. SSH utilizes cryptographic mechanisms to provide the ability to remotely login to another system and execute commands over a protected channel.

Refer to Table 13: Cryptographic Specifications for a list of cryptographic algorithms in the TOE and the protocols utilize those algorithms. In addition, the TOE includes the Nokia SR Linux Cryptographic module (SRLCM) which has achieved the NIST Cryptographic Algorithm Validation (validation number A7218). The SRLCM utilizes OpenSSL 3.0.15 to implement the cryptographic operations.

The functionality described in this section implements FCS_COP.1, FTP_ITC.1 and FTP_TRP.1.

7.1.2.1 TLS Cipher Suites

The supported TLS v1.2 cipher suites in FIPS mode are:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

- TLS_RSA_WITH_AES_256_GCM_SHA384

The supported TLS v1.3 cipher suites are:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256

7.1.2.2 SSH Algorithms

The following algorithms are supported by the SSHv2 server when in FIPS mode.

The supported SSH key exchange algorithms are:

- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group16-sha512
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group14-sha256
- diffie-hellman-group18-sha512

The supported SSH server host key algorithms are:

- ecdsa-sha2-nistp256
- rsa-sha2-512
- rsa-sha2-256

The supported SSH encryption algorithms are:

- aes128-gcm@openssh.com
- aes256-gcm@openssh.com
- aes128-cbc
- aes256-cbc
- aes128-ctr
- aes256-ctr

The supported SSH message authentication code (MAC) algorithms are:

- hmac-sha2-256
- hmac-sha2-512
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com
- hmac-sha1
- hmac-sha1-etm@openssh.com

7.1.3 I&A

7.1.3.1 User Identification and Authentication

The SR Linux validates an administrator name and password combination when an administrator attempts to log in. SR Linux does not provide administrative access to the TOE prior to successful identification and authentication. SR Linux obscures passwords entered by the administrator.

SR Linux supports three user types: Linux users, SR Linux local users, and SR Linux remote users. Each user type is an administrative user and is authenticated via different mechanisms, as described below.

Linux users are configured in the underlying Linux OS, not in the SR Linux configuration. Linux user account information is stored in /etc/passwd in the underlying Linux OS. Linux users are logged directly into the bash shell. By default, the SR Linux has a single Linux user, linuxadmin, who can run all commands in the SR Linux CLI with administrative permissions. There is a default password for this user. Nokia recommends that this default user and password be changed during installation. Other Linux users can be added with the useradd command in the underlying Linux OS. Linux users with a UID less than 1500 are authenticated via the underlying Linux OS, not through the SR Linux aaa_mgr application. In the evaluated configuration, SR Linux will be configured to disable use of Linux users except during installation, setup and troubleshooting. Use of Linux users is outside the evaluated configuration.

SR Linux Local users are users configured within the SR Linux itself. By default, SR Linux supports a single local user, named admin. There is a default password for this user. Nokia recommends that this password is changed during installation. Additional SR Linux local users can be added as necessary.

SR Linux Remote users are configured on a remote server, which is queried when the user attempts to log in to the SR Linux device. Remote users are authenticated via RADIUS or TACACS+.

The order in which password authentication is processed among SR Linux users (RADIUS, TACACS+ and local passwords) is configured by the administrator. SR Linux local users and SR Linux remote users are considered administrators.

The SR Linux authentication function validates an administrator name and password combination when an administrator attempts to log in. When an administrator attempts to log in through the console, or remotely, each client (72x0 IXR) sends an access request to a RADIUS, TACACS+, or local database.

The functionality described in this section implements FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7.

7.1.3.2 Authentication Failure Handling

The TOE detects consecutive unsuccessful authentication attempts to SR Linux and takes actions based on administrator-configured parameters. When the defined number of unsuccessful authentication attempts has been met, the SR Linux will at the option of the Administrator prevent activities that require authentication until an action is taken by an administrator, or until an Administrator defined time period has elapsed.

The following is defined by the administrator for SR Linux authentication via any method:

a. The number of unsuccessful login attempts allowed during a specified time (default: 0 which allows for unlimited failed login attempts, within a range of values 0 – 64)

b. The period of time, in minutes, that a specified number of unsuccessful attempts can occur before the administrator is locked out (default 1 minute; within a range of values 0 — 1440 minutes),

c. The lockout period in minutes during which the administrator is not allowed to login (default: 15; within a range of values 0 - 1440 minutes, where 0 means that the user is locked out until an Administrator unlocks them;)

An SR Linux administrator can unlock their own account if they have a separate existing active session when the account is locked.

The functionality described in this section implements FIA_AFL.1.

7.1.3.3 Verification of Secrets

The password for all SR Linux local users is subject to the password complexity settings defined by the Administrator. In the evaluated configuration, the administrator must set the password as follows:

a. A minimum length (characters) of 8 - 12 characters;

b. A maximum non-hashed password length of 8 - 1023 characters;

c. at least one numeric character;

d. at least one special character. Special characters include: (!"#$ %&'()*+,-./:;<=>?@[\]^_`{|}~"); and

e. at least one upper and one lower case character.

In the CC evaluated configuration, administrators are instructed to only use the "admin" username account during setup and to create user unique administrator accounts for each human user.

SR Linux also implements a password aging feature which sets the number of days after which the user password expires and the user must update their password. The maximum number of days the password is valid shall be configurable within a range of values of 1 – 500.

As part of administrator account creation, one of the following flags is set, either:

a. Y - administrator must change his password at the next login; or

b. N - The administrator is not forced to change his password at the next login (default).

The TOE can also be configured to not allow the username in the password.

The functionality described in this section implements FIA_SOS.1.

7.1.4 Security Management

The SR Linux has a direct connection via the physical RS-232 console interface and a network connection to perform security management functions. The network interface is controlled via an information flow control as defined herein. The SR Linux requires local access to initially configure the TOE. Local console authentication access via a RS-232 port to the router uses administrator names and passwords to authenticate login attempts.

The TOE can be managed either locally or remotely. Local management is provided via the console using the CLI. The CLI can also be accessed remotely via SSH. Remote management is also provided using the gRPC Network Management Interface (gNMI) that is transmitted over HTTPS. (Note: The local Console used to interface with the CLI during installation and startup is outside the TOE boundary.)

Each of the management interfaces require the administrators to identify and authenticate themselves prior to requesting services from the TOE.

SR Linux local users and SR Linux remote users are considered administrators. In the evaluated configuration, Linux users are disabled and administrators may use bash only when executed from the CLI.

7.1.4.1 Security Management Functions

Administrator capabilities are controlled via the assignment of roles. Users can be assigned one or more roles that indicate the commands they are authorized to execute in the system. Roles define permissions to allow or disallow access to any command in the system's management down to the granularity of an individual

command. The following security functions are restricted to the administrators assigned a role allowed to execute the command. The SR Linux user admin has access to execute all commands.

The administrator will perform the following:

a. Reboot;

b. Configure authentication failure handling configurable integer of unsuccessful authentication attempts within configurable range of time, and configurable lock out period of time that occurs related to an administrator's authentication;

c. Configures authentication attempts count, time interval [minutes], and lockout time period [minutes];

d. Enable and configure RADIUS and/or TACACS+ (TOE client-side);

e. Configures authentication-order for local authentication, RADIUS and TACACS+;

f. Configures password management and complexity parameters;

g. Configures Access Control Lists;

h. Configures audit events and logs;

i. Configures user management and roles (used to deny or permit access to CLI command tree permissions, or specific CLI commands);

j. Configure SSH access;

k. Configure audit settings;

l. Configure the system time; and

m. Configure the system banners.

The functionality described in this section implements FMT_MOF.1, FMT_SMF.1.

7.1.4.2 Management of Traffic Filtering Security Attributes

The administrator specifies information flow policy rules (i.e., routing protocols and ingress/egress traffic ACLs) that contain information security attribute values, and an action that permits or disallows the information flow. When a packet arrives at the source interface, the information security attribute values of the packet are compared to each information flow policy rule and when a match is found the action specified by that rule is taken.

Subject and information security attributes used are:

a. IPv4 network address and port of source subject;

b. IPv4 network address and port of destination subject;

c. transport layer protocol and their flags and attributes (UDP, TCP);

d. network layer protocol (IP, ICMP); and

e. interface on which traffic arrives and departs.

The functionality described in this section implements FMT_MSA.1.

7.1.4.3 Static Attribute Initialization

SR Linux equipped systems arrive out-of-the-box configured with no services turned on and with direct console access only. In addition, no IP address is configured on the router by default. This requires physical or out-of-band console access in order to bring a new system up. The SR Linux requires local console access to initially configure an IP address and enable remote access.

Administrators are set up with an individual account configured to only allow the minimum access to perform the assigned support duties. The administrator is instructed in administrative guidance how to set and specify alternative initial default attribute values.

If the packet does not match any ACL rules, the default action is to permit the information flow.

The functionality described in this section implements FMT_MSA.3.

7.1.4.4 Security Roles

The SR Linux allows all authorized administrators with the required privilege to configure and control the associated features. Authorization features allow SR Linux local and SR Linux remote administrators to be assigned roles. The roles limit what CLI commands can be executed by authenticated administrators assigned to those roles. Roles consist of one or more rules which specify a schema path the role can have privileges for, and a corresponding action, which can be read, write, or deny. After authentication, a user is authorized to perform the assigned actions defined in the path for the role assigned to the user.

The Administrator role defined in FMT_SMR.1 is considered to include all possible role definitions.

When an administrator issues a command, the SR Linux processes the rules of the administrator's roles. If the administrator is authorized to issue the command, the command is executed. If the administrator is not authorized to issue the command, then the command is not executed.

The functionality described in this section implements FMT_SMR.1.

7.1.5 TOE Access

7.1.5.1 TSF-initiated Termination

The SR Linux allows configuring login control parameters for console and remote administration sessions.

The SR Linux can be configured to terminate stale (inactive) CLI sessions. The SR Linux terminates interactive CLI sessions after an administrator defined period of inactivity with a default value of 10 minutes (600 seconds), and within a range of 0 to 71,582,788.25 minutes (4,294,967,295 seconds), where 0 indicates that the system will not terminate inactive CLI sessions.

This idle-time parameter configures the idle timeout for SR Linux users and remote sessions before the session is terminated by the system. This would reduce the chance for the unauthorized administrators to access the router through an unattended opened session. By default, an idle time out is set at ten (10) minutes of inactivity. This timer is set per session.

The functionality described in this section implements FTA_SSL.3.

7.1.5.2 User-initiated Termination.

Administrators can initiate termination of their own sessions. The SR Linux allows an administrator to terminate their own session by issuing the command "logout" at the CLI prompt.

The functionality described in this section implements FTA_SSL.4.

7.1.5.3 TOE Access Banners

The SR Linux will display an administrator-configured message to users on the login screen prior to the user entering identification and authentication credentials.

The functionality described in this section implements FTA_TAB.1.

7.1.6 User Data Protection

7.1.6.1 Traffic Filtering Policy ACLs

The TOE enforces a Traffic Filtering SFP whereby the network packets sent through the TOE are subject to ACL rules setup by the administrator. Only IPv4 Interface filters and IPv4 CPM filters are included in the TSF. An IPv4 interface filter is an IPv4 ACL that restricts data traffic allowed to enter or exit the TOE. An IPv4 CPM filter is used to protect control plane traffic. The following ACLs are excluded from use in the evaluated configuration: IPv6 Interface filters, IPv6 Control plane module (CPM) filters, MAC filters, Packet capture filters, and System filters.

The TOE uses ACLs and protocol configuration and protocol state to enforce the Traffic Filtering SFP. The TCP/IP stack is implemented as a common protocol stack for IP, UDP and TCP communications.

Access Control Lists (ACLs) are an ordered set of rules that are evaluated on a packet-by-packet basis to determine whether access should be provided to services or network ports. ACLs control network traffic into (ingress) or out of (egress) a network port based on IPv4 matching criteria. ACLs are applied to packets entering or leaving network interface. Interface ACLs can be used on several interfaces. The same ACLs can be applied to ingress traffic, egress traffic, or both. Ingress filters affect only inbound traffic destined for the routing complex, and egress filters affect only outbound traffic sent from the routing complex. After evaluation by the IPv4 Interface filter, ingress packets that are terminating packets are extracted to the CPM and are processed by the IPv4 CPM filters.

All traffic passing through the router is processed by the ACL attached to the interface/ protocol. The ACL prevents an unknown party (identified by IP match) to access the router/switch's infrastructure and service layer, and provide security protections of both layers.

Each ACL rule has a sequence ID. The rules within an ACL are evaluated starting with the rule with the lowest sequence ID, progressing to the rule with the highest sequence ID. ACL rule evaluation stops at the first matching ACL rule and the associated action is performed with no further evaluation. The ACL is processed until the first match is made. The TOE compares the match criteria specified within an ACL to packets coming through the system. When a packet matches all the parameters specified in a rule, the system takes the specified action. If a packet does not match the rule parameters, the packet continues through the ACL process and is compared to the next rule, and so on. If the packet does not match any of the rules, then by default system accepts the packet. To drop traffic not matching an ACL entry, an administrator can configure an entry in the ACL with the highest sequence ID to drop all traffic.

The administrator specifies ACLs (ingress/egress traffic filtering) that contain information security attribute values, and associate with that rule an action that permits the information flow or disallows the information flow. When a packet arrives at the source interface, the information security attribute values of the packet are compared to each information flow policy rule and when a match is found the action specified by that rule is taken. The set of identifiers are associated with the physical router interfaces.

Subject and information security attributes used are:

a. IPv4 network address, and port of source subject;

b. IPv4 network address and port of destination subject;

c. transport layer protocol and their flags and attributes (UDP, TCP);

d. network layer protocol (IP, ICMP);

e. packet fragmentation;

f. interface on which traffic arrives and departs.

When a packet matches an ACL entry, the action specified by the ACL entry is applied to the packet. Secondary actions are not included in the evaluated configuration.

For traffic passing through the router, ACL entries support the following actions:

- accept – Allow the packet through to the next processing function.
- drop – Discard the packet without ICMP generation.

All traffic that successfully clears the ACLs is processed by the routing tables. The routing table is processed top-down, with processing continuing until the first match is made. The routing table may be statically updated by a privileged administrator or dynamically through routing protocols.

The SR Linux provides automatic detection of attacks triggered by excessive control plane and routing protocol traffic, and it recognizes signatures of some common Distributed and other DoS (D/DoS) attacks and further it will suppress these attacks using the ACLs.

The functionality described in this section implements FDP_IFC.1 and FDP_IFF.1.

7.1.6.2 Traffic Filtering Policy Static Filtering

In addition to filtering by administrator defined ACLs, network packets with attributes (that typically represent malicious traffic and have no common application in other contexts) listed below are rejected by the TOE.

a. The TOE shall reject requests for access or services where the source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;

b. The TSF shall drop requests in which the information received by the TOE does not correspond to an entry in the routing table;

c. The TSF shall deny information flows that do not conform to the layer 3 IP packet header specification;

The functionality described in this section implements FDP_IFF.1.

7.2 TOE SECURITY FUNCTIONS RATIONALE

Table 18 provides a bi-directional mapping of Security Functions to Security Functional Requirements. It shows that each of the SFRs is addressed by at least one of the Security Functions and that each of the Security Functions addresses at least one of the SFRs. For a description of how each Security Functional Requirement is addressed by the corresponding Security Function refer to Section 7.1.

Table 18: Security Functions to SFR Mapping

Security Functional Requirement	Audit	Cryptography	I&A	Security Management	TOE Access	User Data Protection
FAU_GEN.1 Audit Data Generation	X					
FAU_GEN.2 User Identity Association	X					
FAU_SAR.1 Audit Review	X					
FCS_COP.1 Cryptographic Operation		X				
FDP_IFC.1 Subset Information Flow Control						X
FDP_IFF.1 Simple Security Attributes						X
FIA_AFL.1 Authentication Failure Handling			X			
FIA_SOS.1 Verification of Secrets			X			
FIA_UAU.2 User Authentication Before Any Action			X			
FIA_UAU.5 Multiple Authentication Mechanisms			X			
FIA_UAU.7 Protected Authentication Feedback			X			
FIA_UID.2 User Identification Before Any Action			X			
FMT_MOF.1 Management of Security Functions Behaviour				X		
FMT_MSA.1 Management of Security Attributes				X		
FMT_MSA.3 Static Attribute Initialization				X		
FMT_SMF.1 Specification of Management Functions				X		
FMT_SMR.1 Security Roles				X		
FPT_STM.1 Reliable Time Stamps	X					
FTA_SSL.3 TSF-initiated Termination					X	
FTA_SSL.4 User-initiated Termination					X	
FTA_TAB.1 Default TOE access banners					X	
FTP_ITC.1 Inter-TSF Trusted Channel		X				
FTP_TRP.1 Trusted Path		X				

8 OTHER REFERENCES

This section lists references other than the TOE guidance documentation presented in Section 1.6.3.2 that either aid in better understanding the TOE or are referred to directly in this Security Target.

[ANSI X3.64] *Additional Controls for Use with the American National Standard Code for Information Interchange*, ANSI X3.64-1979(R1990), American National Standards Institute (ANSI)

[IEEE 802.3ad] *Amendment to Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications-Aggregation of Multiple Link Segments*, IEEE Standard 802.3ad-2000, Institute of Electrical and Electronic Engineers

[RFC 1305] *Network Time Protocol (Version 3) Specification, Implementation and Analysis*, RFC 1305, March 1992, Internet Engineering Task Force

[RFC 2138] *Remote Authentication Dial In User Service (RADIUS)*, RFC 2138, April 1997, Internet Engineering Task Force

[RFC 2865] *Remote Authentication Dial In User Service (RADIUS)*, RFC 2865, June 2000, Internet Engineering Task Force

[RFC 2866] *RADIUS Accounting*, RFC 2866, June 2000, Internet Engineering Task Force

[RFC 4250] *The Secure Shell (SSH) Protocol Assigned Numbers*, RFC 4250, January 2006, Internet Engineering Task Force

[RFC 4251] *The Secure Shell (SSH) Protocol Architecture*, RFC 4251, January 2006, Internet Engineering Task Force

[RFC 4252] *The Secure Shell (SSH) Authentication Protocol*, RFC 4252, January 2006, Internet Engineering Task Force

[RFC 4253] *The Secure Shell (SSH) Transport Layer Protocol*, RFC 4253, January 2006, Internet Engineering Task Force

[RFC 4254] *The Secure Shell (SSH) Connection Protocol*, RFC 4254, January 2006, Internet Engineering Task Force

[RFC 5424] *The Syslog Protocol*, RFC 5424, March 2009, Internet Engineering Task Force

[RFC 8907] *The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol*, RFC 8907, September 2020, Internet Engineering Task Force

[TIA-232-F] *Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, October 1 1997, Telecommunications Industry Association (TIA)