Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

IP Router

ITSAR Number: ITSAR20101YYMM
ITSAR Name: NCCS/ITSAR/Transport Equipment/IP Routers/IP Router

Date of Release: DD.MM.YYYY
Date of Enforcement:

Version: 2.0.0

MTCTE के तहत जारी:
Issued under MTCTE by:
राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत
National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

Sr. No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	IP Router	ITSAR201011811	1.0.0	12.11.2018	First Release
2.	IP Router	ITSAR201012401	1.0.1	03.01.2024	Editorial Changes
3.	IP Router	ITSAR20101YYMM	2.0.0	DD.MM.YYYY	Second Release

Table of Contents

A) Outline

The objective of this document is to present comprehensive, country-specific security requirements for the IP Routers. The IP Routers are the equipment used for routing IP packets using various routing protocols and user defined routing policies. They find their use in TSP and ISP networks and other networks as Edge Routers, MPLS Routers and Core Routers. IP Routers facilitate the IP connectivity of a network to various access networks, internet or enterprise networks.

The specifications developed by various regional/international standardization bodies/organizations/associations like ETSI, ENISA, 3GPP, Telecommunications Standards Development Society of India (TSDSI) et. al. along with the country-specific security requirements are the basis for this document. The Telecommunication Engineering Centre (TEC)/ TSDSI references made in this document implies that the respective clause has been adopted as it is or with certain modifications.

This document commences with a brief description of the router, types of routers followed by a brief about IP routers, their functionalities and then proceeds to address the common and entity specific security requirements of the IP router.

B) Scope

This document targets on the security requirements of IP router. This ITSAR applies to all types of IP Routers, including but not limited to: Conventional Routers (with or without line card expansion), SDN-based Routers, Cloud-Native Routers (CNF), Virtual Routers (VNF), and Cloud-Managed Routers, as well as similar implementations. The applicability extends across all deployment modes, such as Edge Routers, Core Routers, Access Routers, MPLS Routers and Aggregation Routers. All clauses are universally applicable to all types of IP Routers unless explicitly stated otherwise. Additionally, all CSR clauses shall be extended to relevant components of IP Router implementations, including but not limited to VNF/CNF, NFVI, SDN, APIs, dynamic routing protocols, and other related entities, wherever applicable. Furthermore, any clause specified for IPv4 shall also apply to IPv6.

C) Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or recommended denotes that a particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes the opposite meaning of (3) above.

Chapter 1: Overview

1.1 Introduction

A router is a device that connects networks to each other. Routers operate at Layer 3 (Network Layer) of OSI model. It forwards data packets from one location (host) to another until they reach their destination. Routers are responsible for receiving, analyzing and forwarding data packets among the connected networks. Though routers do their packet forwarding operations in the Network Layer, they do support higher layer protocols for operation and maintenance purposes and lower layer protocols for ethernet connectivity over electrical or optical interfaces.

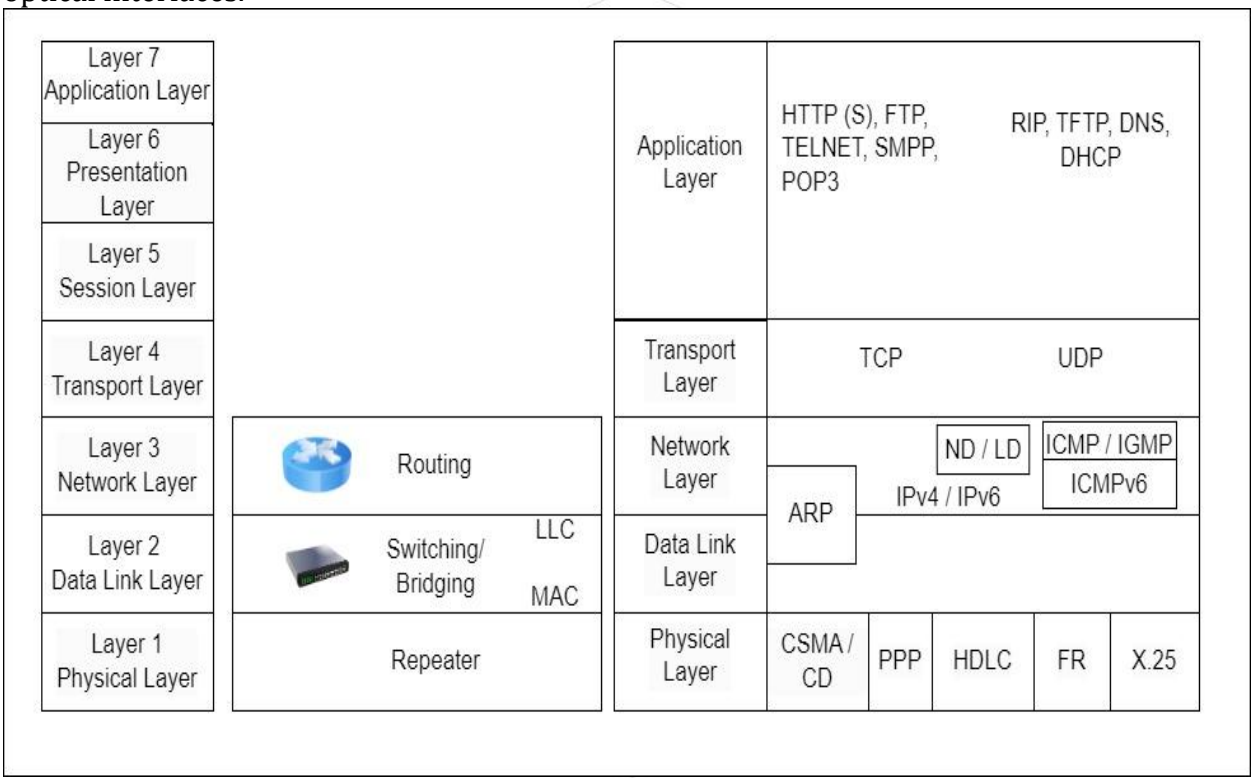

Fig 1: Positioning of a Router in OSI/TCP-IP Model

The router looks at the Layer 3 Packet Header (IP Header) to forward a packet to its intended destination. It determines the fastest path for the packet to reach its destination. However, individual router along the way does not need to determine the complete route, but rather just the next hop on the way to the final destination. The router does this by consulting an internal routing table which contains a list of paths to various destination networks. These paths can be predefined (e.g static routing, default routes and directly connected networks) or dynamically decided most efficient path, based on current network status (e.g dynamic routing using protocols such as RIP, EIGRP, OSPF, IS-IS, BGP etc.).

1.2 Router Architecture

The basic components of a router include:

- Routing Processor (CPU & Memory)
- Switch Fabric
- Input Ports
- Output Ports

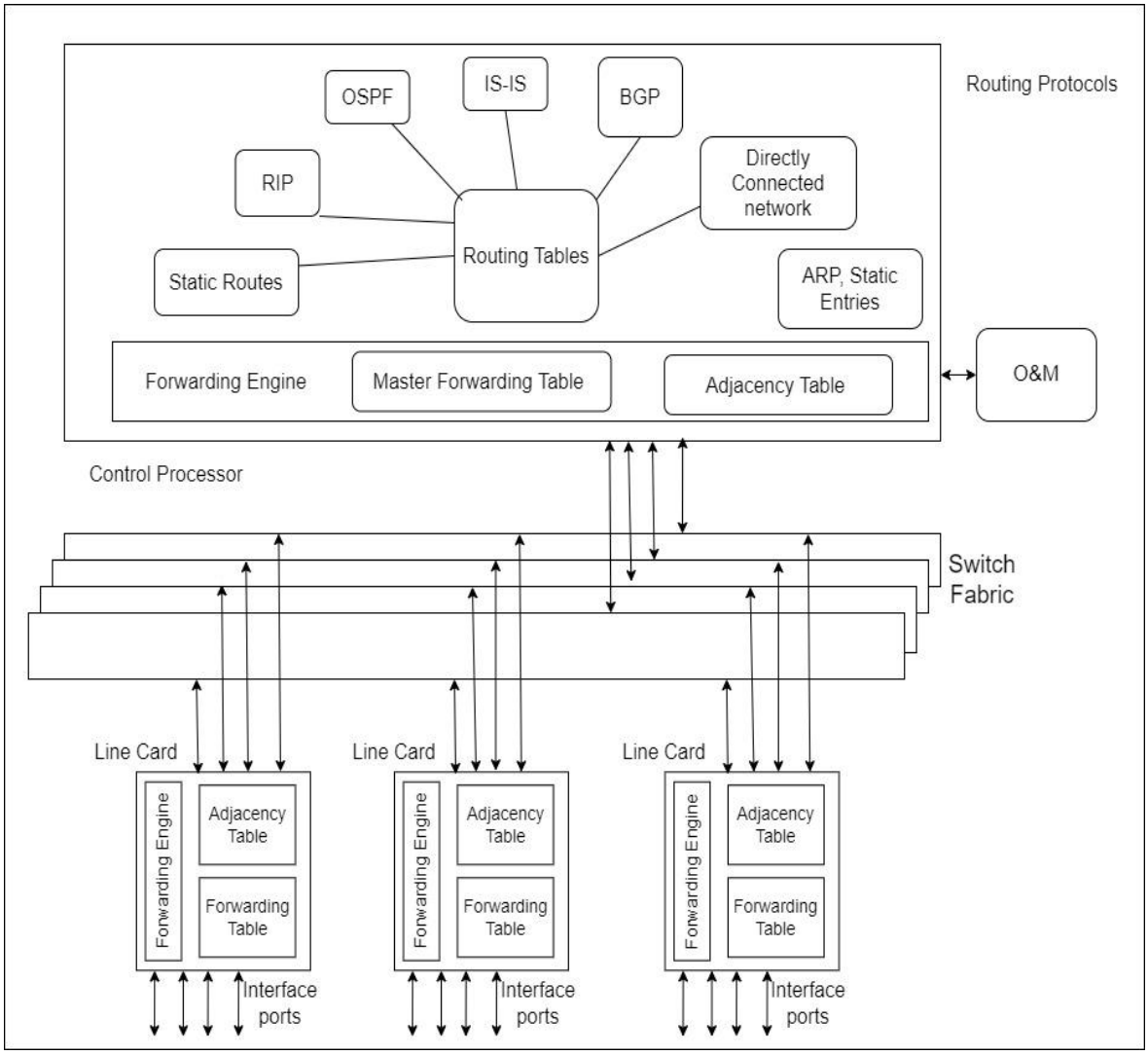

Fig 2: Router Architecture

The major functions of Routing Processor (CPU & Memory) include storing & maintaining of routing tables and link status, compute forwarding tables, execute routing protocols and perform the O & M activities. The switch fabric interconnects input ports to output ports. Input ports terminate the physical connections (ethernet interface) at the router and carry out data link layer & physical layer functionality. Control plane that carries routing protocol information, are exchanged between input/output ports to the routing processor. The input port uses the forwarding table to look up the output port to forward the packet via switch

fabric. Output ports store the packet received from the switch fabric and execute data link layer and physical layer functions and transmit the packets to the outgoing link. Usually the ports are duplex, and the same physical port will act as input as well as output ports.

Simple routers follow a centralized architecture where a single general-purpose CPU run all the control and forwarding functions. Such routers have a shared memory, shared bus & switch fabric. These are known as First Generation Routers. There are Second generation Routers with multiple centralized forwarding engines. In a router architecture with distributed forwarding engines, the forwarding engines are distributed to the line cards to enable them to make packet forwarding decisions locally. The control engine is only responsible for building the master Forwarding Table from its Routing Table, and then distributing copies of that master table information to the line cards.

Additionally, there are SDN (Software Defined Network) routers where the control plane (routing protocols) is separated from the forwarding hardware (NIC) and implemented as a software function. SDN based routers bring programmability and cheaper implementation with the use of general-purpose hardware.

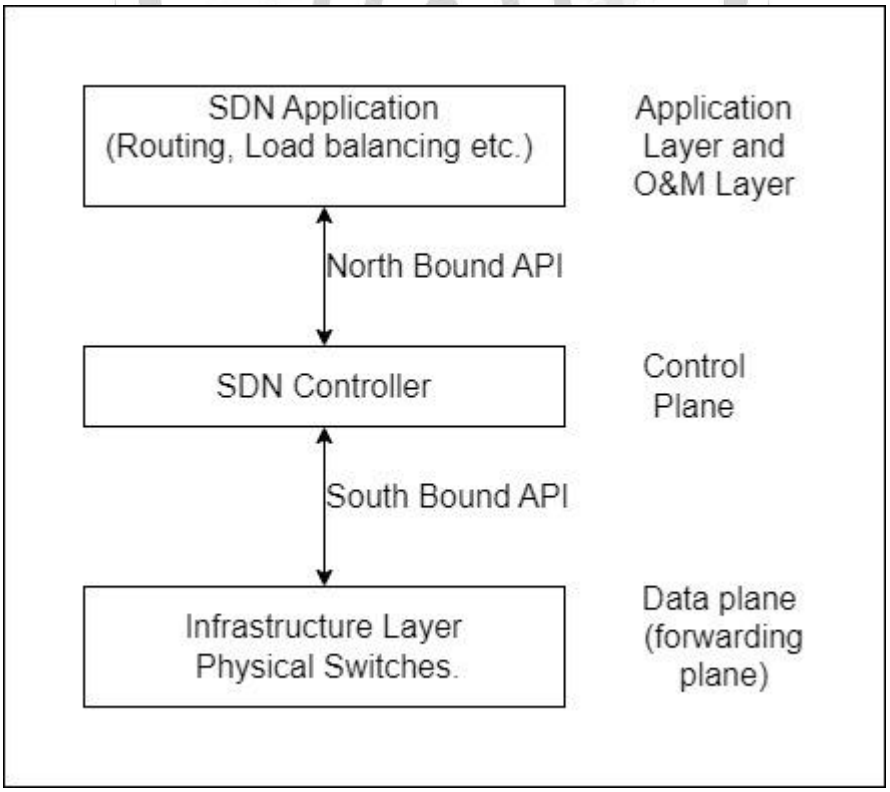

Fig 3: SDN Router Architecture

1.3 Types of Routers based on Deployments

Based on the type of deployments, the routers can be classified as follows:

a) **Core router:** Core Routers are used by large enterprises, ISPs, TSPs and cloud service providers etc. These routers handle high volumes of data packets within the network such as Internet Backbone.

b) **Edge router:** An edge router communicates with core routers and external networks. They reside at the "edge" of a network. Typical use cases include PE (Provider Edge), BNG (Broadband Network Gateway), Data Centre Edge, etc.

This classification does not distinguish the security requirements of a router product.

1.4 Router Classifications

From the security perspective, router architecture implementations can be classified into four types.

a) **Conventional Routers**: Conventional Routers consist of Control Engine (handling control plane), Forwarding Engines (data plane packet forwarding), input and output ports (usually duplex ports either electrical or optical), management interfaces and a switch fabric (to interconnect various ports). All these components are implemented in single unit (with centralized or distributed forwarding plane) with optional capability for interface expansion using line cards.

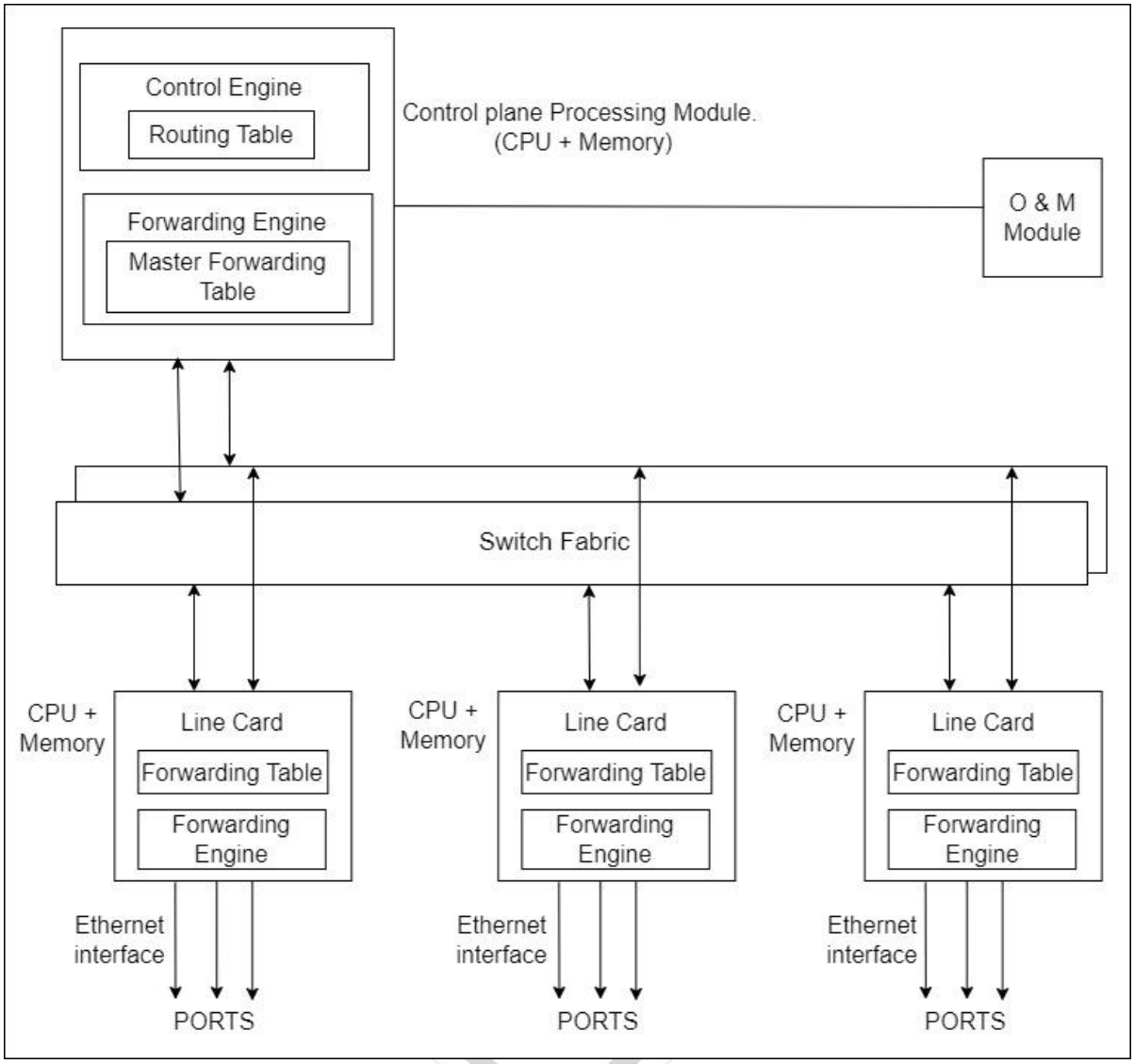

Fig. 4: Conventional Router Architecture

b) SDN Routers: In a conventional router network, each router has its own data plane as well as the control plane. The control plane of various routers exchange topology information (control plane traffic) and construct a forwarding table that decides where an incoming data packet must be forwarded to via the data plane. In an SDN router, the control plane is separated from the forwarding plane and is implemented in a centralized unit called the SDN controller. The O & M plane also is implemented in a centralized location. The centralized function is typically implemented as a VNF. Network administrator can shape traffic via a centralized console without having to configure individual routers. CUPS routers are also a special case of SDN routers.

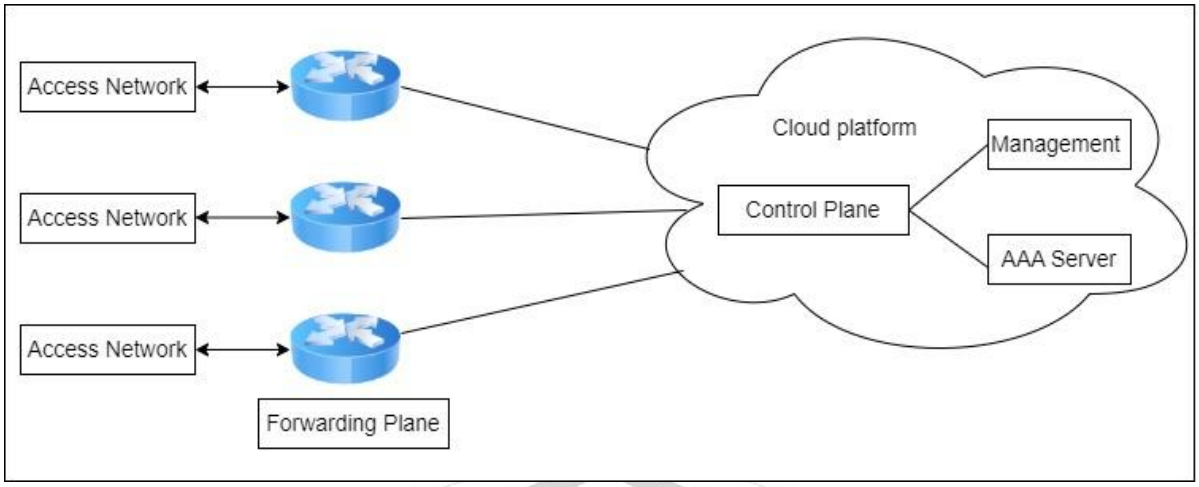

Fig 5A: The SDN based router architecture

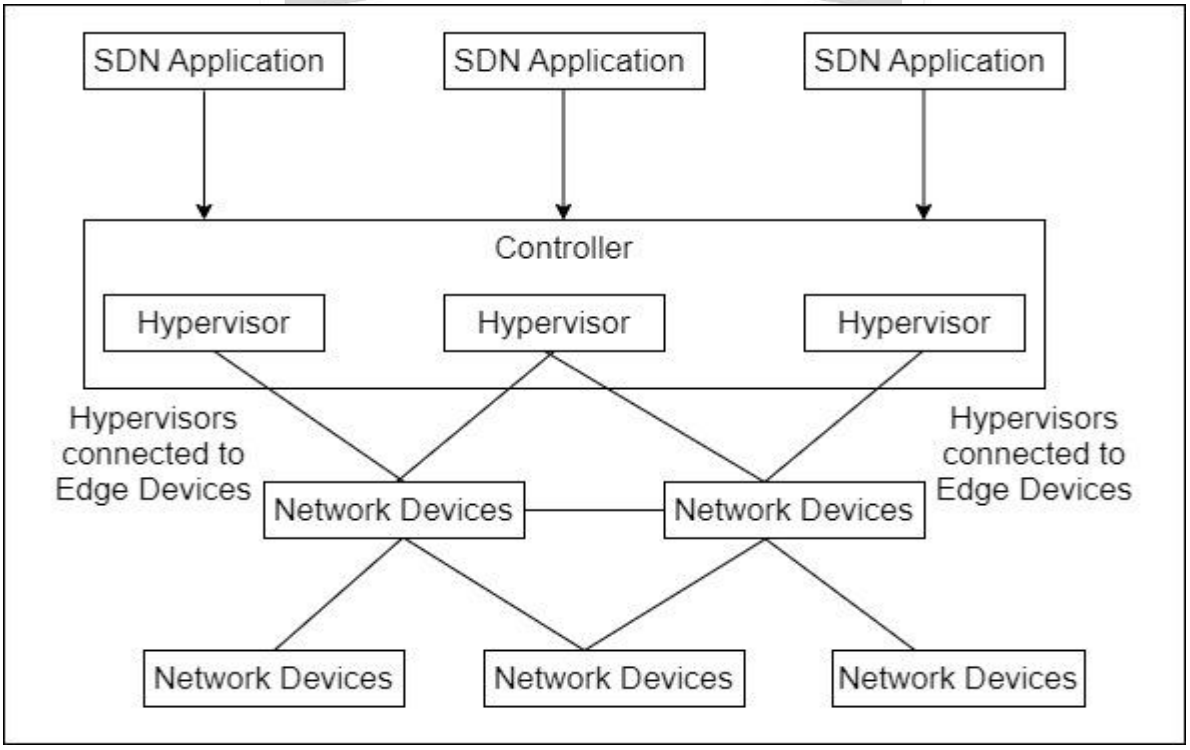

Fig 5B: SDN Via Hypervisor

c) Cloud Native Routers: The entire router implementations are done as a Cloud Native Function with hardware acceleration. The essential components of the router such as control plane and forwarding plane are implemented as a containerized solution. The forwarding plane may be enhanced for faster operations using hardware acceleration techniques such as DPDK, eBPF XPD etc. These routers typically find their applications delay sensitive applications such as Distributed RAN, 5G Edge Cloud, MAEC etc. They generally have L2 & L3 deployment modes. Cloud Native Routers also permit SDN modes, by separating the control plane from the forwarding plane.

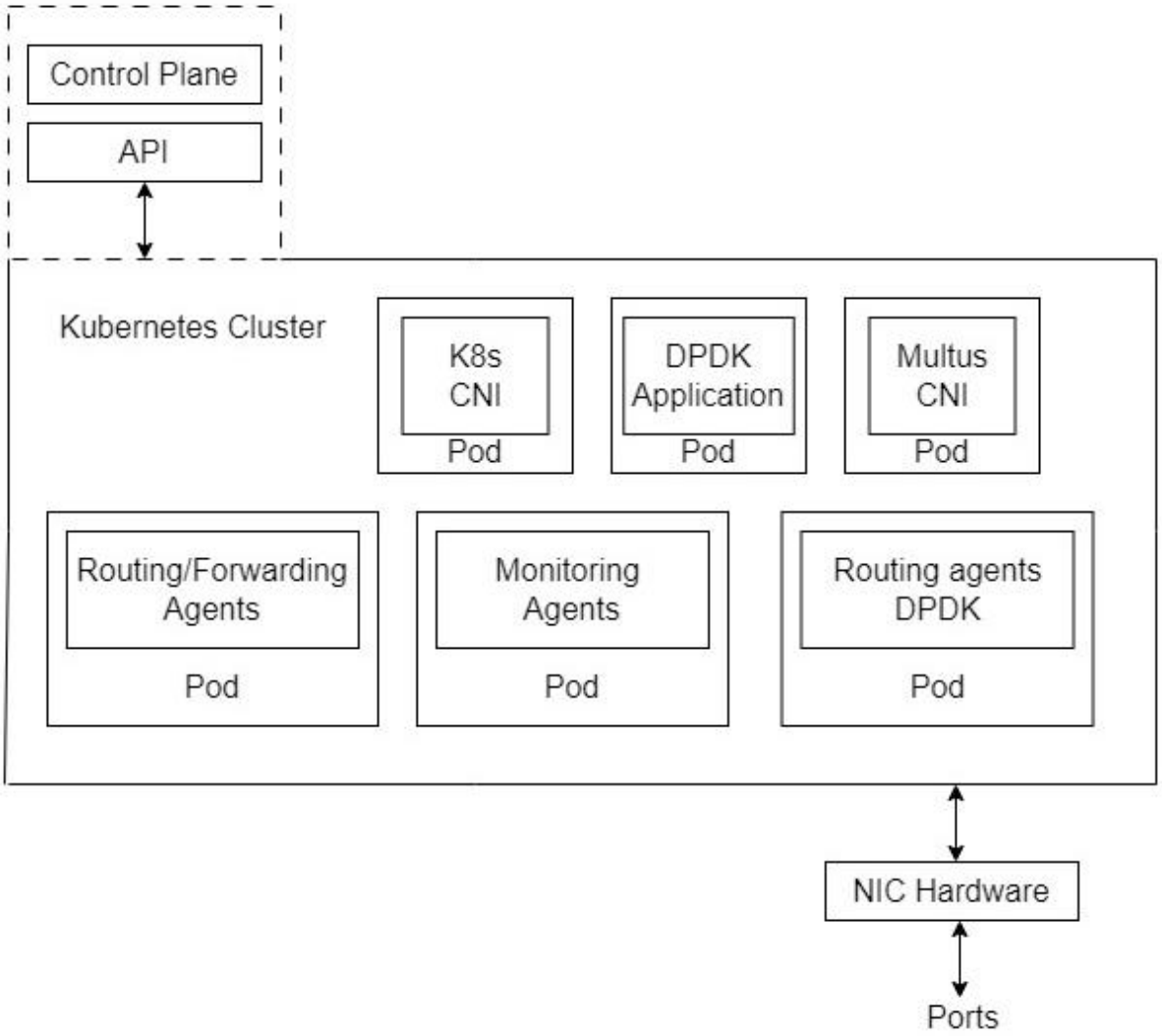

Fig 6: Cloud Native Router Architecture

d) Virtual Routers: Virtualized Router is a form of network functions virtualization (NFV), where the functions of conventional routers are implemented in a software that can be run on standard commercial off-the-shelf (COTS) hardware.

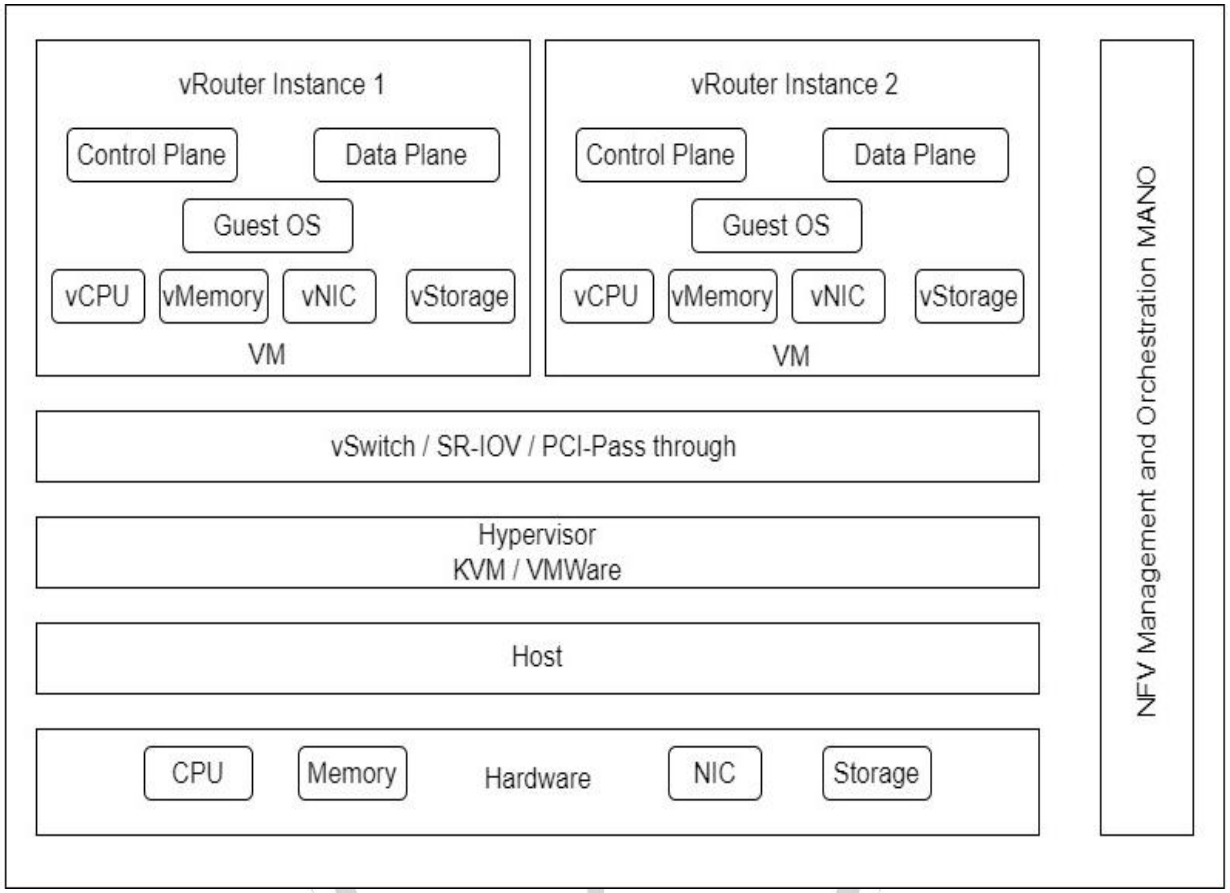

Fig 7: Virtual Router

e) Cloud Managed Routers: In a Cloud Managed Router, the management plane of the router is implemented either on a public cloud or on an on-premise cloud. Control plane and Data Planes are distributed across the devices and management plane is centralized. The cloud-based management plane may include Network Automation, Network Monitoring, Deployment Configurations etc. The cloud-based O & M plane may manage Conventional Routers, Virtual Routers or Cloud Native Routers as per the deployment scenario.

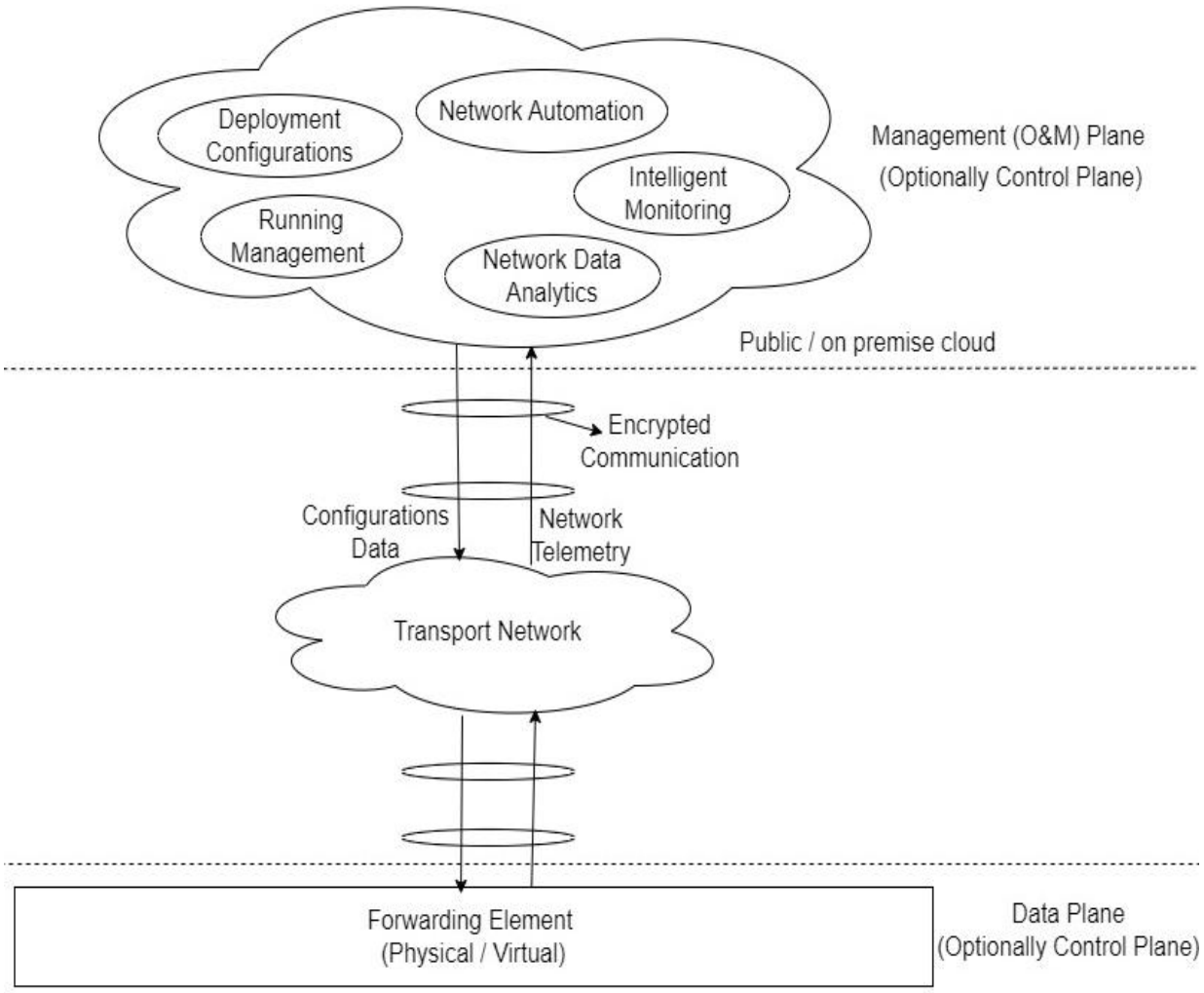

Fig 8: Cloud Managed Routers

Note: Any of the routers listed above can have an optional Wireless LAN interface also.

The various modes of router implementations demand for extended security testing to take care of the requirements such as cloud implementations, SDN implementations, APIs etc.

Chapter 2: Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Authentication for Product Management and Maintenance interfaces

Requirement:

IP Router shall support mutual authentication of entities on management interfaces. The authentication mechanism can rely on the management protocols used for the interface or other means.
Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used for IP Router management and maintenance.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

IP Router management traffic (information exchanged during interactions with OAM) shall be protected strictly using secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR For Cryptographic Controls" only.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.2.4]

2.1.3 Role-Based access control policy

Requirement:

The IP Router shall support Role Based Access Control (RBAC). A role-based access control system shall use a set of controls which determines how users interact with domains and resources. The domains could be Fault Management (FM), Performance Management (PM), System Admin, etc. The RBAC system shall control how users or groups of users are allowed access to the various domains and what type of operation they can perform, i.e. the specific operation command or command group (e.g. View, Modify, Execute).

The IP Router shall support RBAC with minimum of 3 user roles, in particular, for OAM privilege management for network product Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface. The RBAC shall be applicable to API users also.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.4.6.2]

2.1.4 User Authentication – Local/Remote

Requirement:

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute shall be used, which, when combined with the username, shall enable unambiguous authentication and identification of the authorized user.
Authentication attributes include:

- **Cryptographic keys**
- **Token**
- **Passwords**

This means that authentication based on a parameter that can be spoofed (e.g. phone numbers, public IP addresses or VPN membership) shall not be permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

Minimum two of the above Authentication attributes shall be mandatorily combined for protecting all the accounts from misuse. An exception to this requirement is local access and machine accounts where at least one authentication attribute shall be supported

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

Direct Login to IP Routers as root or equivalent highest privileged user shall be limited to the system console only. Root user shall not be allowed to login to IP Router remotely.
This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provide remote access to the IP Router.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.6]

2.1.6 Authorization Policy

Requirement:

The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.

Authorizations to IP Router shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g. configuration and logging files).

Alongside access to data, execution of applications and components shall also take place with

rights that are as low as possible. Applications should not be executed with administrator or system rights.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the IP Router. IP Router shall support the assignment of individual accounts per user, where the user could be a person, or, for Machine Accounts, an application, or a system. IP Router shall not enable the use of group accounts or group credentials, or sharing of the same account between several users

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.1.2]

Section 2.2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:

The usage of a system function without successful authentication, on the basis of the user identity and at least two authentication attributes shall be prevented. For machine accounts and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

Requirement:

If the IP Router supports external authentication mechanism such as AAA server (for authentication, authorization, and accounting services), then the communication between IP Router and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

2.2.3 Protection against brute force and dictionary attacks

Requirement:

Protection against brute force and dictionary attacks that hinder authentication attribute (i.e. password) guessing shall be implemented.
Brute force and dictionary attacks aim to use automated guessing to ascertain passwords for user and machine accounts.
Various measures or a combination of the following measures shall be taken to prevent this.

i) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
ii) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking as an attacker can force this to deactivate accounts and make them unusable.
iii) Using CAPTCHA to prevent automated attempts (often used for Web applications).
iv) Using a password blacklist to prevent vulnerable passwords.

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by IP Router.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

a) The configuration setting shall be such that IP Router shall only accept passwords that comply with the following complexity criteria:

   i) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the IP Router). It shall not be possible to set this absolute minimum length to a lower value by configuration.
   ii) Password shall mandatorily comprise all the following four categories of characters:
      1) At least 1 uppercase character (A-Z)
      2) At least 1 lowercase character (a-z)
      3) At least 1 digit (0-9)
      4) At least 1 special character (e.g., @;!$.)

b) The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.
c) If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this sub-clause.
d) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the IP Router.
e) When a user is changing a password or entering a new password, IP Router/central

system shall check and ensure that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g., application-level, OS-level, etc.).

f) Passwords shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.1]

2.2.5 Inactive Session Timeout

Requirement:

An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period. IP Router shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on pre-configured timers. Unlocking the session shall be permissible only by user authentication. If the inactivity period further continues for a defined period, session/user ID timeout must occur after this inactivity. Re-authentication of the OAM user shall be repeated following any period of inactivity lasting 15 minutes or longer.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used; it shall be possible to implement this function on this system.

Password change shall be enforced after initial login (after successful authentication).

IP Router shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. IP Router shall support a configurable period for expiry of passwords.

Previously used passwords shall not be allowed up to a certain number (Password History).

The number of disallowed previously used passwords shall be:

a) Configurable;

b) Greater than 0;

c) And its minimum value shall be 3. This means that the IP Router shall store at least the three previously set passwords. The maximum number of passwords that the IP Router can store for each user is up to the manufacturer.

When a password is about to expire, a password expiry notification shall be provided to the user.

Above requirements shall be applicable for all passwords used (e.g., application-level, OSlevel, etc.). An exception to this requirement is machine accounts.

IP Router shall have an in-built mechanism to support this requirement. If a central system is

used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause.
And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the IP Router.
The minimum password age shall be set as one day i.e., recycling or flipping of passwords to immediate return to favourite password is not possible.
The password shall be changed (need not be automatic) based on key events including, not limited to

- Indication of compromise (IoC)
- Change of user roles
- When a user leaves the organization

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.2]
[Ref : CIS_Benchmarks_Password_Policy_Guide_v21.12]

2.2.7 Protected Authentication feedback

Requirement:

The Authentication attributes shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password are replaced by a character such as "*".

This requirement shall be applicable for all authentication attributes used (e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, Original Equipment Manufacturer (OEM) or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on first time login to the system or the OEM provides instructions on how to manually change it.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 5.2.3.4.2.3]

2.2.9 Logout Function

Requirement:

The IP Router shall have a function that allows a signed-in user to logout at any time. All processes under the logged-in user ID shall be terminated on logout. IP Router shall be able to continue to operate without interactive sessions.

Only for debugging purposes, processes under a logged-in user ID may be allowed to continue to run after detaching the interactive session.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.5.1]

2.2.10 Policy regarding consecutive failed login attempts

Requirement:

a) The maximum permissible number of consecutive failed user account login attempts shall be configurable by the operator. The definition of the default value set at manufacturing time for the maximum number of failed user account login attempts shall be less than or equal to 8, typically 5. After the maximum permissible number of consecutive failed user account login attempts is exceeded by a user, there shall be a block delay in allowing the user to attempt login again. This block delay and the capability to set the period of the block delay, e.g., double the delay, or 5 minutes delay, or 10 minutes delay, after each login failure should be configurable by the operator. The default value set at manufacturing time for this delay shall be greater than or equal to 5 sec.

b) If supported, infinite (permanent) locking of an account that has exceeded the maximum permissible number of consecutive failed user account login attempts shall also be possible via configuration, with the exception of administrative accounts, which shall get only temporarily locked.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.5]

2.2.11 Suspend accounts on non-use

Requirement:

It shall be possible for the system to automatically suspend an account after 'X' days without a valid login.

Note: X may be specified by operator. It can be implemented centrally also.

[Ref: CIS Password Policy Guide]

Section 2.3: Software Security

2.3.1 Secure Update

Requirement:

a) Software package integrity shall be validated during the software update stage.

b) IP Router shall support software package integrity validation via cryptographic means, e.g.,

digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, the IP Router shall have a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update originated from only these sources.
b) Tampered software shall not be executed or installed if integrity check fails.
c) A security mechanism is required to guarantee that only authorized user can initiate and deploy a software update and modify the list mentioned in (b) above.

Note: Code signing (valid and not time expired) is also allowed as an option in (b) above.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

a) Software package integrity shall be validated during the software upgrade stage.
b) IP Router shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, the IP Router shall have a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software upgrade originated from only these sources.
c) Tampered software shall not be executed or installed if integrity check fails.
d) A security mechanism is required to guarantee that only authorized users can initiate and deploy a software upgrade and modify the list mentioned in (b) above.

Note: Code signing (valid and not time expired) is also allowed as an option in (b) above.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:

i) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at Telecom Security Testing Laboratory (TSTL) premises or at the mutually agreed location for source code review by the designated TSTL. It shall be supported by furnishing the Software Test Document (STD).
ii) Also, OEM shall submit the undertaking as below:
    a. Industry standard best practices of secure coding have been followed during the entire development life cycle of the IP Router software which includes OEM developed code, third party software and open-source code libraries used/embedded in the IP Router.

    b. IP Router software shall be free from Common Weakness Enumeration (CWE) top 25, Open Worldwide Application Security Project (OWASP) top 10 security vulnerabilities

and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.

c. The binaries for IP Router and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in (ii) above.

[Ref : https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html]
[Ref: https://owasp.org/www-project-top-ten/]
[Ref : https://owasp.org/www-project-api-security/]

2.3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that IP Router is free from all known malware and backdoors as on the date of offer of IP Router to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the IP Router to the designated TSTL.

2.3.5 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the IP Router shall not be present/configured. Orphaned software components /packages shall not be present in IP Router. OEM shall provide the list of software that are necessary for IP Router's operation. In addition, OEM shall furnish an undertaking as "IP Router does not contain software that is not used in the functionality of IP Router."

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.3]

2.3.6 Unnecessary Service Removal

Requirement:

IP Router shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services shall be initially configured to be disabled on IP Router by the OEM except if services are needed during deployment. In that case those services shall be disabled according to OEM's instructions after deployment is done. Disabled protocols may still need to be enabled for other reasons by the operators, e.g., remote diagnostics.

IP Router shall not support following services:

a. File Transfer Protocol (FTP)

b. Trivial File Transfer Protocol (TFTP)
c. Telnet
d. rlogin, Rate Control Protocol (RCP), Remote Shell Protocol (RSH)
e. HTTP
f. Simple Network Management Protocol (SNMP) v1 and v2
g. SSHv1
h. Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Small Servers (Echo, Chargen, Discard and Daytime)
i. Finger
j. Bootstrap Protocol (BOOTP) server
k. Discovery protocols (Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP))
l. IP Identification Service (Identd)
m. Packet Assembler/Disassembler (PAD)
n. Maintenance Operations Protocol (MOP)

Any other protocols, services that are vulnerable are also to be permanently disabled.
Full documentation of required protocols and services (communication matrix) of the IP Router and their purpose needs to be provided by the OEM as a prerequisite for the test case.

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:

The IP Router shall boot only from the memory devices intended for this purpose.

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.3.2]

2.3.8 Secure Time Synchronization

Requirement:

IP Router shall establish a secure communication channel through standard interface with the Network Time Protocol (NTP) / Precision Time Protocol (PTP) server as per appropriate TEC ER (essential requirement) document.

IP Router shall establish a secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” with NTP/PTP server. IP Router shall generate audit logs for all changes to time settings.

IP Router shall support NTPv4 or later version to ensure secure time synchronization.

Note: RFC 8915 which proposes Network Time Security (NTS) as an extension field for the NTP version 4 is also permitted.

[Ref: RFC 5905]

2.3.9 Restricted reachability of services

Requirement:

IP Router shall restrict the reachability of services so that they can only be reached on interfaces meant for the purpose. On interfaces where services are active, the reachability shall be limited to legitimate communication peers. This limitation shall be realized on the IP Router itself (without external measures e.g., firewall, at network side) according to the requirement detailed in section 2.7.1 Traffic Filtering. Administrative services (e.g., SSH, Hyper Text Transfer Protocol Secure (HTTPS), Remote Desktop Protocol (RDP)) shall be restricted to interfaces in the management plane to support separation of management traffic from user traffic.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.2]

2.3.10 Self-Testing

Requirement:

The IP Router's cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up during System bootup/restart. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e. security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

Section 2.4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:

Unused functions i.e. the software and hardware functions which are not needed for operation or functionality of the IP Router shall be permanently deactivated. Permanently means that they shall not be reactivated again after the IP Router's reboot. If unused functions of software cannot be deleted or uninstalled individually as required in clause "2.3.5 No unused software" of the present document, such functions shall be deactivated in the configuration of IP Router permanently.
The list of hardware and software functions installed in the system shall match with the ones that have been mentioned and deemed necessary for the operation of the IP Router.

EXAMPLE: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the IP Router.
[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:

OEM to ensure that the IP Router shall not contain software and hardware components that are no longer supported by them or their 3rd Parties (e.g., vendor, producer or developer) including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be provided by OEM.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.5]

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

IP Router shall not contain any access mechanism which is unspecified or not declared. An undertaking shall be given by the OEM as follows:
The IP router does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel.

Section 2.5: User Audit

2.5.1 Audit trail storage and protection

Requirement:

The security event log of IP Routers shall be access controlled (file access rights), so only privilege users shall have access to read the log files but shall not be allowed to delete the log files. This requirement shall be applicable to Administrator also.

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0. V.1.0.0 section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:

The IP Router shall log all security events with unique System References such as IP Address, MAC address, hostname, etc. It shall be possible to log the events as given in the Table below. The IP Router shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.
Additional audit record information, depending on the audit event, shall also be provided as given in the Table below

Sr. No.	Event Types (Mandatory or Optional)	Description	Event data to be logged
1.	Incorrect login attempts (Mandatory)	Records any user's incorrect login attempts to the IP router	Username
			Source (IP address) if remote access
			Outcome of event (Success or failure)
			Timestamp
2.	Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username
			Timestamp
			Length of session
			Outcome of event (Success or failure)
			Source (IP address) if remote access
3.	Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable.	Administrator username
			Administered account
			Activity performed (configure, delete, enable and disable)
			Outcome of event (Success or failure)
			Timestamp
4.	Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have	Value exceeded
			Value reached
			(Here suitable threshold values shall be defined depending on the individual system.)

		exceeded their defined thresholds.	Outcome of event (Success or failure)
			Timestamp
5.	Configuration change (Mandatory)	Changes to configuration of the IP Router	Change made
			Timestamp
			Outcome of event (Success or failure)
			Username
6.	Reboot/shutdown/ crash (Mandatory)	This event records any action on the IP Router that forces a reboot or shutdown OR where the network device/IP Router has crashed.	Action performed (boot, reboot, shutdown, etc.)
			Username (for intentional actions)
			Outcome of event (Success or failure)
			Timestamp
7.	Interface status change (Mandatory)	Change to the status of interfaces on the IP Router (e.g., shutdown)	Interface name and type
			Status (shutdown, down, missing link, etc.)
			Outcome of event (Success or failure)
			Timestamp
8.	Change of group membership or accounts (Mandatory)	Any change of group membership for accounts	Administrator username
			Administered account
			Activity performed (group added or removed)
			Outcome of event (Success or failure)
			Timestamp

9.	Resetting Passwords (Mandatory)	Resetting of user account passwords by the Administrator	Administrator username
			Administered account
			Activity performed (configure, delete, enable and disable)
			Outcome of event (Success or failure)
			Timestamp
10.	Services (Mandatory)	Starting and Stopping of Services (if applicable)	Service Identity
			Activity performed (start, stop, etc.)
			Timestamp
			Outcome of event (Success or failure)
11.	X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
			Reason for failure
			Subject identity
			Type of event
12.	Secure update (Mandatory)	Attempt to initiate manual update, initiation of update, completion of update	User identity
			Timestamp
			Outcome of event (Success or failure)
			Activity performed
13.	Time change (Mandatory)	Change in time settings	Old value of time
			New value of time
			Timestamp

			Origin of attempt to change time (e.g., IP address)
			Subject identity
			Outcome of event (Success or failure)
			User identity
14.	Session unlocking /termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session	User identity (wherever applicable)
			Timestamp
			Outcome of event (Success or failure)
			Subject identity
			Activity performed
			Type of event
15.	Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorized remote administrators (Optional)	Initiation, Termination and Failure of trusted Communication paths	Timestamp
			Initiator identity (as applicable)
			Target identity (as applicable)
			User identity (in case of Remote administrator access)
			Type of event
			Outcome of event (Success or failure, as applicable)
16.	Audit data changes (Mandatory)	Changes to audit data including deletion of audit data	Timestamp
			Type of event (audit data deletion, audit data modification)

			Outcome of event (Success or failure)
			Subject identity
			User identity
			Origin of attempt to change time (e.g., IP address)
			Details of data deleted or modified
17.	User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
			Origin of attempt (IP address)
			Outcome of event (Success or failure)
			Timestamp
18	Access Control Policy violations	Any failure of a packet to match an ACL rule allowing traversal of the router	Date /Time stamps, The source, destination and protocol attributes of the Traffic
19	attempt to initiate manual software update, initiation of software update, completion of update	Logs generation	user identity, Timestamp, Outcome of event (Success or failure), Activity performed
20	All use of identification and authentication mechanism	All use of identification and authentication mechanism	user identity, origin of attempt (e.g.IP address), Timestamp, outcome of event (Success or failure

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:

a. IP Router shall support forwarding of security event logging data to an external system available by push or pull mechanism through diverse links.
b. Log functions shall support secure uploading of log files to a central location or to a system external for the IP Router.
c. IP Router shall be able to store the generated audit/log data locally. The memory for this purpose shall be dimensioned to cater for the continuous storage of two days of audit/log data. OEM shall submit justification document for sufficiency of local storage requirement.
d. Secure Log export shall comply with the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.6.2]

Section 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:

IP Router shall communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

OEM shall submit to TSTL, the list of the connected entities with IP Router and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing communication with each entity and any other details required for verifying this requirement.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the IP Router (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports. An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the IP Router (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards."

[Ref : 1. ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019
2. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf]

2.6.3 Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithm implemented inside the Crypto module of IP Router shall be in compliance with the respective latest FIPS standards (for the specific crypto algorithm). Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.
An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithms implemented inside the Crypto module of IP Router is in compliance with the respective latest FIPS standards (for the specific crypto algorithm embedded inside the IP Router)."

2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

a) When the IP Router is in normal operational mode (i.e. not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear text to users and administrators.

Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e., PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration.

b) Access to maintenance mode shall be restricted only to authorized privileged users.

[Ref : TSDSI STD T1.33.117-17.1.0 V1.1.0. Section 4.2.3.2.2.]

2.6.5 Protecting data and information in storage

Requirement:

a. For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of IP Router that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with appropriate non-repudiation controls.

b. In addition, the following rules apply for:

   i) Systems that need access to identification and authentication data in the clear/readable form e.g., in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by

implementation-specific means.

ii) Systems that do not need access to sensitive data (e.g., user passwords) in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

iii) Stored files in the IP Router shall be protected against manipulation strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

IP Router shall have protection against creating a copy of data in use / data in transit. Protective measure shall exist against use of available system functions / software residing in Network product to create copy of data for illegal transmission. The software functions and components in the IP Router for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement:

a) IP Router shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound overt channels such as, HTTPS, Instant Messaging (IM), Peer to Peer (P2P), Email etc. shall be forbidden if they are auto-initiated by / auto originated from the IP Router.
c) Session logs shall be generated for establishment of any session initiated by either user or IP Router.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) IP Router shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit (within its boundary).
b) Establishment of outbound covert channels and tunnels such as Domain Name System (DNS) Tunnel, HTTPS Tunnel, Internet Control Message Protocol (ICMP) Tunnel, Transport Layer Security (TLS), Secure Sockets Layer (SSL), SSH, Internet Protocol Security (IPSec), Virtual Private Network (VPN), Real-time Transfer Protocol (RTP) Encapsulation etc. shall be forbidden if they are auto-initiated by / auto-originated from the IP Router.
c) Session logs shall be generated for establishment of any session initiated by either user or IP Router.

Section 2.7: Network Services

2.7.1 Traffic Filtering – Network Level

Requirement:

The IP Router shall provide a mechanism to filter incoming IP packets on any IP interface. (Refer to RFC 3871). In particular, the IP Router shall provide a mechanism:

a) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.

b) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions shall be supported:

i. Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.

ii. Accept: the matching message is accepted.

iii. Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action shall be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

c) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.

d) To filter on the basis of the value(s) of any portion of the protocol header.

e) To reset the accounting.

f) IP router shall provide a mechanism to disable/enable each defined rule.

[Ref: 1. TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.6.2.1

2. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2 Traffic Separation

Requirement:

The IP Router shall support the physical or logical separation of traffic belonging to different network domains. For example, OAM traffic and control plane traffic belong to different network domains. Refer to RFC 3871 for further information.

[Ref: 1. TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.5.1]
2. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.3 Traffic Protection –Anti-Spoofing

Requirement:

Systems shall not process IP packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.3.1.1]

Section 2.8: Attack Prevention Mechanisms

2.8.1 Network Level and application-level DDoS

Requirement:

IP Router shall have protection mechanisms against Network-level and Application-level Distributed Denial of Service (DDoS) attacks

IP Router shall provide security measures to deal with overload situations which may occur as a result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided. Potential protective measures may include:

a) Restricting available RAM per application

b) Restricting maximum sessions for a Web/Database application

c) Defining the maximum size of a dataset

d) Restricting Central Processing Unit (CPU) resources per process

e) Prioritizing processes

f) Limiting amount or size of transactions of an user or from an IP address in a specific

g) Limiting amount or size of transactions to an IP address/Port Address in a specific time range

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.1]

2.8.2 Excessive Overload Protection

Requirement:

IP Router shall act in a predictable way if an overload situation cannot be prevented. IP Router shall be built in this way that it can react on an overload situation in a controlled way. However, it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that the IP Router cannot reach an undefined and thus potentially insecure state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.
The OEM shall provide a technical description of the IP Router Over Load Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements).

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.3.3.3]

2.8.3 Filtering IP Options

Requirement:

IP packets with unnecessary options or extension headers shall not be processed by IP Router. IP options and extension headers (e.g. source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered by the IP Router.

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.4.1.1.3]

2.8.4 Interface Robustness Requirements

Requirement:

IP Router shall not be affected in its availability or robustness by incoming packets, from other network elements, that are manipulated or differing the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of IP Router. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.

Examples of such packets are:

a. Mass-produced TCP packets with a set Synchronize (SYN) flag to produce half-open TCP connections (SYN flooding attack).
b. Packets with the same IP sender address and IP recipient address (Land attack).
c. Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).
d. Fragmented IP packets with overlapping offset fields (Teardrop attack).
e. ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IP version 4 (IPv4) packets (Ping-of-death attack).
f. Uncorrelated reply packets (i.e. packets which cannot be correlated to any request).

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.2.6.2.2]

Section 2.9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of IP Router are reasonably robust when receiving unexpected input

Note: Vendor is expected to provide the list of protocols supported by the IP Router

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.4.4]

2.9.2 Port Scanning

Requirement:

It shall be ensured that on all network interfaces of IP Router, only documented ports on the transport layer respond to requests from outside the system.

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:

The purpose of vulnerability scanning is to ensure that there no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on IP Router, both in the OS and in the applications installed, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.

The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide a remediation plan.

Sr. No.	CVSS Score	Severity	Remediation
1	9.0 - 10.0	Critical	To be patched immediately
2	7.0 - 8.9	High	To be patched within a month
3	4.0 - 6.9	Medium	To be patched within three months
4	0.1 - 3.9	Low	To be patched within an year

Zero-day vulnerabilities shall be remediated immediately or as soon as possible.

[Ref : 1. TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.4.3
2. https://nvd.nist.gov/vuln-metrics/cvss
3. GSMA NG 133 Cloud Infrastructure Reference Architecture]

Section 2.10: Operating System

2.10.1 Growing Content Handling

Requirement:

a) Growing or dynamic content shall not influence system functions of IP Router.
b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop IP Router from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided. The countermeasures are usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the IP Router. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk.

ICMP message types which on receipt lead to responses or to configuration changes are not mentioned in this requirement, but they may be necessary to support relevant and specified networking features. Those must be documented.

Certain ICMP types are generally permitted and do not need to be specifically documented.

The IP Router shall not send certain ICMP types by default, but it may support the option to enable utilization of these types (e.g. for debugging). This is marked as "Optional" in below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A

3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet Too Big	Permitted	N/A
N/A	135	Neighbour Solicitation	Permitted	Permitted
N/A	136	Neighbour Advertisement	Permitted	N/A

The IP Router shall not respond to, or process (i.e. do changes to configuration), under any circumstances, certain ICMP message types as marked in below table.

Type (IPv4)	**Type (IPv6)**	**Description**	**Send**	**Respond to**	**Process (i.e. do changes to configuration)**
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e. as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.4.1.1.2]

2.10.3 Authenticated Privilege Escalation only

Requirement:

IP Router shall not support privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:

Each system user account in IP Router shall have a unique User ID (UID) with appropriate non-repudiation controls.

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.2.2]

2.10.5 OS Hardening - Minimized kernel network functions

Requirement:

OEM shall submit the process for OS Hardening undertaken to justify that the OS is sufficiently hardened and Kernel based applications / functions not needed for the operation of the Network product are deactivated.
OEM to provide information on steps taken in this regard. In particular, the following ones shall be disabled by default:

a) IP Packet Forwarding between different interfaces of the IP Router.
b) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
c) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.)
d) IPv4 Multicast handling. In particular, all packets with IP source or destination address belonging to the multicast IP ranges (224.0.0.0 through 239.255.255.255) shall be discarded by default and multicast route caching and forwarding shall be disabled to prevent Smurf and Fraggle attacks. A configuration option shall be available to enable the IPv4 multicast handling if required.
e) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.3.1.2]

2.10.6 No automatic launch of removable media

Requirement:

IP Router shall not automatically launch any application when a removable media device such as Compact Disk (CD), Digital Versatile Disk (DVD), Universal Serial Bus (USB)-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.3.1.3]

2.10.7 Protection from buffer overflows

Requirement:
IP Router shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by OEM.

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.3.1.5]

2.10.8 External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in IP Router in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.
OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g., USB drive, CD ROM etc.) for data transfer.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.3.1.6]

2.10.9 File-system Authorization privileges

Requirement:

IP Router shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.2.7]

2.10.10 SYN Food Prevention

Requirement:

IP Router shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.3.1.4]

2.10.11Handling of IP options and extensions

Requirement:

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g., source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.
[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.2.4.1.1.3]

2.10.12Restrictions on running Scripts / Batch-processes

Requirement:

Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, IP Router shall have feature to restrict Scripts / Batchprocesses / Macros usage among various users. It shall be possible to administratively configure scheduled tasks usage i.e. Cron-Job usage (permit / deny) among various users like Normal users, privileged users.

2.10.13Restrictions on Soft-Restart

Requirement:

IP Router shall restrict software-based system restart options usage among various users. The software reset / restart either through command or use of key-combinations like CTRL+ALT+DEL is not available to normal users for prevention of unintended / malicious trigger of system reset / restart.

Section 2.11: Web Servers

This entire section of the security requirements is applicable if the IP Router supports web management interface.

2.11.1 HTTPS

Requirement:

The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirement ITSAR" only.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.5.1]

2.11.2 Webserver logging

Requirement:

Access to the webserver (both successful as well as failed attempts) shall be logged by IP Router. The web server log shall contain the following information:

1) Access timestamp
2) Source (IP address)
3) Account (if known)
4) Attempted login name (if the associated account does not exist)

5) Relevant fields in http request. The URL should be included whenever possible.
6) Status code of web server response

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.5.2.1]

2.11.3 HTTP input validation

Requirement:

The IP Router Web Server shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks. The IP Router Web Server shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.5.4]

2.11.4 No system privileges

Requirement:

No web server processes shall run with system privileges. This is best achieved if the web server runs under an account that has minimum privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.2]

2.11.5 No unused HTTP methods

Requirement:

HTTP methods that are not required for IP Router operation shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0 section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for IP Router operation. In particular, Common Gateway Interface (CGI) or other scripting components, Server Side Includes (SSI), and Web based Distributed Authoring and Versioning (WebDAV) shall be deactivated if they are not required.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.4]

2.11.7 No compiler, interpreter, or shell via CGI or other server- side scripting

Requirement:

If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory - or other corresponding scripting directory - shall not include compilers or interpreters.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.5]

2.11.8 No CGI or other scripting for uploads

Requirement:

If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.6]

2.11.9 No execution of system commands with SSI

Requirement:

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:

Access rights for IP Router web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.

[Reference: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0 section 4.3.4.8]

2.11.11 No default content

Requirement:

Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the IP Router web server shall be removed.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.9]

2.11.12 No directory listings

Requirement:

Directory listings (indexing) / "Directory browsing" shall be deactivated.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.10]

2.11.13 Web server information in HTTP headers

Requirement:

The HTTP header shall not include information on the version of the IP Router web server and the modules/add-ons used.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.11]

2.11.14 Web server information in error pages

Requirement:

User-defined error pages shall not include version information about the IP Router web server and the modules/add-ons used. Error messages shall not include internal information such as internal
server names, error codes, etc. Default error pages of the IP Router web server shall be replaced by error pages defined by the OEM

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:

File type- or script-mappings that are not required for IP Router operation shall be deleted, e.g. php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.13]

2.11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g. via links or in virtual directories) in the IP Router web server's document directory. In particular, the IP Router web server shall not be able to access files which are not meant to be delivered.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0 section 4.3.4.14]

2.11.17HTTP User sessions

Requirement:

To protect user sessions the IP Router web server shall support the following session ID and session cookie requirements:

a) **The session ID shall uniquely identify the user and distinguish the session from all other active sessions.**

b) **The session ID shall be unpredictable.**

c) **The session ID shall not contain sensitive information in clear text (e.g. account number, social security, etc.).**

d) **In addition to the Session Idle Timeout the IP Router Web server shall terminate automatically sessions after a configurable maximum lifetime. This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.**

e) **Session ID's shall be regenerated for each new session (e.g. each time a user logs in)**

f) **The session ID shall not be reused or renewed in subsequent sessions**

g) **The IP Router shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.**

h) **Where session cookies are used the attribute 'Http Only' shall be set to true**

i) **Where session cookies are used the 'domain' attribute shall be set to ensure that the**

cookie can only be sent to the specified domain.

j) **Where session cookies are used the 'path' attribute shall be set to ensure that cookie can only be sent to the specified directory or sub-directory.**

k) **The IP Router shall not accept session identifiers from GET/POST variables.**

l) **The IP Router shall be configured to only accept server generate session ID's.**

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.5.3]

2.11.18 Execute rights exclusive for CGI/Scripting directory

Requirement:

If CGI or other scripting technology is used, only the CGI/Scripting directory shall be configured with execute rights. Other directories used or meant for web content shall not have execute rights.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.15]

Section 2.12: Other Security requirements

2.12.1 Remote Diagnostic Procedure – Verification

Requirement:
If the IP Router is providing Remote access for troubleshooting purposes/alarm maintenance then it shall be allowed only for authorized users, other than the root user.
All activities performed by the remote user are to be logged by the IP Router with the following parameters:
a) User id
b) Time stamp
c) Interface type
d) Event type (e.g., CRITICAL, MAJOR, MINOR)
e) Command/activity performed
f) Result type (e.g., SUCCESS, FAILURE).
g) IP Address of remote machine

[Ref: GSMA NG 133: GSM Association Non-confidential Official Document NG.133 –

2.12.2 No System Password Recovery

Requirement:

In the event of system password reset, the entire configuration of the IP Router shall be

irretrievably deleted.
No provision shall exist for password recovery.

2.12.3 Secure System Software Revocation

Requirement:

Once the IP Router software image is legally updated/upgraded with New Software Image, it shall normally not be possible to roll back to a previous software image. In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls.
IP Router shall support a well-established control mechanism for rolling back to previous software image.

2.12.4 Software Integrity Check – Installation

Requirement:

IP Router shall validate the software package integrity before the installation stage strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.
Tampered software shall not be executed or installed if integrity check fails.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

2.12.5 Software Integrity Check – Boot

Requirement:

The IP Router shall verify the integrity of a software component by comparing the result of a measurement of the component, typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" to the expected reference value.

2.12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

IP Router shall support the mechanism to verify both the physical and logical interfaces exist in the product. Physical and logical accessible interfaces (except console interface) which are not under use shall be disabled so that they remain inactive even in the event of reboot.

Note: List of the default used Physical/Logical Interfaces/Ports as given by the OEM shall match the list of Physical/Logical Interfaces/Ports that are necessary for the operation of the

IP Router.

2.12.7 Predefined accounts shall be deleted or disabled

Requirement:

Predefined or default user accounts (other than Admin/Root) in IP Router shall be deleted or disabled.

[Ref TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.2.2]

2.12.8 Control Plane Traffic Protection

Requirement:

Control plane traffic shall be protected in the IP Router by using Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls".

2.12.9 Security Algorithm Modification

Requirement:

When IP Router is establishing session/ communication channel with any other Network element, or while communication in the progress, IP Router shall have protection against a downgrade attack/bidding down attack for the use of a weaker algorithm.

Chapter 3: Specific Security Requirements

Section 3.1: Routing Related Requirements

3.1.1 Control Plane Traffic

Requirements:

Router functionalities like building Routing tables, forwarding tables, MAC Tablet, crypto algorithm/Key negotiations are considered under control plane traffic.
Dynamic routing protocols (RIP, OSPF and BGP) are the most widely deployed which comes under control plane, a malicious user may spoof or modify valid routing protocol messages and corrupt or change routing tables of a network. This might result in redirection of some or all network traffic, connectivity problems, excessive bandwidth consumption and potential denial of service of both the router and the routing protocol. Failure to secure the exchange of routing information allows an attacker to introduce false routing information into the network.

Control plane traffic shall be protected by using Routing protocol authentication mechanism, Passive interface (stop sending updates on interfaces that face end users i.e. on LAN), Route filtering, rate-limiting, prevention of unauthorized or excessive traffic etc.

3.1.2 Data Plane Traffic Protection

Requirements:

Data plane traffic is customer generated application traffic by hosts.

Security Threats like IP spoofing (Blind spoofing /No blind IP spoofing), IP Packet header with options like IP Source Routing, Low TTL value attacks shall be effectively addressed by the IP Router.

To secure Data plane traffic, IP Router should at least support protection mechanisms such as Unicast Reverse path forwarding (URPF), prevent IP spoofing with ACL's, preventing ICMP traffic with ACL's, ACL's to filter Packets with IP options, Disable with IP source routing options

3.1.3 NAPT (Network Address Port Translation) services support

Requirements:

If IP Router supports NAPT services, it shall have protection mechanism against possible attacks such as NAT Traversal attacks, Pin hole attacks and NAT Slipstreaming Etc.

3.1.4 Access Banners

Requirements:

IP Router shall provide the requirement of banner displayed prior to the establishment dialogue for a session. Before establishing a user session, IP Router shall display an advisory warning message regarding unauthorized use of IP Router

3.1.5 Inter –VLAN Routing support

Requirements:

IP Router shall not allow Inter –VLAN routing functionality by default. It shall be enabled only through permitted configuration by administrator.

3.1.6 Routing updates security

Requirements:

For Inter AS routing updates, facility shall exist in IP Router for administrative accept /reject routing updates to prevent Routing table poisoning attacks.

3.1.7 Avoidance of Routing Loops

Requirements:

IP Router shall implement routing loop prevention mechanisms such as split horizon, poison reverse, hold down timers etc.

Reference RF 1058, RFC 7868 RFC 4762

3.1.8 Avoidance of Layer 2 Loops

Requirements:

The IP Router shall support STP security mechanisms, including BPDU guard, root guard, and loop guard, to mitigate STP attacks such as rogue bridge insertion.

[Reference: IEEE 802.1D, IEEE 802.1Q & IEEE 802.1w]

3.1.9 Traffic Shaping and Rate Limiting

Requirement:

The IP Router shall provide traffic shaping and rate-limiting capabilities to manage bandwidth allocation on a per-port, per-VLAN, per VRF, or per-traffic-class basis.

- Customizable rate-limiting policies shall prevent individual devices or applications from consuming excessive traffic.
- Administrators shall have the ability to configure traffic shaping rules that prioritize critical traffic over less important network activity.

[Reference: https://www.rfc-editor.org/info/rfc2698 & rfc8325]

3.1.10 Multicast Listener Discovery (MLD) Security

Requirement:

The IP Router shall include MLD snooping for IPv6 multicast traffic and IGMP snooping for IPV4 allowing only valid hosts to join multicast groups. It shall also support MLD filtering to block unauthorized or excessive multicast traffic from congesting the network.

Reference: https://www.rfc-editor.org/info/rfc4541 & section 2.1.2

3.1.11 Protection against ARP Cache Poisoning Attacks

Requirement:

IP Router shall support mechanisms such as Dynamic ARP inspection, TARP, monitoring tools for ARP traffic and detect anomalies like rapidly changing IP-MAC address associations, indicating potential ARP poisoning attempts, packet filtering etc.

3.1.12 DHCP Snooping Security with Detailed Event Logging

Requirement:

The IP Router shall log all DHCP snooping events, including valid and invalid DHCP responses, unauthorized DHCP servers, and suspicious activities like DHCP starvation attempts. Logs shall capture the MAC address, IP address, and interface associated with each DHCP event.

[Ref:https://www.rfc-editor.org/info/rfc7513]

3.1.13 SNMP Trap/Info and Syslog for Security Violations

Requirement:

The IP Router shall support SNMP traps/info and syslog for real-time notifications of security violations, including unauthorized access and configuration changes. SNMP messages must be sent over SNMPv3 with encryption, and Syslog messages must utilize a secure channel. Additionally, the IP Router shall allow for customized security alert thresholds to prioritize critical events

[Reference: https://www.rfc-editor.org/info/rfc5590]

3.1.14 Protection against Routing Table Poisoning Attacks

Requirement:

The IP Router shall support Routing Table Poisoning attack protection mechanisms such as authentication on routing protocols to verify the source of routing updates, route filtering to only accept routing updates from trusted sources, monitoring tools to detect suspicious routing updates and potential poisoning attempts etc.

3.1.15 Protection against BGP Hijacking

Requirement:

The IP Router shall support BGP Prefix origin validation to ensure that the origin AS of route is valid for the advertised routes. The IP Router shall maintain an Origin Validation database consisting of static and dynamic entries (VRP or Validated ROA Payload) for the purposes of determining the origin validation state of received BGP routes. The IP Router shall support the RPKI-RTR protocol over TCP/IPv4 or TCP/IPv6 to learn Dynamic VRP entries. The communication between the IP Router and the validator cache shall be protected as per the requirements specified in RFC 8210.

[Ref RFC 8210, RFC 6480]

3.1.16 Routing Protocol Security

Requirement:

The IP Router shall support authentication mechanisms for Exterior & interior protocols, using cryptographic authentication with SHA algorithms (using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.) for route advertisements and updates. Additionally, route filtering and policy-based routing must be supported to prevent unauthorized route advertisements or incorrect route propagation. IP Router shall also support route filtering and prevention of routing information sharing on UNI.

[Ref: https://www.rfc-editor.org/info/rfc7416]

3.1.17 MAC Table Overflow Protection and Port Security

Requirement:

The IP Router shall protect against MAC table overflow attacks by implementing MAC limiting and port security features, allowing a maximum number of MAC addresses to be

learned per port.

- Dynamic MAC filtering shall be enabled to mitigate MAC address spoofing attempts.
- MAC address filtering rules shall be configurable, allowing for both static and dynamically learned entries with specified limits.
- Upon detecting an unauthorized MAC address, the IP Router shall block access, disable the port, and generate alerts.
- The IP Router shall support MAC address filtering at the port level, permitting only trusted MAC addresses to access the network.

[Ref: IEEE 802.1X & https://www.rfc-editor.org/info/rfc6325]

Section 3.2: API Related

(Applicable if APIs are supported, including APIs towards MANO)

3.2.1 The client and authorization servers shall mutually authenticate

Requirement:
APIs shall only allow themselves to be accessed by authorized users. One solution for authorizing access is the use of OAuth2.0 with access token. The client shall authenticate the resource server and vice versa. Mutual authentication is done by the transport layer protection and is required.

[Ref: 1) ETSI GS NFV-SEC 022 V2.7.1 Section 4.3 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T23, BP-P1]

3.2.2Authentication of the Request Originator

Requirement:
Before accepting the token as valid, the resource server shall authenticate the originator of the request as the legitimate owner of the token. The token shall bound to the subject through the subject Identifier, which shall ensure that the token has been provided for this consumer.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.2.3 Requirements for client credentials

Requirement:

a) The client credentials shall be stored in a secure and tamper-resistant location or stored encrypted with the key protected in a tamper-resistant location.
b) The client credentials shall not be included in the source code and software packages.

c) The client credentials shall be installed in the client in a secure way, eliminating any possibility of gaining access to these credentials during installation.
d) The client credentials shall be possible for the authorization server to revoke the client credentials.

[Reference: 1) ETSI GS NFV-SEC 022 V2.7.1 Section 4.3 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T23]

3.2.4Access Token shall be signed

Requirement:
The access token shall be signed to detect manipulation of the token or production of fake tokens. Access tokens shall be secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS). It shall be possible to encrypt the content of the access token.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.2.5Format of Access Token

Requirement:
The access token shall be defined in a standard format (SAML or JWT).

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.2.6Access tokens shall have limited lifetimes

Requirement:
The access token shall include a claim for the expiration time (expiration).

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.2.7Access tokens shall be restricted to a particular number of operations

Requirement:
There shall be a restriction on the number of operations that an access token can perform in order to mitigate the replay attack by a malicious client.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.2.8Access token shall be bound to the intended resource server.

Requirement:
The access token shall include a claim for the device ID of the Service Producer (audience). By using token binding, a client can enforce the use of a specified external authentication mechanism with the token.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.2.9Tokens shall be bound to the client ID

Requirement:
The access token shall include a claim for the device ID of the Service Consumer (subject) which is the "Client ID."

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.2.10Token Revocation

Requirement:
Token Revocation shall be possible. Unbound tokens shall not be used under any circumstance. The authorization server shall provide a mechanism for token revocation. If not, the lifetime of the Access token shall be kept very short, or the access token shall be single use. If a scheme to bind access tokens to the underlying transport layer relies on non-standard extensions, and those extensions are not available, the system shall fail securely, preventing a bid-down attack.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

Section 3.3: SDN Related (Applicable for SDN supported routers)

3.3.1 Mutual authentication within SDN
Requirement:

There must be mutual authentication between the controller and the switching/routing entities in SDN.

[Ref: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.1.3.1.1]

3.3.2 Centralized Log Auditing
Requirement:

All the SDN elements shall submit security events (e.g. authentication, authorization and accounting, login attempts, administration functions and configurations etc) as defined in Log

table in Ch 2.5.2 to a centralized platform, which shall monitor and analyses in real time the messages for possible attempts at intrusion.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T17]
Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.3.3SDN controller and associated SDN communications

Requirement:

An SDN controller shall always communicate with its associated SDN resources using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: ETSI GS NFV-EVE 005 Section 6.1, REC#1]

3.3.4Prevent attacks via forwarding plane

Requirement:

There shall be mechanisms to prevent attacks mounted via the Forwarding Plane against SDN switches and controllers. OEMs shall submit the list of measures taken to prevent reconnaissance attacks, DoS and resource exhaustion attacks and vulnerability exploits.

[Reference: ETSI GS NFV-EVE 005 Section 6.2, REC#1]

3.3.5 Prevent attacks via control network

Requirement:

a) There shall be mechanisms to mitigate attacks from the control network. TLS 1.2 or higher shall be used to protect integrity.
b) There shall be High-Availability (HA) controller architecture.
c) The configuration of secure and authenticated administrator access to controllers shall be enabled.
d) Role-Based Access Control policies shall be implemented for controller administrators.

[Reference: ETSI GS NFV-EVE 005 Section 6.2, REC#2]

3.3.6Prevent attacks via SDN controller's Application Control Interface

Requirement:

a) There shall be mechanisms to mitigate attacks via the SDN Controller's Application Control Interface such as TLS 1.2 or higher shall be used to secure northbound communications and secure controller management.

b) The SDN systems shall be configured to validate flows in network device tables against controller policy.

[Reference: ETSI GS NFV-EVE 005 Section 6.2, REC#3]

3.3.7Prevent attacks via virtualized environment

Requirement:

There shall be mechanisms to mitigate attacks against controllers and switches via the Virtualized environment. OEMs shall submit the list of measures taken to prevent such attacks.

[Reference: ETSI GS NFV-EVE 005 Section 6.2, REC#4]

3.3.8Northbound Applications

Requirement:

a) Northbound applications, including the orchestrators, shall not be assigned admin level access to the controllers.
b) The identity of northbound applications shall be confirmed through certificates.

3.3.9SDN security management

Requirement:

a) The controls below shall be applied if message bus technology for communication between SDN elements is used.
   i) A strong mechanism to authenticate the integrity of messages must be deployed between the 'publisher' and 'producer' over the message bus.
   ii) No messages shall be accepted or processed by the message broker or 'consumer' systems from unknown, 'fake' or unauthenticated users.
   iii) The communications shall be secured using TLS 1.2 and above security or certificates where supported (e.g. Kafka).
   iv) The message bus shall be monitored for any unauthenticated messages or 'fake' or default usernames and a security alarm raised for investigation.
b) The security functionality shall be deployed that identifies potential attacks on any SDN elements. Any security functionality shall provide automated alarms and the ability to change the network or element configuration to mitigate the attack.
c) A high availability architecture shall be implemented for key SDN components (e.g. SDN Controllers) to ensure operational service is maintained. The design shall include primary and secondary IP links with, where possible, diverse routing to allow for single point of network failure.

d) Any changes to network, service and virtual environments shall be restricted to the orchestrator. The SDN Controller and the VNFM/CNFM and VIM/CISM shall have additional controls applied to them to restrict such access for normal operation. Restricting the SDN Controller and the VNFM/CNFM and VIM/CISM will prevent the application of rules and changes that may break policy and rules during deployment of service templates.

e) The orchestration layer and SDN must be architected so that SDN networks and NFV environments are not operationally dependent on the orchestration or MANO layer to maintain operating services under circumstances that may render the orchestration platform unavailable.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T22]

Section 3.4: MANO Related

(For Cloud Native Routers, Virtual Routers or any router implementation which may use orchestrator)

3.4.1Instantiation of MANO components

Requirement:

The MANO system shall allow instantiation of MANO components and managed entities, the NFVIs, only at explicit geographic locations. It may be enforced through attribute-based access control and attribute based or multi-factor authentication (where location is one of the behavioral factors).

3.4.2Message handling in MANO

Requirement:

The transmitter of a message shall provide means that will allow for the determination of any modification, deletion, insertion, or replay has occurred. The transmitting party shall enable a complete message and session integrity service.

[Ref– ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.3Data Transfer in MANO

Requirement:

Data transferred over any internal interface of MANO shall be protected using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only.

[Ref– ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.4Centralized log auditing

Requirement:

All the MANO elements shall submit security events (e.g. authentication, authorization and accounting, login attempts, administration functions and configurations) to a centralized platform, which shall monitor and analyze in real time the messages for possible attempts at intrusion.

[Ref: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T17]

3.4.5VIM connectivity to virtualization layer

Requirement:

The connectivity between the VIM and the virtualization layer shall support a secure access protocol (e.g. IPSec, TLS) to protect against the eavesdropping of password information. It is also required that the secure access shall support mutual authentication before allowing any O&M connectivity.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T24]

Section 3.5: VNF_CNF Related

(Applicable for Virtual, Cloud Native and Cloud Managed Routers)

3.5.1.VNF/CNF network security profile

Requirement:

a) Each VNF/CNF supporting VNFC functions shall have a predefined network security profile describing its requirements for vNICs, ports, port group, VLANs and the requirement for internal VXLAN connections.
b) The security profile shall also define the vNIC firewall rules related to protocols (port numbers) that need to be supported on each VLAN or VXLAN connection. There shall never be a requirement for all ports to be open, particularly on external standard-based interfaces (e.g. GTP).

3.5.2.VNF/CNF Host Spanning

Requirement:

a) All control plane data in transit between hosts shall be sent over an encrypted and authenticated channel using the protocols as prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR).".

b) User plane traffic between hosts should be protected.

c) The system shall prevent and detect unauthorized VNF/CNF host spanning.

[Ref\: 3GPP TR 33.848-0.11.0 Section 5.15]

3.5.3.Input validation

Requirement:

a) The VNF/CNF must implement the following input validation controls:
   i) Size (length) of all input shall be checked.
   ii) Large-size input that can cause the VNF/CNF to fail shall not be allowed. If the input is a file, the VNF /CNF API must enforce a size limit.
   iii) Input that contains content or characters inappropriate to the input expected by the design shall not be permitted. Inappropriate input, such as SQL expressions shall not be allowed.

[Ref: ONAP- VNF API security requirements, October 2022]

3.5.4.Key Management and security within cloned images

Requirement:

Cloned images shall not possess cryptographic key pairs utilized by their original image. Propagation of two or more images with the same key pairs immediately cancels out the notion of utilizing key pairs for the purpose of establishing identity.

[Ref: ETSI GS NFV-SEC 003 V1.1.1 Section 4.4.3.3.1]

3.5.5.Encrypted Data Processing

Requirement:

a) Sensitive data shall only be decrypted or handled in an unencrypted format in VNFs/CNFs on trusted and well-known hosts.

b) It shall be possible to further restrict VNFs/CNFs on a single host depending on whether they handle decrypted sensitive data.
c) These controls shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.
d) The system shall prevent and detect unauthorized data manipulation and leakage (e.g., modification of VNF/CNF images, instantiating parallel VM(s) on same physical CPU).

[Ref: 3GPP TR 33.848-0.11.0 Section 5.16]

3.5.6.GVNP Life Cycle Management Security

Requirement:

a) VNF shall authenticate VNFM when VNFM initiates a communication to VNF.
b) VNF shall be able to establish securely protected connection with the VNFM.
c) VNF shall check whether VNFM has been authorized when VNFM access VNF's API.
d) VNF shall log VNFM's management operations for auditing.

[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.1]

Note: This test case is optional when the VNF and VNFM belongs to the same VNF vendor. If the VNF and VNFM belongs to the same VNF vendor and the interface between VNF and VNFM is proprietary interface, the API level authorization is not needed

3.5.7.Instantiating VNF from trusted VNF image

Requirement:

A VNF shall be initiated from one or more trusted images in a VNF package. The VNF image(s) shall be signed by an authorized party. The authorized party is trusted by the operators.

[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.3]

3.5.8.Inter-VNF and intra-VNF Traffic Separation

Requirement:

The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated to prevent the security threats from the different networks affecting each other.

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.5.8.5.2]

3.5.9.Security functional requirements on virtualization resource management

Requirement:

a) To prevent a compromised VIM from changing the assigned virtualized resource, the VNF shall alert to the OAM. For example, when an instantiated VNF is running, a compromised VIM can delete a VM which is running VNFCI, and the VNF shall alert the OAM when the VNF cannot detect a VNFC message.
b) A VNF shall log the access from the VIM.

[Reference: 3GPP TS 33.818 v17.1.0 Section 5.2.5.6.7.2 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022)]

3.5.10.VNF package and VNF image integrity

Requirement:

1) VNF package and the image shall contain integrity validation value (e.g. MAC).
2) VNF package shall be integrity protected during onboarding and its integrity shall be validated by the NFVO.

[Reference: 3GPP TS 33.818- 17.1.0 Section 5.2.5.5.3.3.5.1 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T2]

3.5.11.Proper image management of VM images must be done

Requirement:

Images shall be carefully protected against unauthorized access, modification, and replacement by both systems and human actors.

a) Cryptographic checksum protection shall be used to detect unauthorized changes to images and snapshots.
b) Strict control around access, creation and deployment of images/instances shall be implemented. Such activities shall be recorded for audit purposes.

[Reference: ENISA Security Aspects of Virtualization (Feb 2017) G-07, PG 37, OS-01, OS-02]

3.5.12.Secrets in NF Container/VM Image

Requirement:

The VNF/CNF images shall not be packaged with embedded secrets such as passwords or credentials, or any other critical configuration data.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.28]

3.5.13.Container image authorization

Requirement:

Public cloud service provider shall give an undertaking that geo-fencing has been enabled so that container images can only run on particular platforms.
[Reference: CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0]

Section 3.6: Virtual Machine Related

(Applicable to Virtual Routers, Cloud Managed Router or any router implementation which involves VMs)

3.6.1Secure crash measures for VMs running on hypervisors

Requirement:

The following clauses must be satisfied:

a) Hypervisors shall ensure that in the event of the crash of a VNF component instance, all file references, hardware pass-through devices, and memory are safe from access by unauthorized entities.

b) If the application running within the VM crashes, but not the VM itself, the hypervisor shall ensure that no changes to the existing authorizations are made.

NOTE: The hypervisor might be unaware that the application within the VM has crashed.

c) In the event of a crash, arrangements shall be made for the relevant NFV instance to wipe the remote storage (e.g. the VNF Manager might instruct the Virtualization Infrastructure Manager to request this).

d) If the VNF component instance is using swap storage, it shall be marked as such and the hypervisor ought to wipe it in the event of a crash.

[Reference: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.4]

3.6.2Memory Introspection

Requirement:

a) An NFV environment shall use a virtualization platform which prevents one function from inspecting memory of other functions.

b) Delegated administrator roles shall be used to ensure that administrators do not have the ability to inspect memory of functions except under exceptional circumstances such as for network forensics.

c) The system shall manage the hypervisor to enforce network security policies. This includes, but is not limited to, ensuring that: -

i. VMs are isolated from each other
ii. Applications shall be prevented from accessing each other's memory spaces,
iii. VMs shall be prevented from accessing the memory of another VM,
iv. Keys used to encrypt the memory shall be kept under hypervisor control,
v. Hypervisors shall not be allowed to write directly to memory,
vi. Hypervisors shall not be allowed to bypass normal memory access controls and security within the VNF/VM,
vii. Hypervisors shall not be allowed to change data within a 3GPP VNF at run-time.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.8]

Section 3.7: Container Related

(Applicable to Cloud Native Routers or any router implementation which involves containers)

3.7.1Container breakout

Requirement:

a) The virtualization layer shall provide capabilities to limit the impact on co-hosted containers caused by a rogue container escaping its isolation. One of the commonly practiced security controls is to enforce strict resource limits on container usage, which helps in preventing resource starvation due to an attack by a rogue container.

b) The virtualization layer shall enforce the principle of 'least privilege' which ensures that no containers run with a privilege higher than what is actually required.

[Reference: 1) 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.27 2) ENISA NFV Security in 5G -

3.7.2Container Platform Integrity

Requirement:

The following shall be implemented to ensure the integrity of the container platform

a) The Kubernetes cluster shall be hardened against known attacks through suitable configurations. The Container Platform's Kubernetes cluster shall be hardened by following security guidelines and by running appropriate tools.
b) Opening up direct access to worker nodes shall not be resorted.
c) Worker node subnets shall be on private subnets (no access to the Internet) unless explicitly required (e.g., web server).
d) Container platform information and verified firmware and configuration measurements that are retained within an attestation service shall be used for policy enforcement. It shall also be possible to label worker nodes in the database with key value attributes

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

3.7.3Container Image Hygiene

Requirement:

The following best practices shall be implemented

(a) Multi-stage builds shall be used to create minimal images. Container images shall be devoid of build tools and other extraneous binaries.
(b) Container images shall be regularly scanned for any vulnerabilities
(c) Container shall not run as root.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

3.7.4Securely Isolate Network Resources (Pod Security)

Requirement:

a) Pods with containers configured to run as privileged shall be rejected using the technical controls and policies provided by the container orchestration platform.
b) Container shall not allow processes to run as root
c) Container orchestration platforms shall provide technical controls and policies to prevent privilege escalation.

d) Container orchestration platforms shall provide technical controls and policies to restrict directories used by host Path and ensure that those directories are read only.
e) Critical Containers shall be cryptographically isolated using TEEs

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.
[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part II: Securely Isolate Network Resources, 2021]

3.7.5Runtime security

Requirement:

Permitted syscalls shall be restricted to an allow-list to decrease the application's attack surface.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part II: Securely Isolate Network Resources,2021]

3.7.6Real-time threat detection and incident response

Requirement:

a) Attestation services shall be used to verify configuration policy and container metrics (e.g., hash of files, time to execute a module) at both boot and run times.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part II: Securely Isolate Network Resources,2021]

Section 3.8: NFV Infrastructure (Platform) Related

*(Applicability of clauses are based on the router implementation**)***

3.8.1 CPU Pinning

Requirement:

When a VM instance is created, the vCPUs are, by default, not assigned to a particular host CPU. Certain workloads require real-time or near real-time behavior viz., uninterrupted access to their cores. For such workloads, CPU pinning shall be possible to bind an instance's vCPUs to a particular host' cores or SMT threads.

Note: It is possible for OEM to demonstrate this clause with an example of CPU pinning.

[Reference: GSMA NG.133 - Cloud Infrastructure Reference Architecture]

3.8.2 Workload Placement

Requirement:

Affinity Rule: It specifies workloads that shall be hosted on the same computer node.
Non-Affinity Rule: It specifies workloads that shall not be hosted on the same computer node.
It shall be possible to segregate workloads based on server groups (affinity and non-affinity groups)
Note: It should be possible for OEM to demonstrate this clause with examples

[Reference: GSMA NG.133 - Cloud Infrastructure Reference Architecture]

3.8.3 SR-IOV and DPDK Considerations

Requirement:

Acceleration techniques like DPDK, SR-IOV usually bypasses security protections. Measures shall be taken to ensure security when these technologies are employed to accelerate network packet processing.

Note: OEM shall give the list of measures which shall be verified

3.8.4 Hardware-Based Root of Trust (HBRT)

Requirement:

a) The host system shall include an HBRT or Trusted Platform Module (TPM) as Initial Root of Trust. The HBRT shall be based on hardware-based TPM or equivalent hardware root of trust (e.g., Secure Element including TPM functionalities, HSM including TPM functionalities).

b) The host system HBRT shall be able to provide isolated instances of the HBRT capabilities for individual workloads.

c) The host system HBRT shall include a hardware-based compute engine to be used by the workloads for cryptographic and security functionality.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 8.10]

3.8.5 Core Hardware -HBRT

Requirement:

(a) The HBRT shall be both physically and electronically tamper-resistant.
(b) The HBRT shall be both physically and electronically tamper-evident.
(c) The HBRT physical and software interfaces between the HBRT and other hardware components of the host system to which it directly communicates shall be protected from eavesdropping, manipulation, replay or similar attacks.
(d) It shall be possible to restrict the booting procedure if assistance from the HBRT is not available or the HBRT currently does not contain valid cryptographic material.
(e) Any tampering to the HBRT shall lead to detectable degradation of its function.
(f) The HBRT shall be (physically and/or logically) bound to the host system, so that any attempt to remove the HBRT will be detected and prevent normal operation of the host system.
(g) The HBRT shall include an Immutable Unique Identification value physically linked to the physical root of trust that can be used as identification of the platform. This value shall be stored in a shielded location protected from unauthorized use and disclosure.
(h) The HBRT shall provide capabilities to allow itself to be part of an attestation function.

Note: OEM shall submit an undertaking along with Explanatory Note

[Reference: ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 5.1]

3.8.6 Trusted computing technologies

Requirement:

Silicon-based security functionality (for example Intel TXT, SGX, AMD SEV or ARM Trust zone) shall be implemented with a TPM that stores measurements of the entire hypervisor or CIS stack and boot process to provide a trusted hardware platform.

3.8.7 Direct access to memory

Requirement:

The host system shall be able to deny direct access to memory to particular hardware resources.

[Ref: ETSI GS NFV-SEC 012 V3.1.1 section 8.12]

3.8.8 Monitoring of resource usage at both VNF infrastructure (VNFI) and level of guest VNFs

Requirement:

Monitoring shall be put in place at both the infrastructure level and the level of guest VNFs. These two layers will require interfaces with the management & orchestration system to consume monitoring information, then act on it accordingly.

[Ref: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.5.5]

3.8.9 Time Synchronization

Requirement:

Given that token expiration is a component of Identity and Access Management, time synchronization among the servers is critical and hence shall be implemented.

Note: This clause requires IAM for testing. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.
[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.10]

3.8.10 Lifetime of entities

Requirement:

It is important that the lifetime of Management and Orchestration entities shall be long, relative to the lifetime of entities which they control, such as VNFs, and VNFCIs.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 Section 5.3.2]

3.8.11 Provisioning/Deployment

Requirement:

(a) Regarding the provisioning of servers, switches, routers and networking, tools must be used to automate the provisioning eliminating human error.
(b) The deployment tool is a sensitive component storing critical information (deployment scripts, credentials, etc.).

The following rules must be applied:

i) The boot of the server or the VM hosting the deployment tool must be protected
ii) The integrity of the deployment images must be checked, before starting deployment
iii) The deployment must be done through dedicated network (e.g., VLAN)
iv) When the deployment is finished, the deployment tool must be turned-off, if the tool is only dedicated to deployment. Otherwise, any access to the deployment tool must be restricted.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture v1.0 Section: 6.3.6.1]

3.8.12 Confidentiality and Integrity of communications

Requirement:

a) It is essential to secure the infrastructure from external attacks. To counter this threat, API endpoints exposed to external networks shall be protected by either a rate-limiting proxy or web application firewall (WAF), and shall be placed behind a reverse HTTPS proxy.
b) It shall be ensured that integrity and confidentiality of all network communications (internal and external) by using Transport Layer Security (TLS) protocol Ver 1.2 or above.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture v 1.0]

3.8.13 Securing 3rd Party Hosting Environments

Requirement:

a) Sensitive information of virtualized NFs shall be confidentiality protected when using a 3rd party environment (e.g., NFVI).
b) The system shall be able to monitor the attestation of 3rd party hosting environments.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

[Reference: 1)3GPP 33.848-17.1.0 V.0.11.0 Section 5.21 2) ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.9 3) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T29]

3.8.14 Isolation of VM's/Containers (VM and Hypervisor Breakout)

Requirement:

a) The NFVI shall provide security isolation to minimize the impact of and detect hypervisor/VM breakout on a virtualized 3GPP NF.
b) The system shall prevent and detect attacks that breakout from an attacked VNF through the virtualization layer to any other VNF or any other location.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.22]

3.8.15 Backend access Security

Requirement:

The integrity of resources management requests coming from a higher orchestration layer to the Cloud Infrastructure manage shall be validated and verified.

[Reference: GSMA NG 126 Ver 3.0 Section 7.4.2]

Section 3.9: Virtualization Security

(Applicable for any router which includes Hypervisor/CIS with VM/Container as part of its implementation. Applicable for both Hypervisor based VM with its VNF and CIS based Container with its CNF)

3.9.1 Isolation of VM's (VM and Hypervisor Breakout)

Requirement:

a) The NFVI shall provide security isolation to minimize the impact of and detect hypervisor/VM breakout on a virtualized IP Router NF.
b) The system shall prevent and detect attacks that breakout from an attacked VNF through the virtualization layer to any other VNF or any other location.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.22]

3.9.2 Data synchronicity through network

Requirement:

a) The virtualized IP Router NFs shall be protected from distributed monitoring attacks. The system shall dynamically assign VNF resources (e.g. memory address) to prevent long-term data leakage and exposure and protect network resources.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.25]

3.9.3 Availability

Requirement:

It shall be possible to replicate virtual machine/ containers into various zones and clusters to achieve high availability.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 9]

3.9.4 Token Generation

Requirement:

The parameters relevant to the token, i.e., lifespan and key length shall be configurable during the token generation.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.2.2]

3.9.5 Policies for workload placement in Retained data

Requirement:

Retained Data collection, storage and query shall only take place within the country. An undertaking in this regard shall be submitted.

[Reference: ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.5]

3.9.6 Validating the Topology of Virtualized Network Functions

Requirement:

a) The topology of the Virtualized Network functions needs to be validated to ensure that the connectivity of the whole network, including all its virtualized functions meets its security policy.

b) It also needs to be verified that any unauthorized connectivity shall not be present and that it cannot be added by any unauthorized party.

[Reference– ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.1.2]

3.9.7 Network Address Translation

Requirement:

Support for the private IP address to communicate with a host on the public network shall be provided.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.3]

Section 3.10: Wi-Fi Access Related

3.10.1 SSID Scanning

Requirement:

The WiFi capable Network product shall not disclose sensitive information, PIN details on

SSID scan / attack techniques. It must provide disguised feedback to users on unsuccessful attempts without revealing of reason for failures. Option to hide / unhide SSID on user selection is an essential feature.

3.10.2 Unused Physical and logical Interfaces Disabling

Requirement:

The WiFi capable Network product shall support the mechanism to verify all the physically accessible interfaces. Physically accessible Interfaces (including LAN ports) and logical interfaces which are not under use shall be disabled by configuration so that they remain inactive even in the event of a reboot.

3.10.3 Authentication Support - External

Requirement:

If WiFi capable Network product supports external authentication (for the Cyber- Cafe use-case scenario or for WiFi end users), the user authentication credentials shall be protected and securely communicated if the authentication credentials are managed by external authentication servers.

3.10.4 Remote Management Standards for Connected Devices, Additional Features

Requirement:

The remote management mechanisms for devices connected to WiFi capable Network product, or for configuration of additional features like DDNS, UPnP etc., must be compliant with the respective latest standards published at the time of commencement of security testing. These additional features shall be configured as disabled in the factory default settings, with provision for user to enable individual features on menu-selection. Such mechanisms to include entity mutual authentication, encryption of the management traffic.

3.10.5 Restricted reachability of services

Requirement:

The WiFi capable Network product shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. OEM to map the essential services required to be accessed from WAN side, LAN side to limit access to services only on need / functionality basis. For Interfaces on which services are active, the reachability to be limited to legitimate communication peers. One such Use-case scenario is to restrict web-management access of WiFi capable Network product to only LAN ports and not to permit access on Wi-Fi, WAN side.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.2]

3.10.6 Cryptographic Algorithm selection for Wi-Fi Access

Requirement:

WiFi capable Network product shall support WPA2-PSK with AES-128 as default standard. Other internationally accepted encryption standards stronger like AES-192 etc., may also be made available with user choice selection. Weaker encryption options like WEP, WPS, TKIP etc., are not to be available for selection / configuration.

Additionally, WPA2 version must support PMF (Protected Management Frames). WPA2 must have built in KRACK (Key Reinstallation Attack) Mitigation. Also, all the ciphers used must be in compliance with Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)". All types of WiFi capable Network products shall also support WPA3 and WPA shall not be supported.

3.10.7 Cryptographic Based Secure Communication on Wi-Fi Access

Requirement:

The communication security dimension on Wi-Fi access ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). The security mechanism to protect against well-known attacks like capture-decrypting, PIN detection, Key recovery, Key reinstallation attacks.

WiFi capable Network product shall support WPA2-PSK with AES as default standard. Other encryption options stronger than WPA2 shall be made available under configuration menu for user choice selection.

Annexure-I

Definitions

1. **Anti-Spoofing:** Anti Spoofing is a technique for identifying and dropping packets that have a false source address.
2. **API:** An API is a set of definitions and protocols for building and integrating application software. In the context of Wi-Fi CPE, APIs can be used to manage and configure the Wi-Fi CPE device remotely, integrate the Wi-Fi CPE with other network devices and services and collect and analyze data from the Wi-Fi CPE.
3. Bridge Protocol Data Unit (BPDU) is a message unit used in the Spanning Tree Protocol (STP) to share information between switches.
4. **CNF:** A CNF is a network function that is designed to be deployed in a cloud-native environment. CNFs are typically containerized and can be deployed on any cloud platform.
5. **Confidential system internal data:** that contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).
6. **Confidentiality:** The state of keeping or being kept secret or private.
7. **Firewall:** A firewall is a network security device that monitors traffic to or from the network.
8. **Hold Down Timer** in a router is a mechanism used in routing protocols to prevent rapid and unnecessary routing table updates by delaying the advertisement of a route when a link failure is detected, essentially pausing the router from accepting changes to a route for a specific period until the network appears stable again.
9. **Host path:** In Kubernetes, a host Path volume means mounting a file or a directory from the node's host inside the pod. A Kubernetes host path is one of the volumes supported by Kubernetes.
10. **Host system:** collection of hardware, software and firmware making up the system which executes workloads
11. **Hypervisor:** A software which acts as a bridge in between the Virtual Machines and the Host machine. It converts all the operations from the Virtual Machines so that they will be executable on the Host Machine CPU.
12. **KRACK:** KRACK is short for Key Reinstallation Attack. It is an attack that leverages a vulnerability in the Wi-Fi Protected Access 2 (WPA2) protocol, which keeps your Wi-Fi connection secure.
13. **NAT Slipstreaming** is an attack technique that allows attackers to bypass a network's firewall and Network Address Translation (NAT) mechanisms. By exploiting the NAT process, attackers can remotely access TCP/UDP services bound to a victim's machine. This is achieved by tricking the NAT into opening an inbound connection. It tricks the ALG processes to inadvertently create an inbound connection path from the internet to the internal network.

14. **Network Service:** composition of Network Function(s) and/or Network Service(s), defined by its functional and behavioral specification.
15. **Platform:** A computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run.
16. **Pods:** Pods are the isolated environments used to execute 5G network functions in a 5G container centric or hybrid container/virtual network function design and deployment.
17. **Poison Reverse** is a routing protocol technique that prevents loops in computer networks that use distance vector routing protocols.
18. **SDN:** SDN is a network architecture that separates the control plane from the data plane. This allows for more flexible and programmable networks. In the context of Wi-Fi CPE, SDN can be used to centralize the management of multiple Wi-Fi CPE devices, automate the provisioning and configuration of Wi-Fi CPE devices, optimize the performance of the Wi-Fi network.
19. **Sensitive Data:** data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.
20. **Split horizon** is a network protocol technique that prevents routing loops by stopping a router from advertising a route back to the interface it was learned from.
21. **TEE:** A Trusted Execution Environment (TEE) is an area in memory protected by the processor in a computing device. Hardware ensures confidentiality and integrity of code and data inside a TEE. The code that runs in the TEE is authorized, attested, and verified.
22. **VM Image:** A Virtual Machine Image is a fully configured Virtual Machine used to create a VM for deployment.
23. **VNF Image:** It is a fully configured Network Function which is used to deploy the network function in a virtualized environment.
24. **VNF Package:** VNF Package is a ZIP file including VNFD, software images for VM, and other artifact resources such as scripts and config files
25. **Worker nodes:** Worker nodes within the Kubernetes cluster are used to run containerized applications and handle networking to ensure that traffic between applications across the cluster and from outside of the cluster can be properly facilitated.
26. **Workload:** component of the NFV architecture that is virtualized in the context of a particular deployment
27. **WPA2:** WPA2 is a security protocol that is used to encrypt wireless communication. WPA2 is more secure than WEP and WPA.
28. **WPA3:** WPA3 is the latest version of the Wi-Fi Protected Access security protocol. WPA3 is more secure than WPA2.

Annexure-II
Acronyms

3GPP	3rd Generation Partnership Project
AAA Server	Authentication, Authorization, and Accounting Server
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
AS	Autonomous System
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
CERT	Computer emergency response teams
CIS	Container Infrastructure Service
CISM	Container Infrastructure Service Management
CNF	Cloud-Native Function
CWE	Common Weakness Enumeration
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DPDK	Data Plane Development Kit
eBPF XPD	extended Berkley Packet Filter eXpress Data Path
EIGRP	Enhanced Interior Gateway Routing Protocol
EMS	Element management System
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
FR	Frame Relay
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
JSON	JavaScript Object Notation
JWT	JSON Web Token
LD	Listener Discovery
MAC	Media Access Control
MAEC	Multi Access Edge Cloud
NAPT	Network Address and Port Translation
NAT	Network Address Translation
ND	Neighbor Discovery
NE	Network Element
NFV	Network Functions Virtualization

NFVI	Network Functions Virtualization Infrastructure
NIC	Network Interface Controller/Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
O&M	Operation & Maintenance
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAT	Port Address Translation
PTP	Precision Time protocol
RIP	Routing Information Protocol
ROA	Route Origin Authorizations
RPKI	Resource Public Key Infrastructure
RTR	RPKI to Router Protocol
SAML	Security Assertion Markup Language
SDN	Software-Defined Networking
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SR-IOV	Single Root I/O Virtualization
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Security Target
STP	Spanning Tree Protocol
TARP	Ticket-based Address Resolution Protocol
TFTP	Trivial File Transfer Protocol
UNI	User Network Interface
URPF	Unicast Reverse Path Forwarding
VIM	Virtualized Infrastructure Manager
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function
VRF	Virtual Routing and Forwarding
VRP	Virtual Routing Protocol
WPA	Wi-Fi Protected Access

Annexure III

List of Submissions

List of undertakings to be furnished by the OEM for IP Routers Security testing submissions.

1. Source code security assurances (against test case 2.3.3)
2. Know malware and backdoor check (against test case 2.3.4)
3. No unused software (against test case 2.3.5)
4. No unsupported components (against test case 2.4.2)
5. Avoidance of Unspecified mode of Access (against test case 2.4.3)
6. Cryptographic Module Security Assurance 2.6.2)
7. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)
8. Container image authorization (against test case 3.5.13)
9. Core Hardware -HBRT (against test case 3.8.5)
10. Policies for workload placement in Retained data (against test case 3.9.5)

Annexure IV
References

1) 3GPP TR 33.848-0.11.0
2) 3GPP TS 33.818-17.1.0.
3) CIS_Benchmarks_Password_Policy_Guide_v21.12
4) CIS Password Policy Guide
5) ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019
6) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T29
7) ENISA Security Aspects of Virtualization (Feb 2017) G-07, PG 37, OS-01, OS-02
8) TEC 25848:2022: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0
9) ONAP- VNF API security requirements, October 2022
10) RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
11) RFC 8210, RFC 6480, RF 1058, RFC 7868, RFC 4762
12) IEEE802.1D, IEEE802.1Q & IEEE802.1w
13) https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
14) https://owasp.org/www-project-top-ten/
15) https://owasp.org/www-project-api-security/
16) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2
17) https://nvd.nist.gov/vuln-metrics/cvss
18) https://www.rfc-editor.org/info/rfc2698 & rfc8325
19) https://www.rfc-editor.org/info/rfc4541
20) https://www.rfc-editor.org/info/rfc7513
21) https://www.rfc-editor.org/info/rfc5590
22) https://www.rfc-editor.org/info/rfc7416
23) IEEE 802.1X & https://www.rfc-editor.org/info/rfc6325
24) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022)
25) ETSI GS NFV-EVE 005
26) ETSI GS NFV-SEC 022 V2.7.1
27) ETSI GS NFV SEC 001 V1.1.1 (2014-10)
28) ETSI GS NFV-SEC 014 V3.1.1
29) ETSI GS NFV-SEC 012 V3.1.1 (2017-01)
30) ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.9
31) ETSI GS NFV-SEC 002 V1.1.1
32) ETSI GS NFV-SEC 003 V1.1.1
33) NSA-CISA Security Guidance for 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (2021)
34) GSMA NG.133 Cloud Infrastructure Reference Architecture v1.0
35) GSMA NG 126 Ver 3.0
36) GSMA NG 133: GSM Association Non-confidential Official Document NG.133