Indian Telecom Security Assurance Requirements (ITSAR)

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

Group-IV Devices
Common Security Requirements ITSAR

ITSAR Number: ITSAR702042604
ITSAR Name: NCCS/ITSAR/Standards Applicable for Group of Equipment/CSR Group of Devices/Group-IV Devices-V2.0.0

Date of Release: 24.04.2026 Version: 2.0.0
Date of Enforcement:

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. Security Assurance Standards (SAS) division of 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.	Group-IV Devices Common Security Requirements	ITSAR702042504	1.0.0	21.04.2025	First release
2.	Group-IV Devices Common Security Requirements	ITSAR702042604	2.0.0	24.04.2026	Second release

Contents

A) Outline

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies Common Security Requirements for Group-IV devices as mentioned in **office memorandum regarding "Expanding the scope of CSR Testing"** Ltr No. NCCS/SAS/6-1/2024-25/ dated at Bengaluru, 2nd January, 2025.

As per the Office Memorandum (OM) referred above, **Group IV** initially contained ITSARs for the following four devices:

- Wi-Fi CPE V1.0.1
- IP Router V1.0.1
- Cell Broadcast Centre (CBC) V1.0.0
- Private Automatic Branch Exchange (PABX) V1.0.1

Subsequent to the issuance of the OM, the **IP Router** and **Wi-Fi CPE** ITSARs were revised to address technological advancements, resulting in the publication of **IP Router V2.0.0** and **Wi-Fi CPE V2.0.0**

In addition, the **L2 and/or L3 LAN Switch ITSAR** and **Network Next Generation (NG) Firewall including IDS & IPS ITSAR** were published by NCCS in the year 2025. As these equipment categories also fall under Group IV, the scope of CSR testing has been expanded accordingly.

To facilitate ease of designation of TSTLs for the revised IP Router & Wi-Fi CPE, L2/L3 LAN Switch, and Network NG Firewall including IDS & IPS, the **Group IV CSR ITSAR has been revised to Version 2.0.0**, incorporating CSR requirements of the newly published

elements.

Group IV now includes the following equipment categories:

1. Wi-Fi CPE (Customer Premises Equipment) Revised Version: V2.0.0 & Version 1.0.1.
2. IP Router Revised Version: V2.0.0 & Version 1.0.1
3. Cell Broadcast Centre (CBC) V1.0.0.
4. Private Automatic Branch Exchange (PABX) Version: V1.0.1
5. L2 and/or L3 LAN Switch V1.0.0
6. Network Next Generation (NG) Firewall including IDS & IPS V1.0.0

A **Wi-Fi CPE (Customer Premises Equipment)** device is a networking device used to connect end users to an internet service provider (ISP) via Wi-Fi. These devices are commonly used in home and business networks and can take different forms depending on the type of internet connection.

An **IP router** is a networking device that directs data packets between computer networks, ensuring efficient communication between devices. It operates at the network layer (Layer 3) of the OSI model and determines the best path for data to travel across interconnected networks.

A **Cell Broadcast Center (CBC)** is a telecommunications system responsible for sending cell broadcast messages to mobile users within a specific geographic area. It is widely used for emergency alerts, weather warnings, disaster notifications, and government announcements.

A **PABX (Private Automatic Branch Exchange)** is a private telephone system used within an organization to manage internal and external calls. It enables businesses to connect multiple phone lines and extensions without requiring a separate phone line for each user.

A **L2 and (or) L3 LAN Switch** is a networking device that connects computers and other equipment within a local area network. An **L2 switch** forwards traffic based on MAC addresses at the data link layer, while an **L3 switch** adds routing intelligence, using IP addresses to move traffic between different subnets.

A **Network Next Generation Firewall including IDS & IPS** is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to create a barrier between a trusted internal network and untrusted external networks, such as the internet. Traditional firewalls operate by filtering traffic based on IP addresses, port numbers, and protocols. They can block unauthorized access while permitting legitimate communication.

This document begins with an overview of Grouping, including its scope and objectives, and then proceeds to outline the Common Security Requirements of the ITSARs applicable to Group IV devices.

B) Scope

This document defines Common Security Requirements for Indian Telecom Security Assurance Requirements (ITSARs) of Group IV devices (Wi-Fi CPE V1.0.1& V2.0.0, IP Router V1.0.1 & V2.0.0, Cell Broadcast Centre V1.0.0 and Private Automatic Branch Exchange V1.0.1, L2 and (or) L3 LAN Switch V1.0.0 and Network Next Generation Firewall including IDS & IPS V1.0.0).

It serves as the basis for designating labs as TSTLs for testing the Common Security Requirements of these devices and security certification of these devices till TSTL capable of testing SSR is available.

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.

D) Applicability of the clauses

If a requirement explicitly specifies the applicability to a particular device, it applies and is tested only on that device; otherwise, it applies to and is tested on any one or all Group IV devices

1.1 Introduction:

The ITSARs are consisting of Common Security Requirements (CSR) and Specific Security Requirements (SSR). The CSR clauses are common across most of the ITSARs. SSR clauses are specific to the Communication device. However, the testing infrastructure requirement, skill set requirement may vary from device to device or from group of devices to group of devices.

In an endeavour to mandate testing CSR clauses of a group of devices and designate the TSTL for testing CSR clauses of a group of devices **"Grouping of devices"** is done.

Chapter 2 of this ITSAR outlines the Common Security Requirements applicable for designating the labs for CSR testing of Group IV device ITSARs.

Section 2.1: Access and Authorization

2.1.1 Management Protocols Entity Mutual Authentication

('Authentication for Product Management and Maintenance interfaces' is the clause name in IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Wi-Fi CPE (V2.0.0))

('Management Protocols Mutual Authentication' is the clause name in IP Router (V1.0.1), CBC, Network Next Generation Firewall including IDS & IPS, Wi-Fi CPE (V1.0.1), PABX)

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE shall communicate with authenticated management entities only. The protocols used for the CPE management shall support mutual authentication mechanisms, preferably with pre- shared key arrangements or by equivalent entity mutual authentication mechanisms. This shall be verified for all protocols used for CPE management. (This feature shall be supported on all WAN management interfaces).

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

The protocols used for the device's management shall support mutual authentication mechanisms. There is mutual authentication of entities for management interfaces on the device. HTTPS with TLS 1.2, SNMP V3 Protocols are allowed.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.4.4.1]

Requirement:
(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)

The protocols used for the device management and maintenance shall support mutual authentication mechanisms only. Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for device management and maintenance.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.4.4.1]

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch, and Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

Group IV device 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: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.4.1]
[Ref: TSDSI STD T1.3GPP 33.117-17.5.0 V1.5.0 Section 4.2.3.4.4.1]
[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.0.1.1.0. Section 4.2.3.4.4.1]

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

The Wi-Fi CPE shall communicate with authenticated management entities only. The protocols used for the Wi-Fi CPE management shall support mutual authentication mechanisms, preferably with pre-shared key arrangements or by equivalent entity mutual authentication mechanisms. This shall be verified for all protocols used for Wi-Fi CPE management. 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 system management and maintenance.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.4.1]
Management Traffic Protection

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Usage of cryptographically protected network protocols is required. The transmission of data with a need of protection shall use industry standard network protocols with sufficient security measures and industry accepted algorithms. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used. Verify the mechanisms implemented to protect data and information in transfer to and from the Device's OAM interface.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.4]

Requirement:
(applicable to CBC, PABX, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS *only; to be tested on any one of CBC, PABX, IP Router (V2.0.0), or* L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS Switch *of Group IV)*

Group IV device management traffic (information exchanged during interactions with OAM) shall be protected strictly using secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" only.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.2.4]

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.4]

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

All management traffic shall be protected by integrity and encryption. Unprotected sessions shall not be accepted. The remote access methods can support traffic encryption using protocols such as HTTPS, SSHV2.0.0 or can be based on lower tunneling protocols (IPsec VPN, TLS VPN, etc.).

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

All management traffic shall be protected by integrity and encryption. Unprotected sessions shall not be accepted. The remote access methods shall support traffic encryption using protocols such as HTTPS, SSHv2 or shall be based on lower tunnelling protocols (IPsec VPN, TLS VPN, etc.).

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 system management.

[Ref: TEC 64498:2024/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

('Role-based access control policy- Local/Remote' is the clause name for Network Next Generation Firewall including IDS & IPS)

('Role-Based access control policy' is the clause name for IP Router (V2.0.0), and L2 and (or) L3 LAN Switch)

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

CPE shall support Role-Based Access Control (RBAC) which provides at least two different access levels or domains to guarantee that individuals can only perform the operations that they are authorized for. The RBAC system controls how users are allowed access to the various domains and what type of operations.

In case of Wi-Fi CPE split into two or more devices like AP, Controller etc., the network product 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 provision should also be extended for Wi-Fi end users (for user-based access restriction) and API users (for different privilege levels), as applicable.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.6.2]

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

CPE shall support Role-Based Access Control (RBAC) which provides at least two different access levels or domains to guarantee that individuals can only perform the operations that they are authorized for. The RBAC system controls how users are allowed access to the various domains and what type of operation

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

CBC shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which determines how users interact with domains and resources. The RBAC system controls 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. CBC supports Role Based Access Control (RBAC) with minimum of 3 user roles, in particular, for OAM privilege management for CBC Management and Maintenance, including authorization of the operation for configuration data and software.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.2]

Requirement:
(applicable to PABX, IP Router (V1.0.1), and Network Next Generation Firewall including IDS & IPS of Group IV; to be tested on any one of PABX, IP Router (V1.0.1), or Network Next Generation Firewall including IDS & IPS of Group IV)

The network product shall support Role Based Access Control (RBAC). A role-based access control system uses 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 controls 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 network product supports 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.2]

[Ref: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.4.6.2]

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

The Group IV device 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 Group IV device 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]

[Ref: TSDSI STD T1.3GPP 33.117-17.5.0V1.5.0 Section 4.2.3.4.6.2]

2.1.4 User Authentication - Local/Remote

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

Local/Remote access to the CPE for configuration and maintenance purposes shall be granted only to authenticated users or machines using at least one authentication attribute. This authentication attribute when combined with the user's name shall enable unambiguous authentication and identification of the authorized user. No methods to exist providing authentication-bypass attacks to succeed under all combinations of interface / methods of authentication.

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the username, enables 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) is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

NOTE: Several of the above options can be combined (dual-factor authentication) to achieve a higher level of security. Whether or not this is suitable and necessary depends on the protection needs of the individual system and its data and is evaluated for individual cases.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.1]

Requirement:
(applicable to CBC, IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), *L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, IP Router (V2.0.0),* Wi-Fi CPE (V2.0.0), *L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS of Group IV)*

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.1]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the username, enables 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 is not 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 the all accounts from misuse.

Local access: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from PABX local hardware interface.

Remote access: The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.2.1]

2.1.5 Remote Management Standards

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) only; to be tested only on Wi-Fi CPE (V1.0.1 & V2.0.0) of Group IV)

The remote management mechanisms for CPE to be fully compliant with the remote management standards that the OEM chose to implement, example: TR-069 or any other relevant standards, such mechanisms to include entity mutual authentication, encryption of the management traffic.

2.1.6 Remote login restrictions for privileged users

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Direct login as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to the system remotely.

[Reference TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.6]

Requirement:
(applicable to CBC, PABX, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, or PABX of Group IV)

Direct Login to Group IV device as root or equivalent highest privileged user shall be limited to the system console only. Root user shall not be allowed to login to Group IV device 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 Group IV device.

2.1.7 Authorization Policy

('Authorization Policy- Local/Remote' is the clause name for Network Next Generation Firewall including IDS & IPS)

Requirement:
(applicable to CBC, PABX, IP Router (V1.0.1 and V2.0.0), L2 and (or) L3 LAN Switch, and Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, PABX and IP Router (V1.0.1 and V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.1]
[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.4.6.1]

2.1.8 Unambiguous identification of the user & group accounts removal

('Unambiguous identification of the user & removal of group accounts' is the clause name in CBC)

('Unambiguous identification of the user & group' is the clause name in Wi-Fi CPE (V1.0.1))

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE shall identify each login user unambiguously. CPE shall be able to assign individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. It is a desirable feature to configure user preferred USERID name in configuration menu instead of pre-configured ADMIN User ID. Use of group accounts or group credentials or sharing of the same account between several users shall not be enabled by CPE.

Requirement:

(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

The Wi-Fi CPE shall identify each login user unambiguously. Wi-Fi CPE shall be able to assign individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. The Wi-Fi CPE shall support the feature to configure user preferred USERID name in the configuration menu instead of pre configured ADMIN User ID. Use of group accounts or group credentials or sharing of the same account between several users shall not be enabled by Wi-Fi CPE.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.4.1.2]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Sections 4.2.3.4.1.2]

Requirement:
(applicable to CBC, PABX, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, IP Router

(V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, or PABX of Group IV)

Users shall be identified unambiguously by the Group IV device. Group IV device 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. I Group IV device shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.1.2]

2.1.9 Remote Management Standards for Connected Devices, Additional Features

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE shall identify each login user unambiguously. CPE shall be able to assign individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. It is a desirable feature to configure user preferred USERID name in configuration menu instead of pre-configured ADMIN User ID. Use of group accounts or group credentials or sharing of the same account between several users shall not be enabled by CPE.

Section 2.2: Authentication and Attribute Management

2.2.1 Authentication Policy

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The usage of a system functions such as network services (like SSH, SFTP, Web services), management access, local usage of operating systems and applications shall be allowed only after successful authentication on the basis of the user identity and at least one authentication attribute (e.g., password, certificate).
This requirement shall also be applied to accounts that are only used for communication between systems.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0), IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch only; to be tested on any one of Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, or IP Router (V2.0.0) of Group IV)

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: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.1.1]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g., password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, 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. An exception to the authentication and authorization requirement are functions for public use such as those for a Web server on the Internet, via which information is made available to the public.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.1.1]

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (e.g. password, certificate, token) shall be prevented. For machine-to-machine accounts one authentication attribute will be sufficient. System functions comprise, for example network services (like SSH, 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.1.1]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (e.g. password, certificate, token) shall be prevented. System functions comprise, for example network services (like SSH, 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

External authentication mechanism if supported by IP router (support authentication, authorization, and accounting server capabilities) should be through secure (encrypted) communication channel.

Requirement:

(applicable to CBC, PABX, IP Router (V2.0.0), to L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS *only; to be tested on any one of CBC, PABX, IP Router (V2.0.0, to L2 and (or) L3 LAN Switch, or* Network Next Generation Firewall including IDS & IPS *of Group IV)*

If the Group IV device supports external authentication mechanism such as AAA server (for authentication, authorization, and accounting services), then the communication between Group IV device 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.

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

If CPE supports external authentication (for the Cyber- Cafe use-case scenario), the user authentication credentials should be protected and securely communicated if the authentication credentials are managed by external authentication servers

2.2.3 Protection against brute force and dictionary attacks

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

If a password is used as an authentication attribute, a protection against brute force and dictionary attacks that hinder 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 these measures can be taken to prevent this. The most commonly used protection measures are:

i. Using the timer delay (this delay could be the same or increased depending on 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 and 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, it is often meaningful to combine two or more of the measures named here. It is left to the vendor to select appropriate measures. Above requirements shall be applicable for all passwords used (e.g., application-level, OS-level, etc.).

An exception to this requirement is machine accounts.

NOTE 1: Password management and blacklist configuration may be done in a separate node that is different to the node under test, e.g., a SSO server or any other central credential manager.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section4.2.3.4.3.3]

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

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 Group IV device.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.4.3.3]

Requirement:
(applicable to CBC, PABX, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, PABX, or Network Next Generation Firewall including IDS & IPS of Group IV)

Protection against brute force and dictionary attacks that hinder authentication attribute (i.e., password) guessing shall be implemented in Group IV device. Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attributes for user and machine accounts.

Various measures or a combination of the following measures can be taken to prevent this:

Using the timer delay (this delay could be the same or increased depending on the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").

a. 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 and an attacker can force this to deactivate accounts and make them unusable.
b. Using an authentication attribute blacklist to prevent vulnerable passwords.
c. Using Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) to prevent automated attempts (often used for Web applications). In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by Group IV device. An exception to this requirement is machine accounts

[Ref : TSDSI STD T1.3GPP 33.117-17.1.0 V1.0.1.1.0. Section 4.2.3.4.3.3]

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

CPE shall have a mechanism that provides a protection against brute force and dictionary attacks which aim to use manual/automated guessing to obtain the passwords for user and machine accounts.

CPE to detect repeated invalid attempts to sign into an account with incorrect passwords during a short period of time and it may implement at least one of the following most commonly used protection measures:

a) Increasing the delay (e.g., doubling) for each newly entered incorrect password.
b) Blocking an account after a specified number of incorrect attempts (typically 5) for acertain period of time.
c) Using CAPTCHA to prevent automated attempts.

This feature to be enabled for login attempts for CPE and on authentication attempts on Wi-Fi access through SSID with PSK.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

Wi-Fi CPE shall have a mechanism that provides a protection against brute force and dictionary attacks which aim to use manual/automated guessing to obtain the passwords for user and machine accounts.

Wi-Fi CPE to detect repeated invalid attempts to sign into an account with incorrect passwords during a short period of time and it shall implement at least one of the following, most commonly used protection measures:

i. Increasing the delay (e.g., doubling) for each newly entered incorrect password.
ii. Blocking an account after a specified number of incorrect attempts (typically 5) for a certain period of time.

iii. Using CAPTCHA to prevent automated attempts.
iv. Using a password blacklist to prevent vulnerable passwords

This feature to be enabled for login attempts for Wi-Fi CPE and on authentication attempts on Wi- Fi access through SSID with PSK.

Note: WPA3 also shall be part of the protection measures.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)
The setting by the vendor shall be such that a network product 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 network product). It shall not be possible setting this absolute minimum length to a lower value by configuration.

(ii) Comprising at least three of the following categories:
- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (e.g. @;!$.)

The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The default minimum length is the value configured by the vendor before any operator-specific configuration has been applied. The special characters may be categorized in sets according to their Unicode category.

If a central system is used for user authentication password policy is performed on the central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this subclause. If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the Network Product.

When a user is changing a password or entering a new password the system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g., application-level, OS-level, etc.).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3]

Requirement:
(applicable to CBC, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

a) The configuration setting shall be such that Group IV device 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 Group IV device). 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 Group IV device .

e) When a user is changing a password or entering a new password, Group IV device /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: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.1]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

The configuration setting shall be such that an PABX 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 PABX). It shall not be possible setting this absolute minimum length to a lower value by configuration.

(ii) Password shall mandatorily comprise all the following four categories of characters:

- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (e.g. @;!$.)

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.
PABX shall have in-built mechanism to support this requirement, further 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 subclause.
And if a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the PABX.
When a user is changing a password or entering a new password, PABX/central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).
[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.3.4.3.1]

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

CPE shall only accept passwords that comply with the following complexity criteria:

1. Password containing a minimum length of 8 characters are only permitted by default. Shorter lengths shall be rejected by the NE.
2. Minimum password length - the default minimum value of 8 characters.
3. Password comprises at least three of the following categories:
    a. at least 1 uppercase character (A-Z)
    b. at least 1 lowercase character (a-z)
    c. at least 1 digit (0-9)
    d. at least 1 special character (e.g., @; $.)

CPE shall support password field length of minimum 64 characters.

This Feature to be enabled for CPE Login-IDs as well as for the PSK key associated with SSID for Wi-Fi access.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

a. The configuration setting shall be such that Wi-Fi CPE 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 Wi-Fi CPE). It shall not be possible setting this absolute minimum length to a lower value by configuration. ii.
    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 Wi-Fi CPE.
e. When a user is changing a password or entering a new password, Wi-Fi CPE /central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g., application-level, OS level, etc.). Passwords shall not be stored in clear text in the system; passwords shall be salted and hashed.

f. This Feature to be enabled for Wi-Fi CPE Login-IDs as well as for the PSK key associated with SSID for Wi-Fi access.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.4.3.1]

2.2.5 Inactive Session Timeout

Requirement:

(applicable to CBC and PABX only; to be tested on any one of CBC or PABX of Group IV)

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.

Device shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values can be admin configurable as per requirement, normally set between 2 to 5 minutes.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.5.2]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

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.

NOTE: The kind of activity required to reset the timeout timer depends on the type of user session.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.5.2]

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS *only; to be tested on any one of IP Router (V2.0.0), L2 and (or) L3 LAN Switch, or* Network Next Generation Firewall including IDS & IPS *of Group IV)*

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. Group IV device

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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.5.2]

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

CPE shall monitor inactive sessions of administrative login users, Data users either on LAN or Wi-Fi and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values can be admin configurable as per requirement. When the time out occurs, the same screen must be cleared of all displayed information.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

Wi-Fi CPE shall monitor inactive sessions of administrative login users, data users either connected over Wi-Fi and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values shall be admin configurable as per requirement. When the time out occurs, the same screen must be cleared of all displayed information for admin users.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.5.2]

2.2.6 Password Change

('Password Change facility, 1st Installation /Factory Reset' is the clause name in Wi-Fi CPE (V1.0.1 & V2.0.0))

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

CPE shall enforce change of authentication attribute (eg: - password) on 1st installation configuration or on factory reset conditions. If a password is used as an authentication attribute, then the CPE shall provide a function that facilitates the user to change his password at any time. However, the CPE shall not allow the previously used passwords up to a certain number (Password History)

Requirement:
(applicable to Wi-Fi CPE (V2.0.0), IP Router (V1.0.1) only; to be tested on any one of Wi-Fi

CPE (V2.0.0), or IP Router (V1.0.1) of Group IV)

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 is possible to redirect or implement this function on this system. Password change shall be enforced after initial login. The system shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. 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 default value shall be 3.

This means that the device shall store at least the three previously set passwords. The maximum number of passwords that the device 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, OS-level, etc.). An exception to this requirement is machine accounts.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.4.3.2]

Requirement:
(applicable to CBC and PABX only; to be tested on any one of CBC, or PABX of Group IV)

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

Password change shall be enforced after initial login.

Group IV device shall enforce password change based on password management policy.

In particular, the system shall enforce password expiry. Group IV device shall support a configurable period for expiry of passwords.

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

The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its minimum value shall be 3. This means that the Group IV device shall store at least the three previously set passwords. The maximum number of passwords that the Group IV device 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, OS level, etc.). An exception to this requirement is machine accounts.

Group IV device to have 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 Group IV device .

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.2]

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

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). Group IV device shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. Group IV device 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 Group IV device shall store at least the three previously set passwords. The maximum number of passwords that the Group IV device 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, OS level, etc.). An exception to this requirement is machine accounts.

Group IV device 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 Group IV device.

The minimum password age shall be set as one day i.e., recycling or flipping of passwords to immediate return to favorite 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: TEC 64498:2024/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]
[Ref [Network Next Generation Firewall including IDS & IPS]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.0.1.1.0. Section 4.2.3.4.3.2]
[Ref [Network Next Generation Firewall including IDS & IPS]: CIS_Benchmarks_Password_Policy_Guide_V2.0.01.12]

2.2.7 Protected Authentication feedback

Requirement:
(applicable to CBC, Wi-Fi CPE (V1.0.1) and PABX only; to be tested on any one of CBC, Wi-Fi CPE (V1.0.1) and PABX of Group IV)

The Authentication attribute 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 is replaced by a character such as "*".

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.4]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

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 "*". Under certain circumstances it may be permissible for an individual character to be displayed briefly during input. Such a function is used, for example, on smartphones to make input easier. However, the entire password is never output to the display in plaintext.

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.4]

Requirement:
(applicable to Wi-Fi CPE (V2.0.0), IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch only; to be tested on any one of Wi-Fi CPE (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, or IP Router (V2.0.0) of Group IV)

The Authentication attribute 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 passwords used (e.g., application-level, OS level, Wireless Access etc.). An exception to this requirement is machine accounts.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.4.3.4]
[Ref: TSDSI STD T1.3GPP 33.117-17.5.0 V1.0.1.5.0 Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), CBC, L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS and PABX only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), CBC, L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS or PABX of Group IV)

Predefined or default authentication attributes shall be deleted or disabled. Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, vendor, 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 vendor provides instructions on how to manually change it.

[Reference CBC, PABX and IP Router V1.0.1: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 5.2.3.4.2.3]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V1.0.1.1.0. Section 4.2.3.4.2.3]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section 5.2.3.4.2.3]

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) only; to be tested only on Wi-Fi CPE (V1.0.1 &

V2.0.0) of Group IV)

Wi-Fi CPE may come with predefined (by the vendor, developer, or producer) authentication attributes such as password or cryptographic keys. Wi-Fi CPE shall remove the predefined / default authentication attributes from its run-time configuration. Such predefined authentication attributes shall be restored only through factory reset, preferably through operating a physical button.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.4.2.3]

2.2.9 Logout Function

Requirement:

(applicable to IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS or Wi-Fi CPE (V2.0.0) of Group IV)

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: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.5.1]

2.2.10 Storage of Passwords in encrypted form

Requirement:

(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

User passwords should be stored using password hashes or encrypted, based on a strong hashing mechanism designed for use with passwords (example: HMAC, PBKDF2, Argon2), OEM may choose his own hashing mechanism for implementation. Passwords may not be stored in clear text. This requirement does not apply to pre-shared keys that must be used in raw form, such as IKE pre-shared keys.

2.2.11 Policy regarding consecutive failed login attempts

Requirement:

(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS and Wi-Fi CPE (V2.0.0) only; to be tested on any one of IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS or Wi-Fi CPE (V2.0.0) of Group IV)

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: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.5]

2.2.12 Suspend accounts on non-use

Requirement:
(applicable to IP Router (V2.0.0) and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0) or L2 and (or) L3 LAN Switch of Group IV)

It shall be possible for the system to automatically suspend an account after 'X' days without a valid login. Only the highest privilege accounts shall be exempted from this requirement.

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

[Ref: CIS Password Policy Guide]

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

It shall be possible to configure 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_Benchmarks_Password_Policy_Guide_v21.12

Section 2.3: Software Security

2.3.1 Secure Update

Requirement:

(applicable to CBC only; to be tested only on CBC of Group IV)

For software updates, device shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using the secure cryptographic controls prescribed in Table1 of the latest

document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

To this end, the device has a list of public keys or certificates of authorized software sources and uses the keys to verify that the software update is originated from only these sources.

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Device’s system software updates should be secure and shall be based on signed certificates. Device shall allow updates only if code signing certificate is valid and time not expired, the software update integrity shall be verified by hashing mechanism (like SHA2).

Note: TSPs are responsible to ensure that Software updates/patches implemented are secure and safe from any vulnerability. TSPs to maintain information about updates as per Licensing agreement /amendment conditions. However, if there is any patch/update/version change which affects the security functionality then the details of the same should be reported to TTSC/DOT by vendor /TSPs.

Requirement:

(applicable to IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch *only; to be tested on any one of IP Router (V2.0.0),* Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch *of Group IV)*

a) Software package integrity shall be validated during the software update stage.
b) Group IV device 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 Group IV device 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: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.3.5]

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.0.1.1.0. Section 4.2.3.3.5]

Requirement:

(applicable to PABX only; to be tested only on PABX of Group IV)

PABX’s system software updates shall be carried out strictly using the secure

cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

PABX shall allow updates only if code signing certificate is valid and not time expired. Software update integrity shall be verified strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

Requirement:
(applicable to Wi-Fi CPE (V1.01) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)
The update process should verify the authenticity of the source repository and the integrity of the software patch preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity before updating the software in the CPE. The update mechanism should prevent illegal software patching.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

The update process shall verify the authenticity of the source repository and the integrity of the software patch preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity before updating the software in the Wi-Fi CPE. (Digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only). The update mechanism shall prevent illegal software patching. A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

2.3.2 Secure Upgrade

('Secure Upgrade Requirement' is the clause name in CBC)

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

CPE should support authenticity and integrity check while performing software upgrade Preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

Wi-Fi CPE shall support authenticity and integrity check while performing software upgrade and installation preferably employing digital certificate for authenticity and hashing (example: SHA2) for integrity. (Digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only). A security mechanism is required to guarantee that only authorized individualscan initiate and deploy a software upgrade.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

i. Software package integrity shall be validated in the installation/upgrade stage.
ii. Network product shall support software package integrity validation via cryptographic means, e.g., digital signature. To this end, the network product has a list of public keys or certificates of authorized software sources and uses the keys to verify that the software update is originated from only these sources.
iii. Tampered software shall not be executed or installed if integrity check fails.
iv. A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in bullet (ii).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5]

Requirement:
(applicable to CBC, PABX, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, PABX, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

a) Software package integrity shall be validated during the software upgrade stage.
b) Group IV device 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 Group IV device 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: TEC 64498:2024/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:
(applicable to CBC, PABX, Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, and Network Next Generation Firewall including IDS & IPS; to be tested on any one of CBC, PABX, Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

"In fulfillment of this clause, the OEM shall submit the following documents:

i) Internal test report excluding Intellectual Property (IP) related information, but mandatorily including summary of number of security vulnerabilities/weaknesses classified by risk.

ii) The "Self-Declaration of Conformity" to the extent of adhering to the development and
testing procedure stipulated in ITSAR as per the enclosed proforma/format"

2.3.4 Known Malware and backdoor check

('Known Malware Check' is the clause name in Wi-Fi CPE (V1.0.1 & V2.0.0) and IP Router (V1.0.1))

Requirement:
(applicable to CBC, PABX, Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, and Network Next Generation Firewall including IDS & IPS; to be tested on any one of CBC, PABX, Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

OEM shall submit Self Declaration of Conformity in the enclosed proforma/format stating that the product is free from all known malware as per the malware signature database prescribed by NCCS and also it is free from backdoors.

2.3.5 No unused software

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

Unused software components or parts of software which are not needed for operation or functionality of the CPE shall not be installed or shall be deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g., default web pages, example databases, test data). OEM to provide Software Test Document (STD) in this regard.

Requirement:
(applicable to CBC, Wi-Fi CPE (V2.0.0), IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, or IP Router (V2.0.0) of Group IV)

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

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.3.2.3]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Unused software components or parts of software which are not needed for operation or functionality of the Device shall not be installed or shall be deleted after installation. This also includes parts of a software, which will be installed as examples but typically not be used (e.g. default web pages, example databases, test data).

Note: Vendor shall provide the list of software that are necessary for its operation.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.3]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

Software components or parts of software which are not needed for operation or functionality of the PABX shall not be present. Orphaned software components /packages shall not be present in PABX. OEM shall provide the list of software that are necessary for its operation.

[Reference: TSDSI STD T1.3GPP 33.117 -14.2.0 V.1.0.0 Section 4.3.2.3]

2.3.6 Unnecessary Service Removal

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The OEM to provide list of essential services and the related ports required for functioning of CPE, list of optimal services supported by CPE and their related ports. The CPE 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 and their ports shall be initially configured to be disabled on the CPE by the vendor.

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPV1.0.1 and V2.0.0
- SSHV1.0.1, HNAP
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server

- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD
- MOP

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

Wi-Fi CPE 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 Wi-Fi CPE by the vendor except if services are needed during deployment.

In that case those services shall be disabled according to vendor's instructions after deployment is done. Disabled protocols may still need to be enabled for other reasons by the operators, e.g., remote diagnostics.

Wi-Fi CPE 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) V1.0.1 and V2.0.0
g) SSHV1.0.1
h) Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Small Servers (Echo, Charges, 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 Wi-Fi CPE and their purpose need to be provided by the OEM as a prerequisite for the test case.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.3.2.1]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Device shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. device shall not support following services

i) FTP
ii) TFTP
iii) Telnet
iv) rlogin, RCP, RSH
v) HTTP
vi) SNMPV1.0.1 and V2.0.0
vii) SSHV1.0.1, HNAP
viii) TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
ix) Finger
x) BOOTP server
xi) Discovery protocols (CDP, LLDP)
xii) IP Identification Service (Identd)
xiii) PAD
xiv) 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 device and their purpose needs to be provided by the OEM as prerequisite for the test case. OEM shall submit "Communication Matrix" clearly showing the services and ports used.

NOTE 1: As an alternative to disabling the HTTP service, it is also possible for this service to remain active for reasons of user friendliness. In this case, however, queries to the web service may not be answered directly on this port but from a redirected to HTTPS service.

NOTE 2: Full documentation of required protocols and services of the Network product and their purpose needs to be provided by the vendor as prerequisite for the test case.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.1]

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

Group IV device 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 Group IV device 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. Group IV device 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, Charges, 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 (Idents)
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 Group IV device and their purpose need to be provided by the OEM as a prerequisite for the test case.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.1]

Requirement:
(applicable to CBC and PABX only; to be tested on any one of CBC or PABX of Group IV)
Group IV device shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. Group IV device shall not support following services

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPv1 and v2
- SSHv1
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD

Any other protocols, services that are vulnerable are also to be permanently disabled. Full documentation of required protocols and services (communication matrix) of the Group

IV device and their purpose needs to be provided by the OEM as prerequisite for the test case. OEM shall submit "Communication Matrix" clearly showing the services and ports used.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.1]

2.3.7 Secure Time Synchronization

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE shall support time synchronization feature for its core functionality or for the additional supported functionality. For CPEs that have time synchronization feature, it shall support the secure time synchronization feature preferably by using Network Time Protocol NTP.

The CPE clock shall be synchronized with NTP server in a secure manner. The CPE client should be able to verify the authentication and authorization of the NTP Server.

OEM shall plugin well known vulnerabilities, input validation vulnerabilities related to NTP feature.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch, IP Router (V2.0.0) only; to be tested on any one of Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch, or IP Router (V2.0.0) of Group IV)

Group IV device 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.

Group IV device 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. Group IV device shall generate audit logs for all changes to time settings.

Group IV device 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.

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Device shall provide reliable time and date information provided manually by itself or through NTP server. Device should generate audit logs for all changes to time settings. Device should support to configure authentication between itself and external NTP server.

Requirement:
(applicable to CBC and PABX only; to be tested any one of CBC and PABX of Group IV)

Group IV device shall provide reliable time and date information provided through NTP/PTP server. Group IV device shall establish secure communication channel with the NTP/PTP server. Group IV device shall establish secure communication channel strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" with NTP/PTP server. Group IV device shall generate audit logs for all changes to time settings.

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

Next Generation Firewall 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.

Next Generation Firewall 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.

Next Generation Firewall shall generate audit logs for all changes to time settings.

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

[Ref [7]: RFC 8915 - Network Time Security for the Network Time Protocol (NTP).]

2.3.8 Self-Testing

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE shall support the detection mechanism for identification of failure of underlying security mechanisms (such as software image integrity, runtime integrity, cryptographic modules etc.) used. The CPE to perform such self-tests periodically/at the time of booting, visual indication on failure is a desirable feature.

Requirement:

(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

The Wi-Fi CPE's cryptographic module shall perform power-up self-tests and should perform periodic 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 boot up/restart.

Conditional self-tests should 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.

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Device shall perform self-tests to identify failures in its security Mechanisms during i) power on ii) when administrator instructs. (e.g., integrity of the firmware and software as well as for the correct operation of cryptographic functions, etc.,)

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

The Group IV device's cryptographic module shall perform power-up self-tests and should perform 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 should 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.

Requirement:

(applicable to CBC only; to be tested only on CBC of Group IV)

Device shall perform self-tests (integrity of the firmware and software as well as correct operation of cryptographic Module as per security requirement area of "self-test" of FIPS140-2 or Later version etc.,) to identify failures in its security mechanisms during i) power on ii) when the Administrator Instructs iii) Periodic, with period configurable and iv) at the time of restart.

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

PABX shall perform self-tests (integrity of the firmware and software as well as correct operation of cryptographic Module as per security requirement area of "self-test" of FIPS 140-2 or Later version etc.,) to identify failures in its security mechanisms during i) power on ii) when Administrator Instructs iii) Periodic, with period configurable.

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

Next Generation Firewall'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.

2.3.9 Restricted reachability of services

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE 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 CPE to only LAN ports and not to permit access on Wi-Fi, WAN side.

Requirement:
(applicable to IP Router (V2.0.0 & V2.0.0), L2 and (or) L3 LAN Switch only; to be tested on any one of and IP Router (V1.0.1 & V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

The Group IV device shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. On interfaces where services are active, the reachability should be limited to legitimate communication peers. This limitation shall be realized on the device itself.

Example: Administrative services (e.g., SSH, HTTPS, RDP) shall be restricted to interfaces in the management network to support separation of management traffic from user traffic.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.2]

Requirement:
(applicable to CBC and PABX only; to be tested on any one of CBC, or PABX of Group IV)

The Group IV device shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers. Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted to interfaces in the management plane for separation of management traffic from user traffic.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.2]

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

Next Generation Firewall 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 should be limited to legitimate communication peers. This limitation shall be realized on the Next Generation Firewall itself (without 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 [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.3.2.2]

2.3.10 Restricting System Boot Source

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, CBC and PABX only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), CBC, Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, or PABX and of Group IV)

The Group IV device can boot only from the memory devices intended for this purpose. The device can only boot from memory devices intended for this purpose (e.g., not from external memory like USB key).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.]
[Reference [IP Router (V2.0.0)]: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.3.2]

2.3.11 Avoidance of Unspecified Wireless Access

('Avoidance of Unspecified mode of Access' is the clause name in CBC, Network Next Generation Firewall including IDS & IPS, IP Router (V2.0.0), L2 and (or) L3 LAN Switch)

Requirement:
(applicable to CBC, IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, and PABX only; to be tested on any one of CBC, Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, or PABX of Group IV)

Group IV device shall not contain any access mechanism which is unspecified or not declared. An undertaking shall be given by the OEM as follows:

Group IV device does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel.
Note: Network product supporting standard wireless technologies would also need to be tested for this requirement apart from wireless technology related tests.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.6.1]

2.3.12 Feature / Service Activation Policy

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) only; to be tested only on Wi-Fi CPE (V1.0.1 & V2.0.0) of Group IV)

The Wi-Fi CPE shall have factory default settings where only the essential features, services and ports necessary for its primary operational functions of Wi-Fi CPE are enabled. Optional features, additional services and future oriented applications should be disabled by default. These disabled services can only be activated after successful authentication and selection by an ADMIN user.

Section 2.4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS and IP Router (V1.0.1 & V2.0.0) only of Group IV; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS and IP Router (V1.0.1 & V2.0.0) of Group IV)

Unused functions of the Group IV device software and hardware shall be deactivated. During installation of software and hardware often functions will be activated that are not required for operation or function of the system. If unused functions of software cannot be deleted or de-installed individually as given under requirement "2.3.6 No unused software" of this document, such functions shall be deactivated in the configuration of the

Group IV device permanently.

Also, hardware functions which are not required for operation or function of the system (e.g., unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after Group IV device reboot. Example: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the Group IV device.

OEM to provide report in this regard, List of the used functions of the Group IV device software and hardware as given by the OEM shall match the list of used software and hardware functions that are necessary for the operation of the Group IV device.

Note: List of the used functions of the Networks s software and hardware as given by the vendor shall match the list of used software and hardware functions that are necessary for the operation of the Network product.

[Ref [Wi-Fi CPE (V2.0.0)]: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.3.2.4]
[Reference [IP Router (V1.0.1)]: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.4]
[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.3.2.4]

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

Unused functions i.e the software and hardware functions which are not needed for operation or functionality of the CBC shall be deactivated in the CBC's software and/or hardware. 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 CBC.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.4]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

Unused functions i.e. the software and/or hardware functions which are not needed for operation or functionality of the PABX shall not be present in the PABX's software and/or hardware. List of the used functions of the Networks s software and hardware as given by the OEM shall match the list of used software and hardware functions that are necessary for the operation of the PABX.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) only; to be tested only on Wi-Fi CPE (V1.0.1 & V2.0.0) of Group IV)

The Group IV device shall not contain software and hardware components that are no longer supported by their vendor, producer, or developer, such as components that have reached end-of-life or end- of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime. OEM to provide report and declaration to this effect.

[Ref [Wi-Fi CPE (V2.0.0)]: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.3.2.5]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

The Network product shall not contain software and hardware components that are no longer supported by their vendor, producer or developer, such as components that have reached end of-life or end-of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.5]

Requirement:
(applicable to CBC, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch only; to be tested on any one of CBC, Network Next Generation Firewall including IDS & IPS, IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

OEM to ensure that the Group IV device 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 open-source 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: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.5]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

OEM to ensure that the PABX shall not contain software and/or hardware components that are no longer supported by OEM or its third parties including the open-source communities, such as components that have reached end-of-life or end-of-support.

2.4.3 No Known Vulnerabilities in System on Chip (SOC) solution

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

This test is applicable for such CPEs which have System on Chip solutions, where majority of CPE functions are realized in a VLSI chip. OEM to provide self-test / third-party / Chip vendor test report indicating that the SOC is free from malware, known-vulnerabilities.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

This test is applicable for such Wi-Fi CPEs which have System on Chip solutions, where majority of Wi-Fi CPE functions are realized in a VLSI chip. OEM to provide self-test / third-party / Chip- vendor test report indicating that the SOC is free from malware, known-vulnerabilities for all products manufactured after publishing of this ITSAR. In respect of products manufactured before publishing of this ITSAR, OEM to provide either self-test / third-party / Chip- vendor test report indicating that the SOC is free from malware, known-vulnerabilities, or a proof that the product is listed in Trusted Telecom Portal (TTP).

Section 2.5: User Audit

2.5.1 Audit trail storage and protection

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch of Group IV)

The security event log of Group IV device 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 (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0 section 4.2.3.6.3]
[Reference (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0. V.1.0.0 section 4.2.3.6.3]

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

The security event log shall be access controlled (file access rights) such that only privilege users including the administrator have access to read the log files. The only allowed operations on security event log are archiving/saving and viewing.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0. section 4.2.3.6.3]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

The security event log shall be access controlled using file access rights such that only privilege users including the administrator have access to read the log files. Log file shall not to be manually deleted/modifiable by the user.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0 section 4.2.3.6.3]

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

The security event log shall be access-controlled (file access rights) such only privileged users have access to the log files.

[Ref : TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

CPE to have capability to log important Security events. The audit logs may preferably be stored in non-volatile memory. If applicable (for cyber-cafe, Public Data Office usage scenario) provision for secure log export should exist and logs may capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

Wi-Fi CPE shall have capability to log all Security events. The audit logs shall be stored in non-volatile memory. Logs shall capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc. In particular, it shall be possible to log the following events (which are intended to be supported by the device and which can be enabled by default at manufacturing time or at a later time by the network operator):

Additional audit record information, depending on the audit event, shall also be provided as given in the Table (*Refer Group IV Event Table below*):

[Ref (Wi-Fi CPE (V2.0.0)): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.6.1]

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, CBC and PABX only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, CBC, or PABX of Group IV)

The Group IV device shall log all important security events with unique system reference details as given in the Table below.

Group IV device 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 (*Refer Group IV Event Table below*):

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.6.1 and section 4.2.3.2.5]

[Reference (IP Router (V2.0.0)): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. Section 4.2.3.6.1]

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

Next Generation Firewall shall log all important Security events with unique System Reference details as given in the table below. Next Generation Firewall shall record within each audit record at least information pertaining to date and time of the event, type of event, subject identity, protocol, service or program used for access, source and destination IP addresses & ports 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 (*Refer the Group IV Events Table below*):
Note: The security events generated by IdAM/IAM are also acceptable.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.6.1]

Group IV Events Table

Sl.no	Event Types (Mandatory or optional)	Description	Event data to be logged
1	Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the Group IV device	Username, Source (IP address) if remote access Outcome of event (Success or

			failure) (not applicable to Wi-Fi CPE V2.0.0)
			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) (not applicable to Wi-Fi CPE V2.0.0)
			Source (IP address) if remote access
3	Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, copy (not applicable in IP Router (V1.0.1), PABX, Wi-Fi CPE (V2.0.0)), enable, and disable.	Administrator username,
			Administered account,
			Activity performed (configure, delete, enable and disable)
			Outcome of event (Success or failure) (not applicable to Wi-Fi CPE V2.0.0)
			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 exceeded their defined thresholds.	Value exceeded,
			Value reached (Here suitable threshold values shall be defined depending on the individual system.)
			Outcome of event (Success or failure) (not applicable to Wi-Fi CPE V2.0.0) (Exclusive to CBC: Outcome of event (Threshold Exceeded))
			Timestamp
5	Configuration change (Mandatory)	Changes to configuration of the Group IV device	Change made
			Timestamp (not applicable to Wi-Fi CPE V2.0.0)
			Outcome of event (Success or failure) (not applicable to Wi-Fi CPE V2.0.0)
			Username
6	Reboot/shutdown/crash (Mandatory)	This event records any action on the Group IV device that forces a reboot or shutdown OR where the Group IV device has crashed	Action performed (reboot, shutdown, etc.)
			Username (for intentional actions)
			Outcome of event (Success or failure) (not applicable to Wi-Fi CPE V2.0.0)

			Timestamp
7	Interface status change (Mandatory)	Change to the status of interfaces on the Group IV device (e.g. shutdown)	Interface name and type
			Status (shutdown, missing link, etc.)
			Outcome of event (Success or failure) (not applicable to Wi-Fi CPE V2.0.0)
			Timestamp
8	Change of group membership or accounts (Mandatory) (Optional) in IP Router (V1.0.1), PABX, Wi-Fi CPE (V2.0.0)	Any change of group membership for accounts	Administrator username,
			Administered account,
			Activity performed (group added or removed)
			Outcome of event (Success or failure) (not applicable to Wi-Fi CPE V2.0.0)
			Timestamp.
9	Resetting Passwords (Mandatory) (Optional) in IP Router V1.0.1,PABX, and CBC (Not applicable to Wi-Fi CPE V2.0.0)	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) (Optional) in IP Router V1.0.1, PABX, and CBC (Not applicable to Wi-Fi CPE V2.0.0)	Starting and Stopping of Services (if applicable)	Service identity
			Activity performed (start, stop, etc.)
			Timestamp
			Outcome of event (Success or failure)
11	User login (Mandatory) (Not applicable to Wi-Fi V2.0.0)	All use of identification and authentication mechanism	user identity
			origin of attempt (e.g. IP address)
			Timestamp
			outcome of event (Success or failure)
12	X.509 Certificate Validation (Optional) (Not applicable to Wi-Fi CPE V2.0.0)	Unsuccessful attempt to validate a certificate	Timestamp
			Reason for failure
			Subject identity
			Type of event
13	Secure Update (Mandatory) (Optional) in IP Router V1.0.1, PABX, and CBC (Not applicable to Wi-Fi CPE V2.0.0)	Attempt to initiate manual update, initiation of update, completion of update	user identity
			Timestamp
			Outcome of event (Success or failure)
			Activity performed
14	Time change (Mandatory)	Change in time	Old value of time

	(Not applicable to Wi-Fi CPE V2.0.0)	settings	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
15	Session unlocking/ termination (Optional) (Not applicable to Wi-Fi CPE V2.0.0)	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
16	Trusted Communication paths (with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorized remote administrators) (Optional) (Not applicable to Wi-Fi CPE V2.0.0)	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)
17	Audit data changes (Mandatory) (Optional) in IP Router V1.0.1, PABX, and CBC (Not applicable to Wi-Fi V2.0.0)	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, as applicable)
			Subject identity
			user identity
			origin of attempt to change time (e.g. IP address)
			Details of data deleted or modified
18	Port Scan Attempt (Not applicable to Wi-Fi CPE V2.0.0, IP Router V1.0.1 & V2.0.0, LAN Switch, NGFW) (Exclusive to CBC and PABX only)	Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters	Date
			Time Stamp
			Source IP address
			Destination Port address

19	Access Control Policy violations (mandatory) (Not applicable to Wi-Fi CPE V2.0.0, CBC, IP Router V1.0.1, PABX, NGFW) (Exclusive to L2 and (or) L3 LAN Switch and IP Router V2.0.0 only)	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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.6.1; 2) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.5]

2.5.3 Secure Log Export

Requirement:
(applicable IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

a) The Group IV device shall support forward of security event logging data to an external system.
b) Log functions should support secure uploading of log files to a central location or to a system external for the Group IV device that is logging.
   i. Group IV device shall be able to store generated audit data itself may be with limitations.
   ii. In the absence of external system, Group IV device shall support facility to drop new audit data or overwrite old audit data based on defined criteria in case of its own log buffer full.
   iii. Group IV device shall alert administrator when its log buffer reaches configured threshold limit.

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

a. Group IV device 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 Group IV device.
c. Group IV device 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.

[Reference: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.6.2]

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

a) Next Generation Firewall shall support (near real time) forwarding of security event logging data to an external system available in redundant configuration by push or pull mechanism through diverse links.
b) Log functions should support secure uploading of log files to a central location or to a system external for the Next Generation Firewall.
c) Next Generation Firewall shall be able to store the generated audit data locally. The memory for this purpose shall be dimensioned to cater for the continuous storage of two days of audit 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 33.117-17.1.0 V.1.1.0. Section 4.2.3.6.2]

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

(a) (i) The CBC shall support forwarding of security event logging data to an external system by push or pull mechanism.
(ii) Log functions should support secure uploading of log files to a central location or to a system external for the CBC.
(b) CBC shall be able to store the generated audit data itself may be with limitations.
(c) CBC shall alert administrator when its security log buffer reaches configured threshold limit.
(d) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), CBC shall have mechanism to store audit data locally. CBC shall have sufficient memory (minimum 100 MB) allocated for this purpose. The OEM to submit justification document for sufficiency of local storage requirement.
(e) Secure Log export shall comply the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.6.2]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)
(i) (a) The PABX shall support forward of security event logging data to an external

system by push or pull mechanism.

(b) Log functions should support secure uploading of log files to a central location or to a system external for the PABX.

(ii) PABX shall be able to store generated audit data itself, may be with limitations.

(iii) PABX shall alert administrator when its security log buffer reaches configured threshold limit.

(iv) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), PABX shall have mechanism to store audit data locally. PABX shall have sufficient memory to be allocated for storing minimum 10000 security events for this purpose. OEM to submit justification document for sufficiency of local storage requirement.

(v) Secure Log export shall comply the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.6.2]

2.5.4 Logging access to personal data

Requirement:

(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

In some cases, access to personal data in clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes, such logging is not available, a coarser grain logging is allowed.

In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation.

[Ref: TSDSI STD T1.33.117-17.1.0 V1.0.1.1.0. Section 4.2.3.2.5]

2.5.5 Security audit log:

Requirement:

(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

The security audit log must not contain

1) Authentication credentials, even if encrypted (e.g. password)

2) Access Tokens-To be masked when outputting

3) Proprietary or sensitive personal information

[Ref: GSMA NG 133 Cloud Infrastructure Reference Architecture Ver 2.0 6.3.7.3]

2.5.6 Audit Logs

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

1) All security logging mechanisms must be active from system initialization

2) Logs must be time synchronized

3) Security audit logs must be protected in transit and at rest

4) The following systems events must be logged (apart from those listed in 2.5.2)

   a) Successful and unsuccessful changes to privilege level

   b) Successful and unsuccessful security policy changes

   c) Starting and stopping of security logging

   d) Starting and stopping of processes including attempts to start unauthorized processes

   e) All command line activity performed by innate OS programs known to otherwise leave no evidence upon command completion including Power shell on windows system.

[Ref: GSMA NG 133 Cloud Infrastructure Reference Architecture version 2.0 6.3.7.1 and 6.3.7.2]

2.5.7 Centralized log Auditing

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

Next Generation Firewall must be able to 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.

Note: This clause requires external system 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 fulfilment of this clause.

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

Section 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The communication security dimension 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 data is protected against well know attacks related to Sniffing, Disclosure, reconnaissance etc.,

The secure communication mechanisms between the CPE and connected entities shall use industry standard protocols such as IPSEC, VPN, SSH, TLS/SSL, etc., and NIST specified cryptographic algorithms with specific key sizes such as SHA, Diffie-Hellman, AES etc.

Requirement
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

The communication security dimension 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 data is protected against well know attacks related to Sniffing, Disclosure, reconnaissance etc.,

The secure communication mechanisms between the Wi-Fi CPE and connected entities shall use industry standard protocols such as IPSEC, VPN, SSH, TLS/SSL, etc. with specified cryptographic algorithms with specific key sizes such as SHA, Diffie-Hellman, AES etc. The Wi-Fi CPE 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 Wi-Fi CPE 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.

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Secure communication mechanism between the group IV device and the connected entities shall use only the industry standard and NIST recommended cryptographic protocols such as IPSEC, VPN, SSH, TLS/SSL, etc.
Also, group IV device shall provide all cryptographic service such as encryption, decryption, key exchange, authentication, data integrity etc. using the industry accepted

and NIST recommended cryptographic algorithms (with standard key lengths) such as SHA, Diffie-Hellman, AES, RSA etc.

Requirement:
(applicable to IP Router (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

Group IV device 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 Group IV device 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.

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

PABX shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)"

2.6.2 Cryptographic Based Secure Communication on Wi-Fi Access

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

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.

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

2.6.3 Cryptographic Module Security Assurance

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

An undertaking shall be provided by the vendor as below: Cryptographic module embedded inside the Group IV device (which may be in the form of hardware, software, or firmware) that provides all the necessary security services such as authentication,

integrity and confidentiality are designed and implemented in compliance with FIPS 140-2 standards for different levels of security.

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch, and Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

Cryptographic module embedded inside the Group IV device (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 Group IV device (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]

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

Cryptographic module embedded inside the CBC (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 CBC (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". OEM shall also submit cryptographic module testing document and the detailed self / Lab test report along with test results for scrutiny CBC shall support the minimum-security level of 2 as defined in FIPS 140-2.

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the PABX (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." OEM shall submit cryptographic Module testing document and the detailed self / Lab test report along with test results for scrutiny.

2.6.4 Cryptographic Algorithms implementation Security Assurance

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

An undertaking shall be provided by the vendor as below:
Cryptographic algorithms embedded in the crypto module of Group IV device are implemented in compliance with respective FIPS standards (for the specific crypto algorithm).

Requirement:
(applicable to IP Router (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

Cryptographic algorithm implemented inside the Crypto module of Group IV device 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 Group IV device)."

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithms embedded in the crypto module of PABX shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm)." OEM shall submit cryptographic algorithm implementation testing document and the detailed self / Lab test report along with test results for scrutiny.

2.6.5 Cryptographic Algorithm selection for Wi-Fi Access

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

It 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.

2.6.6 Protecting data and information – Confidential System Internal Data

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

When CPE is not in debug (maintenance) mode, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such system functions could be, for example, local or remote OAM CLI or GUI, error messages, 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 and could be of advantage to attackers (i.e., stack traces in error messages).

[Ref (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0. Section 4.2.3.2.2.]

Requirement:
(applicable to Wi-Fi CPE (V2.0.0), IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, CBC and PABX only; to be tested on any one of Wi-Fi CPE (V2.0.0), IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS, CBC and PABX of Group IV)

a. When Group IV device 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 to users and administrators. Such system functions could be, for example, local or remote OAM CLI or GUI, error messages, 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 and could be of advantage to attackers (i.e., stack traces in error messages).

b. Access to maintenance mode should be restricted only to authorized privileged user.

[Reference(V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.2.2]
[Ref (V2.0.0): TSDSI STD T1.33.117-17.1.0 V1.0.1.1.0. Section 4.2.3.2.2.]
[Ref (CBC and PABX): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section.4.2.3.2.2]

2.6.7 Crypto-Key Protection Mechanism

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE to have protection mechanisms against access to keys in the CPE against Key disclosure, reconnaissance, re-installation attacks, nonce-resets, Zeroing blocks of key etc.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

The Wi-Fi CPE shall have protection mechanisms against access to keys in the Wi-Fi CPE against key disclosure or any equivalent.

2.6.8 Protecting data and information in storage

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation.

Requirement:
(applicable to CBC, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, *Wi-Fi CPE (V2.0.0), and IP Router (V2.0.0) only; to be tested on any one of CBC,* Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 LAN Switch, *Wi-Fi CPE (V2.0.0), or IP Router (V2.0.0) of Group IV)*

a. For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of Group IV device 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 Group IV device shall be protected against manipulation strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.2.3]
[Ref(LAN): TSDSI STD T1.3GPP 33.117-17.5.0V1.5.0 Section 4.2.3.2.3]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of system that are needed for the functionality shall be protected against manipulation.

In addition, the following rules apply for:

i) Systems that need access to identification and authentication data in the clear, e.g., in order to perform an authentication. Such systems shall not store this data in the clear, 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.
iii) Stored files: examples for protection against manipulation are the use of checksum or cryptographic methods.

[Reference (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

For Sensitive data in storage (persistent or temporary), read access rights shall be restricted. Files of PABX system that are needed for the functionality shall be protected against manipulation.

In addition, the following rules apply for:

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, encrypt it by implementation-specific means, strictly using the cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)."

Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)".

Stored files: Files having sensitive data shall be protected against manipulation strictly using checksum or cryptographic methods as defined in NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)".

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.

2.6.9 Protection against Copy of Data

Requirement:
(applicable to CBC, Wi-Fi CPE (V1.0.1) and IP Router (V1.0.1) only; to be tested on any one of CBC, Wi-Fi CPE (V1.0.1) or IP Router (V1.0.1) of Group IV)
Group IV device shall have protection against creating a copy of data in use / data in transit. Protective measures should exist against use of available system functions / software residing in Group IV device to create copy of data for illegal transmission. The software functions, components in the Group IV device for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch and IP Router (V2.0.0) only; to be tested on any one of Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch or IP Router (V2.0.0) of Group IV)

The Group IV device shall have protection against creating a copy of data in use / data in transit. Protective measures shall exist against use of available system functions / software residing in Group IV device create copy of data for illegal transmission. The software functions, components in the Group IV device for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on of Network Next Generation Firewall including IDS & IPS of Group IV)

a) Without authentication& authorization and except for specified purposes, Next Generation Firewall shall not create a copy of data in use or data in transit.
b) Protective measures shall exist against use of available system functions / software residing in system to create copy of data for illegal transmission.

2.6.10 Protection against Data Exfiltration - Overt Channel

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) and IP Router (V1.0.1) only; to be tested on any one of Wi-Fi CPE (V1.0.1) or IP Router (V1.0.1) of Group IV)

Group IV Device shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound overt channels such as *FTP, HTTP*, HTTPS IM, P2P, Email etc. are to be forbidden if they are initiated by / originate from the Group IV Device. Outbound-use of such services are to be disabled in the Group IV Device, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

Requirement:
(applicable to CBC, L2 and (or) L3 LAN Switch, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS and Wi-Fi CPE (V2.0.0) only; to be tested on any one of CBC, L2

and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, IP Router (V2.0.0), or Wi-Fi CPE (V2.0.0) of Group IV)

a) Group IV device 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.

2.6.11 Protection against Data Exfiltration - Covert Channel

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

CPE shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are initiated by / originate from the CPE. Outbound-use of such services are to be disabled in the CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

Requirement:
(applicable to CBC, IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch including IDS & IPS, and Network Next Generation Firewall only; to be tested on any one of CBC, IP Router (V2.0.0), or Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch including IDS & IPS, or Network Next Generation Firewall of Group IV)

a) Group IV device 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 Group IV device.
c) Session logs shall be generated for establishment of any session initiated by either user or Group IV device.

Section 2.7: Network Services

2.7.1 Traffic Filtering - Network Level

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE shall provide a mechanism to filter incoming IP packets on any IP interface. It is preferable to configure Access Control List (ACL) as default deny-all on WAN port, with feature to enable the types of traffic permitted on user selection.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0), and Network Next Generation Firewall including IDS & IPS only; to be tested on any one of Wi-Fi CPE (V2.0.0), or Network Next Generation Firewall including IDS & IPS of Group IV)

The Group IV device shall provide a mechanism to filter incoming IP packets on any IP interface. In particular the Device shall provide a mechanism:

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

ii. To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
   - Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
   - Accept: the matching message is accepted.
   - Account: the matching message is accounted for i.e., a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

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

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

v. To reset the accounting.

vi. The Group IV device shall provide a mechanism to disable/enable each defined rule.

Note (Exclusive to Wi-Fi CPE (V2.0.0)): Applicable for both split configuration and cloud hosted/managed configuration. Access Points that are not capable of operating in standalone mode (i.e., require a controller for functionality) shall be exempted from this clause. However, the associated controller device, which is essential for the functioning of such Access Points, shall be tested for compliance with this clause.

[Ref (Wi-Fi CPE V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.6.2.1]

[Ref (Wi-Fi CPE V2.0.0): RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested on any one of IP Router (V1.0.1) of Group IV)

The Network product shall provide a mechanism to filter incoming IP packets on any IP interface.

In particular the Network product shall provide a mechanism:

(i). To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of

the stack ISO/OSI.

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

- Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
- Accept: the matching message is accepted.
- Account: the matching message is accounted for i.e., a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

(iii). To enable/disable for each rule the logging for Dropped packets, i.e., details on messages

matching the rule for troubleshooting.

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

(v). To reset the accounting.

(vi). The Network product shall provide a mechanism to disable/enable each defined rule.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.6.2.1]

Requirement:
(applicable to IP Router (V2.0.0), and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

The Group IV device shall provide a mechanism to filter incoming IP packets on any IP interface (Refer to RFC 3871). In particular, the L2 and (or) L3 LAN Switch 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) Group IV device shall provide a mechanism to disable/enable each defined rule.

[Ref: 1. TSDSI STD T1.3GPP 33.117-17.5.0V1.5.0 section 4.2.6.2.1 2.RFC 3871: Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

[Ref (IP Router V2.0.0): 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]

[Ref. L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.2.6.2.1

[Ref: RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2 Traffic Separation

Requirement:

(applicable to IP Router (V1.0.1), CBC, Wi-Fi CPE (V2.0.0) and PABX only; to be tested on any one of IP Router (V1.0.1), CBC, Wi-Fi CPE (V2.0.0) and PABX of Group IV)

[Exclusive to Wi-Fi CPE(V2.0.0): (applicable for both split configuration and cloud hosted/managed configuration)]

The Network product shall support physical or logical separation of O&M and control plane traffic. See RFC 3871 for further information.

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.5.1]

Requirement:

(applicable to IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch of Group IV)

The Group IV device 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. TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 section 4.3.5.1

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

[Ref. Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.5.1]

[Ref. L2 and (or) L3 LAN: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.5.1]

[Ref.: RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.3 Traffic Protection –Anti-Spoofing

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, Wi-Fi CPE (V2.0.0) *and CBC only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS,* Wi-Fi CPE (V2.0.0), *or CBC of Group IV)*

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.

Note (Applicable to Wi-Fi CPE V2.0.0): Applicable for any component system such as Controllers or any other management/provisioning entity which has layer 3 interfaces in use.

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.3.1.1]

[Reference (IP Router (V2.0.0)): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.3.1.1]

[Reference (CBC): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.3.1.1]

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 section 4.3.3.1.1]

Section 2.8: Attack Prevention Mechanism

2.8.1 Excessive Overload Protection

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The Group IV device may provide security measures to deal with overload situations

which may occur during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

Wi-Fi CPE shall act in a predictable way if an overload situation cannot be prevented. Wi Fi CPE shall be built in such a way that it can react to 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 a case it shall be ensured that Wi-Fi CPE 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. OEM shall provide a technical description of the Wi-Fi CPE 's overload control mechanisms. (especially whether these mechanisms rely on cooperation of other network elements)

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0. Section 4.2.3.3.3]

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

The system shall act in a predictable way if an overload situation cannot be prevented. A system 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 system 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 vendor shall provide a technical description of the network products' Overload Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements) and the accompanying test case for this requirement will check that the description provides sufficient detail in order for an evaluator to understand how the mechanism is designed.

Requirement:
(applicable to IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), or Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

The Group IV device shall act in a predictable way if an overload situation cannot be prevented. Group IV device 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 Group IV device 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 Group IV device Over Load Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements).

[Ref *IP Router (V2.0.0)*: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.3.3.3]
[Ref Network Next Generation Firewall including IDS & IPS: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.3]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.2.3.3.3]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

PABX shall act in a predictable way if an overload situation cannot be prevented. PABX 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 PABX cannot reach an undefined and thus potentially insecure state. In an extreme case, a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

CBC shall act in a predictable way if an overload situation cannot be prevented. CBC 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 CBC cannot reach an undefined and thus potentially insecure, state. In an extreme case, CBC shall continue to work in degraded mode with less traffic handling capacity but without loss of system security functions.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.3.3.3]

2.8.2 Filtering IP Options

(2.10.6 'Handling of IP options and extensions' is the clause title for Network Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch Switch)

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), *Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch* and CBC *only; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0),* IP Router (V1.0.1 & V2.0.0), *Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch* and CBC *of Group IV)*

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. OEMs may refer to standards such as RFC 6192, RFC 7126.

Note (Applicable to Wi-Fi CPE V2.0.0): Access Points that cannot operate in standalone mode (i.e., without a controller) shall be exempted from this clause. However, the controller device required for the operation of such Access Points shall be subject to evaluation under this clause.

[Reference (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.4.1.1.3]
[Reference (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.4.1.1.3]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section - 4.2.4.1.1.3]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section - 4.2.4.1.1.3]

2.8.3 Network Level and application-level DDoS

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

The system 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 include:

i. Restricting of available RAM per application
ii. Restricting of maximum sessions for a Web application
iii. Defining the maximum size of a dataset
iv. Restricting CPU resources per process
v. Prioritizing processes
vi. Limiting of amount or size of transactions of a user or from an IP address in a specific time range

Note: Network product should have protection mechanism against known network level and Application DDoS attacks

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.3.1]

Requirement:
(applicable to CBC, PABX, Network Next Generation Firewall including IDS & IPS, IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch only; to be tested on any one of CBC, PABX, Network Next Generation Firewall including IDS & IPS, Wi-Fi CPE (V2.0.0), or IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

Group IV device shall have protection mechanisms against Network-level and Application-level Distributed Denial of Service (DDoS) attacks. Group IV device 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 a user or from an IP address in a specific time range
g) Limiting amount or size of transactions to an IP address/Port Address in a specific time range

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.1]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V1.0.1.1.0. Section 4.2.3.3.1]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section 4.2.3.3.1]

2.8.4 Interface robustness requirements

Requirement:
(applicable to IP Router (V2.0.0) , Network Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0) or Network Next Generation Firewall including IDS & IPS or L2 and (or) L3 LAN Switch of Group IV)

The Group IV device shall be 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 the Group IV device. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.

a) Mass-produced TCP packets with a set 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 IPv4 packets (Ping-of-death attack).
f) Uncorrelated reply packets (i.e. packets which cannot be correlated to any request).

[Ref IP Router (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 section 4.2.6.2.2]

[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.6.2.2]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.2.6.2.2]

Section 2.9 Vulnerability Testing Requirements

2.9.1 Fuzzing - Network and Application Level

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), Network Next

Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, CBC and PABX; to be tested on any one of Wi-Fi CPE (V1.0.1 or V2.0.0), IP Router (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, CBC, or PABX of Group IV)

It shall be ensured that externally reachable services of Group IV device are reasonably robust when receiving unexpected input.

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

[Ref Wi-Fi CPE (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0. section 4.4.4]
[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.4]
[Reference (IP Router (V2.0.0)): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.4.4]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V1.0.1.1.0. section 4.4.4]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0. section 4.4.4]

2.9.2 Port Scanning

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) only; to be tested only on Wi-Fi CPE (V1.0.1 or V2.0.0) of Group IV)

It shall be ensured that on all network interfaces, only vendor documented/identified ports on the transport layer respond to requests from outside the system.

List of the identified open ports shall match the list of network services that are necessary for the operation of the CPE.

[Ref (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 section 4.4.2]

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), CBC, *Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch* and PABX *only; to be tested on any one of IP Router (V1.0.1 or V2.0.0),* CBC, *Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch,* or PABX *of Group IV)*

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

[Reference (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.2]
[Reference (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.4.2]
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.2]

[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.4.2]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:
(applicable to Wi-Fi CPE (V1.0.1), and IP Router (V1.0.1) only; to be tested on any one of Wi-Fi CPE (V1.0.1), or IP Router (V1.0.1) of Group IV)

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Group IV device, 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. OEM to provide self-test report establishing that no publicly known vulnerability exists.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

Requirement:
(applicable to Wi-Fi CPE (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, IP Router (V2.0.0) only; to be tested on any one of Wi-Fi CPE (V2.0.0), Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch or IP Router (V2.0.0) of Group IV)

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Network Product, 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 a year

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

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 section 4.4.3]
[Ref: https://nvd.nist.gov/vuln-metrics/cvss]
[Ref: GSMA NG 133 Cloud Infrastructure Reference Architecture]

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

It shall be ensured that no known critical/high/medium (as per CVE-IDs of NIST-NVD) vulnerabilities (as on date of offer of CBC to the designated TTSL for testing) shall exist in the CBC. For low/uncategorized (as per CVE-IDs of NIST-NVD) category vulnerabilities remediation plan is to be provided.

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

It shall be ensured that no known vulnerabilities (as on date of offer of PABX to designated TSTL for testing) shall exist in the PABX.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

2.9.4 SSID Scanning

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE shall not disclose sensitive information, PIN details on SSID scan / attack techniques. It needs to 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.

Section 2.10: Operating System

2.10.1 Handling of ICMP

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the CPE. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk. Refer standards such as RFC 6192, RFC 7279, RFC 4890.

Requirement:
(applicable to IP Router (V1.0.1), CBC, PABX, and Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V1.0.1), CBC, PABX, or Network Next Generation Firewall including IDS & IPS of Group IV)

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the Group IV device. 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 Group IV device 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	129	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	128	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	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

The Group IV device 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

Requirement:
(applicable to IP Router (V2.0.0), L2 and (or) L3 LAN Switch, and Wi-Fi CPE (V2.0.0) only; to be tested on any one of IP Router (V2.0.0), L2 and (or) L3 LAN Switch, or Wi-Fi CPE (V2.0.0) of Group IV)

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the Group IV device. 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 Group IV device 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	129	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	128	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	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

The Group IV device 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 request	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	Permitted	Permitted
N/A	134	Router Advertisement	N/A	N/A	Permitted

2.10.2 Growing Content Handling

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Growing or dynamic content (e.g., log files, uploads) shall not influence system functions. A file system that reaches its maximum capacity shall not stop a system from operating properly. Therefore, countermeasures shall be taken such as usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring to ensure that this scenario is avoided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.1.1]

Requirement:
(applicable to CBC, PABX, IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 LAN Switch only; to be tested on any one of CBC, PABX, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, or Wi-Fi CPE (V2.0.0) of Group IV)

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

[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.4.1.1.1]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section 4.2.4.1.1.1]

2.10.3 Authenticated Privilege Escalation only

('Privilege Escalation' is the clause name in Wi-Fi CPE (V1.0.1))

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), CBC, PABX, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), CBC, PABX, Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

Group IV device 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: TEC 64498:2024/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:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) and IP Router (V1.0.1) only; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0) or IP Router (V1.0.1) of Group IV)

Each system account in Operating system of the device shall have a unique identification, the OEM to provide information on implementation mechanism for this requirement.

[Ref (Wi-Fi CPE (V2.0.0)): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.4.2.2]
[Reference (IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.2.2]

Requirement:
(applicable to CBC, PABX, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 Lan Switch only; to be tested on any one of CBC, PABX, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 Lan Switch of Group IV)

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

[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.4.2.2]
[Ref L2 and (or) L3 Lan Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section 4.2.4.2.2]

2.10.5 OS-Hardening Kernel Security

("OS Hardening" clause name is applicable to CBC and PABX)
("OS Hardening - Minimized kernel network functions" clause name is applicable

to IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 LAN Switch)

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) and IP Router (V1.0.1) only; to be tested on any one of Wi-Fi CPE and IP Router (V1.0.1) of Group IV)

OEM/Vendor may 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 Group IV device are deactivated. OEM/Vendor to provide information on steps taken in this regard.

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.2]

Requirement:
(applicable to CBC and PABX only; to be tested on any one of CBC or PABX of Group IV)

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in Group IV device.

Kernel based network functions not needed for the operation of the Group IV device shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.2]

Requirement:
(applicable to Wi-Fi CPE (V2.0.0) only; to be tested only on Wi-Fi CPE (V2.0.0) of Group IV)

Kernel based network functions not needed for the operation of the network element shall be deactivated. In particular, the following ones shall be disabled by default:

a) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
b) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.,)
c) 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. d) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section - 4.3.3.1.2]

Requirement:
(applicable to Network Next Generation Firewall including IDS & IPS only; to be tested only on Network Next Generation Firewall including IDS & IPS of Group IV)

Kernel based network functions not needed for the operation of the Next Generation Firewall shall be deactivated. In particular the following ones shall be disabled by default:

1. IP Packet Forwarding between different interfaces of the network product.
2. Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
3. Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.,)
4. 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.
5. Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

[Ref (NGFW): TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section – 4.3.3.1.2]

Requirement:
(applicable to IP Router (V2.0.0) and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

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) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
b) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.)
c) 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.
d) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

[Ref (L2 and (Or) L3 LAN Switch): TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section - 4.3.3.1.2]
[Ref (IP Router (V2.0.0)): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section - 4.3.3.1.2]

2.10.6 Protection from buffer overflows

Requirement:
(applicable to IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2

and (or) L3 LAN Switch, Wi-Fi CPE (V1.0.1 & V2.0.0), CBC and PABX only; to be tested on any one of IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, Wi-Fi CPE (V1.0.1 & V2.0.0), CBC, or PABX of Group IV)

The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and how to check that they have been enabled and/or implemented shall be provided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.5]
[Ref (Wi-Fi CPE (V2.0.0)): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section - 4.3.3.1.5]
[Ref (IP Router (V2.0.0)): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section - 4.3.3.1.5]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section – 4.3.3.1.5]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section - 4.3.3.1.5]

2.10.7 External file system mount restrictions

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) and IP Router (V1.0.1) only; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0) or IP Router IP Router (V1.0.1) of Group IV)

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.6]
[Ref (Wi-Fi CPE (V2.0.0)): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section - 4.3.3.1.5]

Requirement:
(applicable to CBC, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch and PABX only; to be tested on any one of CBC, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch or PABX of Group IV)

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in the device 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 CBC and PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.6]

[Ref IP Router V2.0.0: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.3.1.6]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-

17.1.0 V.1.1.0. Section – 4.3.3.1.6]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section - 4.3.3.1.6]

2.10.8 No automatic launch of removable media

Requirement:
(applicable to IP router (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, Wi-Fi CPE (V2.0.0) only; to be tested on any one of IP router (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch or Wi-Fi CPE (V2.0.0) of Group IV)

The Group IV device shall not automatically launch any application when removable media device such as CD, DVD, 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.

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.3]
[Ref (IP Router (V2.0.0) & Wi-Fi CPE (V2.0.0)): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section - 4.3.3.1.3]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section – 4.3.3.1.3]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section - 4.3.3.1.3]

Requirement:
(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)

Group IV device shall not automatically launch any application when removable media device is connected.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.3]

2.10.9 File-system Authorization privileges

Requirement:
(applicable to IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, and PABX only; to be tested on any one of IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, or PABX of Group IV)

Group IV device 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.7]
[Ref (Wi-Fi CPE (V2.0.0)): TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section - 4.3.2.7]
[Ref (IP Router (V2.0.0)): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0

Section - 4.3.2.7]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section - 4.3.2.7]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section - 4.3.2.7]

2.10.10 Restrictions on running Scripts / Batch-processes

Requirement:
(applicable to IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), CBC, L2 and (or) L3 LAN Switch and Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), CBC, L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

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, Group IV Device shall have feature to restrict Scripts / Batch processes / 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.

2.10.11 SYN Flood Prevention

Requirement:
(applicable to IP Router (V2.0.0) and Wi-Fi CPE (V2.0.0) and Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch Group IV)

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

[Ref IP Router (V2.0.0) and Wi-Fi CPE (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section - 4.3.3.1.4]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section - 4.3.3.1.4]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section - 4.3.3.1.4]

2.10.12 Restrictions on Soft-Restart

Requirement:
(applicable to IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

Group IV device 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 Interface

This entire section of the security requirements is applicable if the Group IV device supports web management interface.

2.11.1 HTTPS

('HTTPS Support' is the clause name for Wi-Fi CPE (V1.0.1 & V2.0.0))

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

The communication between Web client and Web server shall be protected using industry standard secured communication protocols such as TLS/HTTPS. Cipher suites with NULL encryption shall not be supported.

[Ref IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.1]

Requirement:
(applicable to CBC, IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS and PABX only; to be tested on any one of CBC, IP Router (V2.0.0), Wi-Fi CPE (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch and PABX of Group IV)

The communication between Group IV Device web client and web server shall be protected strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Ref CBC and PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.5.1]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.5.1]
[Ref IP Router (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.5.1]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.5.0 section 4.2.5.1
[Ref Wi-Fi CPE (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0. section 4.2.5.1]

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The communication between Web client and Web server to be protected using industry standard secured communication protocols TLS/HTTPS. Cipher suites with NULL encryption shall not be supported. CPE to be protected against sniffing and side jacking

attacks.

2.11.2 Webserver logging

('Logging' is the clause name for Wi-Fi CPE (V1.0.1 & 2.0.0))

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0), CBC, L2 and (or) L3 LAN Switch, IP Router (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS and PABX; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0), CBC, L2 and (or) L3 LAN Switch, IP Router (V1.0.1 & V2.0.0) , Network Next Generation Firewall including IDS & IPS, PABX of Group IV)

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

- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.
- Status code of web server response

[Ref CBC, Network Next Generation Firewall including IDS & IPS, IP Router (V1.0.1) and PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.2.1]
[Ref IP Router (V2.0.0) and Wi-Fi CPR (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.5.2.1]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.2.5.2.1]
[Ref: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.2.5.2]

2.11.3 HTTP User sessions

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, and Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, or Network Next Generation Firewall including IDS & IPS of Group IV)

To protect user sessions the Group IV device shall support the following session ID and session cookie:

i. The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
ii. The session ID shall be unpredictable.
iii. The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
iv. In addition to the Session Idle Timeout (see clause 2.2.5 Inactive Session Timeout), the Group IV device shall automatically terminate 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.

v. Session IDs shall be regenerated for each new session (e.g. each time a user logs-in)
vi. The session ID shall not be reused or renewed in subsequent sessions.
vii. The Group IV device 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.
viii. Where session cookies are used the attribute 'Http Only' shall be set to true.
ix. Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
x. 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.
xi. The Group IV device shall not accept session identifiers from GET/POST variables.
xii. The Group IV device shall be configured to only accept server generate session IDs.

[Reference IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.3]
[Ref IP Router (V2.0.0)/Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.5.3]
[Ref [NGFW]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.5.3]
[Ref [L2 and (or) L3 LAN Switch]: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.2.5.3]

Requirement
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) only; to be tested only on Wi-Fi CPE (V1.0.1 & V2.0.0) of Group IV)

i. The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
ii. The session ID shall be unpredictable.
iii. The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
iv. In addition to the Session Idle Time out.
v. Session IDs shall be regenerated for each new session (e.g. each time a user logs in).
vi. The session ID shall not be reused or renewed in subsequent sessions.
vii. The Wi-Fi CPE shall not use persistent cookies to manage sessions but only session cookies.
viii. Where session cookies are used the attribute 'Http Only' shall be set to true.
ix. Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
x. Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.
xi. The Wi-Fi CPE shall not accept session identifiers from GET/POST variables.
xii. The Wi-Fi CPE shall be configured to only accept server generate session ID's.

2.11.4 HTTP input validation

('HTTPS input validation' is the clause name in CBC and Network Next Generation Firewall including IDS & IPS)

Requirement:
(applicable to CBC, Network Next Generation Firewall including IDS & IPS, PABX, Wi-Fi CPE (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch and IP Router (V1.0.1 & V2.0.0); to be tested on any one of CBC, Network Next Generation Firewall including IDS & IPS, PABX, Wi-Fi CPE (V1.0.1 & V2.0.0), or IP Router (V1.0.1 & V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

The Group IV device shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks. The Group IV device 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.

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.4]
[Ref (IP Router (V2.0.0)/Wi-Fi CPE (V2.0.0)): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.2.5.4]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.2.5.4]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.5.4]
[Reference CBC, PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.4]

2.11.5 No unused HTTP methods

('No unused HTTPS methods' is the clause name in CBC, PABX and Network Next Generation Firewall including IDS & IPS)

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) and IP Router (V1.0.1) only; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0) and IP Router (V1.0.1) of Group IV)

HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.3]
[Reference (Wi-Fi CPE (V2.0.0)): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0 section 4.3.4.3]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.3]

Requirement:
(applicable to IP Router (V2.0.0), CBC, PABX, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V2.0.0), CBC, PABX, Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

HTTPS methods that are not required for Group IV device operation shall be deactivated.

[Ref CBC, PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.3]
[Ref Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, PABX and L2 and (or) L3 LAN Switch; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, PABX, or L2 and (or) L3 LAN Switch of Group IV)

All optional add-ons and components of the web server shall be deactivated if they are not required for Group IV device 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.

[Reference (IP Router (V1.0.1)): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.4]
[Ref (IP Router (V2.0.0)/Wi-Fi CPE (V2.0.0)): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.4]
[Reference CBC, PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.4]
[Ref Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.4]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.4]

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

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, and PABX only; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1 & V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, or PABX of Group IV)

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 (e.g., PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).

[Reference IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.5]

[Ref IP Router (V2.0.0)/Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.5]

[Ref CBC, PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.5]

[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.5]

2.11.8 No CGI or other Scripting for uploads

Requirement:
(applicable to CBC, IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS, PABX and L2 and (or) L3 LAN Switch; to be tested on any one of CBC, Network Next Generation Firewall including IDS & IPS, PABX, IP Router (V1.0.1 &V2.0.0), Wi-Fi CPE (V1.0.1 & V2.0.0) and L2 and (or) L3 LAN Switch of Group IV)

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

[Ref CBC, PABX, IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.6]
[Ref Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.6]
[Ref IP Router (V2.0.0), Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.6]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.6]

2.11.9 No execution of system Commands with SSI

Requirement:
(applicable to CBC, IP Router (V1.0.1 & V2.0.0), Wi-Fi (V1.0.1 & V2.0.0), PABX, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch; to be tested on any one of CBC, IP Router (V1.0.1 & V2.0.0), Wi-Fi (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS, PABX, or L2 and (or) L3 LAN Switch of Group IV)

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

[Reference CBC, IP Router (V1.0.1), PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.7]
[Ref IP Router (V2.0.0)/Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.7]
[Next Generation Firewall including IDS & IPS is Referred from TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.7]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.7]

2.11.10 No Default Content

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Wi-Fi (V1.0.1 & V2.0.0), CBC, PBX, Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 LAN Switch; to be tested on any one of IP Router (V1.0.1 & V2.0.0), Wi-Fi (V1.0.1 & V2.0.0), CBC, PBX, Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

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

[Reference CBC, IP Router (V1.0.1), PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.9]
[Ref IP Router (V2.0.0)/Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.9]
[Next Generation Firewall including IDS & IPS is Referred from TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.7]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.9]

2.11.11 No Directory Listing

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Wi-Fi (V1.0.1 & V2.0.0), CBC, PBX, Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 LAN Switch; to be tested on any one of IP Router (V1.0.1 & V2.0.0), Wi-Fi (V1.0.1 & V2.0.0), CBC, PBX, Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

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

[Reference IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.10]
[Ref IP Router (V2.0.0)/Wi-Fi (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.10]
[Next Generation Firewall including IDS & IPS is Referred from TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.7]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.10]

2.11.12 Web Server Information in HTTP headers

('Information in HTTP Headers' is the clause name in Wi-Fi CPE (V1.0.1 & V2.0.0)
('Web Server Information in HTTPS headers' is the clause name in CBC, Network Next Generation Firewall including IDS & IPS, PABX)

Requirement:

(applicable to IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Wi-Fi CPE (V1.0.1 & V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS and PABX; to be tested on any one of IP Router (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Wi-Fi CPE (V1.0.1 & V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, or PABX of Group IV)

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

[Ref (IP Router V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.11]
[Ref (IP Router V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.11]
[Ref: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.11]
[Ref Wi-Fi CPE (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0

section 4.3.4.11]
[Ref CBC and PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.11]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.11]

2.11.13 Web Server Information in Error Page

('Information in Error Page' is the clause name for Wi-Fi CPE (V1.0.1 & V2.0.0)

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V1.0.1 & V2.0.0), CBC, *Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch,* and PABX*; to be tested on any one of IP Router (V1.0.1 or V2.0.0), Wi-Fi CPE (V1.0.1 & V2.0.0),* CBC, *Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch,* or PABX *of Group IV)*

User-defined error pages shall not include version information about the 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 web server shall be replaced by error pages defined by the vendor/OEM.

[Reference IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.12]
[Ref IP Router (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.12]
[Ref CBC and PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.12]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.11]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.12]
[Ref Wi-Fi CPE (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 section 4.3.4.12]

2.11.14 No system privileges

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch and Wi-Fi CPE (V2.0.0) only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, or Wi-Fi CPE (V2.0.0) of Group IV)

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 IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]
[Ref IP Router (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.2]
[Ref Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.2]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-

17.1.0 V.1.1.0. section 4.3.4.2]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.2]

Requirement:
(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)

No device web server processes shall run with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]

2.11.15 Access rights for web server configuration

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V2.0.0), CBC, PABX, Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V2.0.0), CBC, PABX, Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

Access rights for Group IV device 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.

[Ref IP Router (V1.0.1), CBC, PABX: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.8]
[Ref IP Router (V2.0.0), Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0 section 4.3.4.8]
[Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.8]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.8]

2.11.16 Minimized file type mappings

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V2.0.0), CBC, *Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch* and PABX *only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V2.0.0),* CBC, *Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch,* or PABX *of Group IV)*

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

[Ref IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]
[Ref IP Router (V2.0.0) and Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0.

section 4.3.4.13]
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]
[Ref Network Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.13]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.5.0 section 4.3.4.13]

2.11.17 Restricted file access

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, and PABX only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, or PABX of Group IV)

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

[Reference IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.14]
[Ref IP Router (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0 section 4.3.4.14]
[Ref Wi-Fi CPE (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 section 4.3.4.14]
[Ref [Network Next Generation Firewall including IDS & IPS]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.14]
[Ref [L2 and (or) L3 LAN Switch]: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 section 4.3.4.14]

2.11.18 Execute rights exclusive for CGI/Scripting directory

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V2.0.0), CBC, PABX, L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V1.0.1 & V2.0.0) and Wi-Fi CPE (V2.0.0), CBC, PABX or L2 and (or) L3 LAN Switch of Group IV)

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

[Reference (IP Router (V1.0.1), PABX and CBC): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.15]
[Ref (IP Router (V2.0.0)): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.15]
[Ref (Wi-Fi CPE (V2.0.0)): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.15]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0. section 4.3.4.15]

Section 2.12: Other Security Requirement

2.12.1 Remote Diagnostic Procedure - Verification

Requirement:
(applicable to IP Router (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, PABX and Wi-Fi CPE (V2.0.0) only; to be tested on any one of IP Router (V2.0.0), CBC, Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, PABX and Wi-Fi CPE (V2.0.0) of Group IV)

If the Group IV device 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 with the following parameters:

1. User id
2. Time stamp
3. Interface type
4. Event level (e.g. CRITICAL, MAJOR, MINOR)
5. Command/activity performed and
6. Result type (e.g. SUCCESS, FAILURE).
7. IP Address of remote machine

[Ref IP Router (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.15]
[Ref Wi-Fi CPE (V2.0.0): TSDSI STD T1.3GPP 33.117-17.2.0 V.1.0.0. section 4.3.4.15]
[Ref [Network Next Generation Firewall including IDS & IPS]: GSMA 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack, section:2.2.7.7]
[Ref L2 and (or) L3 LAN Switch: GSMA NG 133: GSM Association Non-confidential Official Document NG.133

Requirement:
(applicable to IP Router (V1.0.1), Wi-Fi CPE (V1.0.1) only; to be tested on any one of IP Router (V1.0.1), or Wi-Fi CPE (V1.0.1) of Group IV)

If the Network product is providing Remote access for troubleshooting purposes/alarm maintenance, then it should be allowed only for authorized users and all activities performed by the remote user is to be logged with parameters like User id, time stamp, interface type, event level (e.g. CRITICAL, MAJOR, MINOR), result type (e.g. SUCCESS, FAILURE).

[Reference IP Router (V1.0.1): TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.6]

2.12.2 No System Password Recovery

('No Password Recovery' is the clause name for Wi-Fi CPE (V1.0.1), PABX and IP Router (V1.0.1))
('No System/Root Password Recovery' is the clause name for CBC)

Requirement:
(applicable to IP Router (V1.0.1) and Wi-Fi CPE (V1.0.1) only; to be tested on any one of IP

Router (V1.0.1) and Wi-Fi CPE (V1.0.1) of Group IV)

Network devices have a function that resets the current system password. In the event of system password reset, the entire configuration of the Network product shall be irretrievably deleted. No provision should exist for password recovery.

Requirement:
(applicable to PABX, Wi-Fi CPE (V2.0.0), IP Router (V2.0.0), and L2 and (or) L3 LAN Switch only; to be tested on any one of PABX, Wi-Fi CPE (V2.0.0), or IP Router (V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

In the event of system password reset, the entire configuration of the Group IV device shall be irretrievably deleted. No provision shall exist for password recovery.

Requirement:
(applicable to CBC, Network Next Generation Firewall including IDS & IPS; to be tested on any one of CBC, or Network Next Generation Firewall including IDS & IPS of Group IV)

No provision shall exist for firewall System / Root password recovery in the Group IV device.

2.12.3 Secure System Software Revocation

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

Once the software image is legally updated, it should not be possible to roll back to a previous exploitable software image. In case roll back is essential, it shall be done only by the administrator. Group IV device shall support a well-established control mechanism for rolling back to previous exploitable software image.

Requirement:
(applicable to CBC, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch and Wi-Fi CPE (V2.0.0) only; to be tested on any one of CBC, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, or Wi-Fi CPE (V2.0.0) of Group IV)

Once the Group IV device 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.
Group IV device shall support a well-established control mechanism for rolling back to previous software image.

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

Once the PABX software image is legally updated/upgraded with new software image, it shall 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. PABX shall support a well-established control mechanism for rolling back to previous software image. Whosoever is performing roll-back, the privilege rights, all the activities, commands, etc should be logged in.

2.12.4 Software Integrity Check - Installation

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) and IP router (V1.0.1) only; to be tested on any one of Wi-Fi CPE (V1.0.1), or IP Router (V1.0.1) of Group IV)

Group IV device should validate the software package integrity before the installation/ upgrade. Tampered software shall not be executed or installed if integrity check fails.

Requirement:
(applicable to CBC, PABX, IP Router (V2.0.0), Next Generation Firewall including IDS & IPS and L2 and (or) L3 LAN Switch only; to be tested on any one of CBC, PABX, IP Router (V2.0.0), Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

Group IV device 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: TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]
[Ref Next Generation Firewall including IDS & IPS: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.3.5]
[Ref L2 and (or) L3 LAN Switch: TSDSI STD T1.3GPP 33.117-17.5.0V1.0.1.5.0 Section 4.2.3.3.5]

2.12.5 Software Integrity Check - Boot

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0), IP Router (V1.0.1) only; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0), or IP Router (V1.0.1) of Group IV)

The CPE shall verify the integrity of a software component at the time of boot / re-boot typically by comparing the result of a measurement (typically a cryptographic hash / CRC) of the component to the expected reference value.

Requirement:
(applicable to PABX, IP Router (V2.0.0), Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch and CBC only; to be tested on any one of PABX, IP Router (V2.0.0), Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch, or CBC of Group IV)

The Group IV device 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 Interfaces Disabling

Requirement:
(applicable to IP Router (V1.0.1) only; to be tested only on IP Router (V1.0.1) of Group IV)

The device shall support the mechanism to verify all the physically accessible interfaces. Physically accessible Interfaces which are not under use shall be disabled by configuration that they remain inactive even in the event of a reboot.

Note: List of the default used Physical Interfaces/Ports as given by the vendor shall match the list of Physical Interfaces/Ports that are necessary for the operation of the Network product.

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

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

2.12.7 Unused Physical and Logical Interfaces Disabling

Requirement:
(applicable to CBC, PABX, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, and L2 and (or) L3 LAN Switch only; to be tested on any one of CBC, PABX, IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, or L2 and (or) L3 LAN Switch of Group IV)

Group IV device 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 Group IV device.

Requirement:
(applicable to Wi-Fi CPE (V1.0.1) only; to be tested only on Wi-Fi CPE (V1.0.1) of Group IV)

The CPE 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.

[Ref: Ltr no. NCCS/SAS/ITSAR-Amendments/2024-25/2 Dated at Bangalore, the

24.10.2024; A7]

2.12.8 No Default Profile

('Predefined accounts shall be deleted or disabled' is the clause name for IP Router (V2.0.0), Network Next Generation Firewall including IDS & IPS, L2 and (or) L3 LAN Switch)

Requirement:
(applicable to Wi-Fi CPE (V1.0.1 & V2.0.0) and IP Router (V1.0.1) only; to be tested on any one of Wi-Fi CPE (V1.0.1 & V2.0.0) and IP Router (V1.0.1) of Group IV)

Predefined or default user accounts shall be deleted or disabled. Default accounts such as guest, master are generally preconfigured with known or nil authentication attribute and therefore such standard users shall be deleted or disabled.

[Ref Wi-Fi CPE (V2.0.0): TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.0.1.2.0 Section 4.2.3.4.2.2]

Requirement:
(applicable to CBC, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS only; to be tested on any one of CBC, IP Router (V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS of Group IV)

Predefined or default user accounts (other than Admin/Root) in Group IV device shall be deleted or disabled.

[Ref TEC 64498:2024/TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.2.2]

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

Predefined or default user accounts in PABX shall be deleted or disabled.

2.12.9 Security Algorithm Modification

('Security Algorithm/Protocol Downgrade attack' is the clause name for CBC)

Requirement:
(applicable to IP Router (V1.0.1 & V2.0.0) and L2 and (or) L3 LAN Switch only; to be tested on any one of IP Router (V1.0.1 & V2.0.0), or L2 and (or) L3 LAN Switch of Group IV)

When Group IV device is establishing session/ communication channel with other Group IV device or while communication in the progress, Group IV device shall have protection against a downgrade attack/bidding down attack for the use of a weaker algorithm.

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

It shall not be possible to modify security algorithms supported by PABX.

Requirement:
(applicable to CBC only; to be tested only on CBC of Group IV)

It shall not be possible to downgrade security algorithms/protocols supported by CBC to those not listed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0"

2.12.10 Management Interface Isolation

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

PABX shall support management software usage/critical command execution only through a dedicated management interface.

2.12.11 External Alert Generation

Requirement:
(applicable to PABX only; to be tested only on PABX of Group IV)

PABX shall support configuring the thresholds for system parameter values such as memory, hard disk space, CPU load and it shall generate an external alert when these system parameter values exceed their defined thresholds.

2.12.12 Secure VPN connection

Requirement
(applicable to PABX only; to be tested only on PABX of Group IV)

PABX shall establish VPN connections with its peers strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

2.12.13 Control Plane Traffic Protection

Requirement:
(applicable to IP Router (V1.0.1), and Network Next Generation Firewall including IDS & IPS only; to be tested on any one of IP Router (V1.0.1), or Network Next Generation Firewall including IDS & IPS of Group IV)

Control plane traffic shall be protected in the Next General Firewall using standard cryptographic mechanisms i.e., by using the industry standard cryptographic secure protocols such as TLS, IPSec, etc.

Annexure I

Acronym	Expansion
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ACS	Auto-Configuration Server
AES	Advanced Encryption Standard
BGP	Border Gateway Protocol
CBC	Cell Broadcast Centre
CERT	Computer Emergency Response Team
CPE	Customer Premises Equipment
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DoS	Denial of Service
EMS	Element Management System
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ITSAR	Indian Telecom Security Assurance Requirements
L2/L3	Layer 2 / Layer 3
LAN	Local Area Network
MAC	Message Authentication Code
MTCTE	Mandatory Testing and Certification of Telecom Equipment
NCCS	National Centre for Communication Security
NG Firewall	Next Generation Firewall (including IDS & IPS)
NIST	National Institute of Standards and Technology
NMS	Network Management System
NTP	Network Time Protocol
OAM	Operations, Administration and Maintenance
OS	Operating System
OSPF	Open Shortest Path First
PABX	Private Automatic Branch Exchange
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RFC	Request for Comments

Acronym	Expansion
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TSDSI	Telecommunications Standards Development Society, India
TSTL	Telecom Security Testing Laboratory
TLS	Transport Layer Security
VPN	Virtual Private Network

Annexure-II

List of Submissions

The following undertakings / declarations / documents must be furnished by the OEM/Vendor for Group-IV device CSR testing (as applicable to the specific device under test). These support verification of key clauses and align with standard NCCS requirements for Group ITSARs.

1. **Source Code Security Assurance** (clause 2.3.3) – Undertaking confirming adherence to secure coding practices and absence of intentional backdoors or hidden functionalities.
2. **Known Malware and Backdoor Check** (clause 2.3.4) – Declaration or independent scan report (e.g., using approved tools) confirming no known malware, trojans, or backdoors.
3. **No Unused Software / Components** (clauses 2.3.5 and 2.4.2) – Complete list of all installed software/components with justification for each; undertaking that all unused items have been removed or disabled.
4. **Avoidance of Unspecified Wireless Access** (clause 2.3.11) – Declaration that no undocumented or unspecified wireless interfaces (e.g., hidden Wi-Fi, Bluetooth) exist in the device.
5. **No Unsupported Components** (clause 2.4.2) – List of all hardware and software components, including end-of-support / end-of-life status and mitigation plans where applicable.
6. **Cryptographic Module Security Assurance** (clause 2.6.3) – FIPS 140-2/140-3 (or equivalent) validation report or self-declaration for cryptographic modules, along with confirmation of compliance with Table 1 of the latest "ITSAR for Cryptographic Controls" (ITSAR001962411 V2.0.0).
7. **Cryptographic Algorithms Implementation Security Assurance** (clause 2.6.4) – Undertaking that only algorithms and key lengths from Table 1 of the latest "Indian Telecom Security Assurance Requirements (ITSAR) for Cryptographic Controls" are implemented.
8. **OS-Hardening Kernel Security** (clauses 2.10.5) – Detailed OS hardening report or configuration checklist demonstrating deactivation of unnecessary kernel functions and network services.

9. **Software Integrity Check Mechanisms** (clauses 2.12.4 – 2.12.5) – Description and evidence of boot-time and installation-time integrity verification mechanisms (e.g., cryptographic hash comparison using approved algorithms).
10. **Buffer Overflow Protection** (clause 2.10.6) – Documentation of implemented mechanisms (e.g., ASLR, stack canaries, NX bit, DEP) and instructions on how to verify they are enabled and effective.
11. **Additional Device-Specific Submissions** (as applicable for Wi-Fi CPE, IP Router, NG Firewall, L2/L3 LAN Switch, etc.) – Evidence for RBAC implementation, ICMP handling, web interface hardening, and any API/OAuth-related controls (especially for Wi-Fi CPE V1.0.1 clauses in 2.12.14–2.12.24).

OEMs must submit these in a consolidated dossier during testing. NCCS/TSTL may request additional evidence or on-site verification.

Annexure-III

References

1. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 – Catalogue of General Security Assurance Requirements.
2. TSDSI STD T1.3GPP 33.117-17.2.0 V.1.2.0 (and related versions for V2.0.0 devices) – Updates for specific Group-IV equipment (e.g., IP Router, Wi-Fi CPE).
3. TSDSI STD T1.3GPP 33.117-17.5.0 V1.5.0 – Requirements for L2 and/or L3 LAN Switch.
4. TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0 (and related) – Requirements for Network Next Generation Firewall including IDS & IPS.
5. ITSAR001962411 V2.0.0 dated 21.11.2024 – Indian Telecom Security Assurance Requirements (ITSAR) for Cryptographic Controls (effective from 01.01.2026; all references to "latest document 'ITSAR for Cryptographic Controls'" or equivalent point to this).
6. TEC 64498:2024 – Technical specifications for Wi-Fi CPE V2.0.0 and IP Router V2.0.0.
7. GSMA NG.133 – Cloud Infrastructure Reference Architecture (referenced for NG Firewall management and remote access logging).
8. RFC 6192, RFC 7126, RFC 7279, RFC 4890 – Security guidelines for network devices (ICMP handling, IP options/extensions, etc.).
9. NIST National Vulnerability Database (NVD) – For CVE assessment, CVSS scoring, and remediation timelines.
10. CIS Benchmarks – Password policy and system hardening guidelines

(referenced in authentication and OS sections).

11. Office Memorandum NCCS/SAS/6-1/2024-25 dated 02.01.2025 – Expanding the scope of CSR testing for Group-IV devices.
12. NCCS/SAS/ITSAR-Amendments/2024-25 letters (various dates in Oct 2024) – Specific amendments for Wi-Fi CPE and other Group-IV clarifications.