सत्यमेव जयते

Indian Telecommunication Security Assurance Requirements (ITSAR)

Network Function Virtualization (NFV)

(As applicable to Mobile Generation Technologies)

NCCS
Securing Networks

Draft for comments

Release Date: Version: 1.0.0
Enforcement Date:

Security Assurance Standards Facility
National Centre For Communication Security
Department of Telecommunications, Bengaluru-560027

About NCCS

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

Document History

Sl. No	ITSAR Reference	Title	Remarks
1			

Contents

A) Outline: iv

B) Scope: v

C) Conventions v

Chapter 1 – Overview 1

Chapter 2 – Common Security Requirements 8

Chapter 3 Specific Security Requirements 49

Part I NFV Infrastructure 49

Part II Virtualization Security 79

Part II (A)Virtual Machine 115

Part II (B) Container 130

Part III-SDN 147

Part IV MANO 152

Annexure-I (Definition) 164

Annexure-II(Acronyms) 168

Annexure-III(List of Submissions) 170

Annexure-IV (References) 171

A) Outline:

The objective of this document is to present a comprehensive country specific security requirement for the Network Function Virtualization (NFV) as applicable to the mobile generation technologies. NFV allows for the network functions developed by various vendors to run on commercially off the shelf hardware (COTS) servers by using virtualization technologies. While the introduction of NFV in the mobile network has benefits of savings on OPEX/CAPEX and automation gain, the virtualization technologies, and the underpinning COTS hardware present new challenges to network security in realizing the network functions.

The specifications produced by various regional/ international standardization bodies viz 3GPP, ITU-T, ISO, ETSI, IEEE, IETF, TSDSI along with the publications of ENISA, NIST, CISA NGMN, GSMA are the basis for the preparation of this document. The references indicated against each of the clauses imply that the respective clause has been adopted as it is or with certain modifications.

This document commences with a brief description of Network Function Virtualization (NFV) and then proceeds to address the security requirements of various facets of NFV.

B) Scope:

This document targets on the security requirements of the various facets of the Network Function Virtualization (NFV) as applicable to mobile generational technologies. The document specifies the security requirements related to NFV Infrastructure (Platform), Virtual Network Functions (both container and Virtual Machine based), Management and Network Orchestration (MANO) and Software Defined Networking (SDN) as defined in ETSI NFV reference framework . This document does not cover the security requirements of Multi Access Edge Computing (MEC).

The regulations regarding Remote Access and Lawful Interceptions are not part of this ITSAR. The requirements specified here are binding both on operators (aka Telecommunication Service Provider- TSP), Network Equipment providers (aka OEMs-Original Equipment Manufacturer) and Cloud Service Providers as per their roles.

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. Shall or Recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Shall not or not Recommended denotes the opposite meaning of (3) above.

Chapter 1 – Overview

Introduction: Traditionally, Network Functions have been bundled into bespoke hardware appliances. In contrast, network function virtualization is the deployment of these services as software modules that run on common off-the-shelf generic hardware over a hypervisor or container that controls access to hardware devices. In principle all network functions and nodes may be considered for virtualization. The greatest impetus for the NFV came from 3GPP when it proposed Service Based Architecture (SBA)for realization of 5G Core.

NFV provides the following benefits

1) OPEX and CAPEX savings due to the use of commodity hardware, the ability to share computing resources between functions, reduced energy consumption etc.
2) The operators can use the introduction of virtualized networking and cloud technologies to adopt tools similar to those used by IT industry to automate many aspects of operations and managements. This will enable operators to shorten time to market of new services and scaling of resources as per the dynamic demands.

1. NFV Technologies: The key technology used in the NFV is virtualization**.** Virtualization can be Hypervisor based or container based.

i) Hypervisor based: Hypervisor-based virtualization provides isolated environments on top of a shared pool of resources. Hypervisor is a software layer that abstracts the underlying physical resources and provides virtual machines (VM) with the full functionalities of a real system. The hypervisor is responsible for resource allocation to the VM as well as being responsible for monitoring and managing VMs through coordination with the primary OS of the underlying hardware.

There are two types of hypervisors known as Type 1 and Type 2. Pl refer Fig 1.

Type-1 Hypervisor: Also known as Bare-metal Hypervisor, it runs directly on the host machine's physical hardware. It does not need an underlying host OS because the communication to hardware resources is direct with full visibility of hardware resources.

Type-2 Hypervisor: A Type-2 hypervisor is typically installed on top of an existing OS. It is sometimes called a hosted hypervisor because it relies on the host machine's pre-existing OS to manage allocation of CPU, memory, storage, and network resources to the VM.

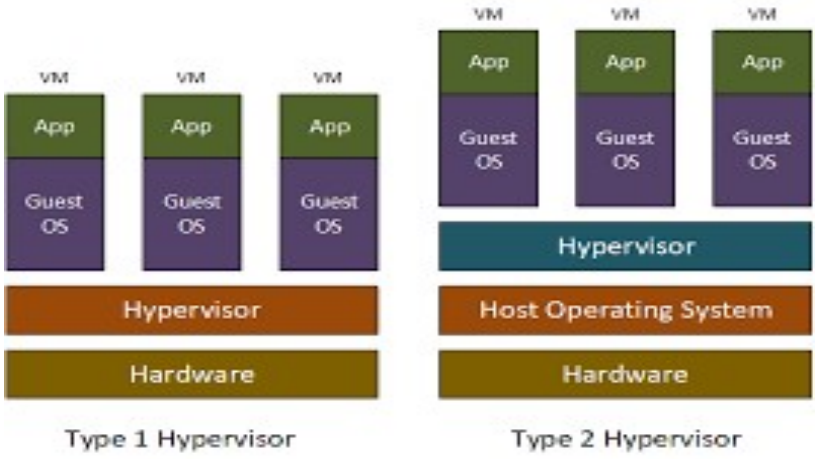

Fig 1 Type 1 and Type 2 Hypervisors

Virtual Machine (VM): A virtual machine (VM) is a type of virtualization that splits bare metal servers into numerous independent instances, each of which has its own operating system. The operating system, applications and services are all bundled into a single image that is accessed via a hypervisor, built on virtualized hardware.
A VM consists of several files that are stored on a storage device. The key files are the configuration file, virtual disk file, NVRAM setting file and log file.

ii) OS level Virtualization: OS-level virtualization represents the containerization model, which envisages that only the applications and their dependencies are integrated into a container. Each container shares the host OS kernel operating on bare metal, as well as its binaries and libraries so the applications run quickly and reliably from one computing environment to another. Containerized network function is best suited for cloud native environment and hence also called as Cloud native Network Function (CNF)

iii) Hybrid virtualization: It is the mixture of both VMs and Containers.

The Software Defined Networking (SDN) is the complementary technology which will benefit NFV implementation. The core similarity between software-defined networking (SDN) and network functions virtualization (NFV) is that they both use network abstraction. SDN seeks to separate network control functions from network forwarding functions, while NFV seeks to abstract network forwarding and other networking functions from the hardware on which it runs. SDN has three components viz. SDN application layer, SDN Control Layer and SDN infrastructure layer/Resource layer. Fig 2 below shows the concept of SDN.

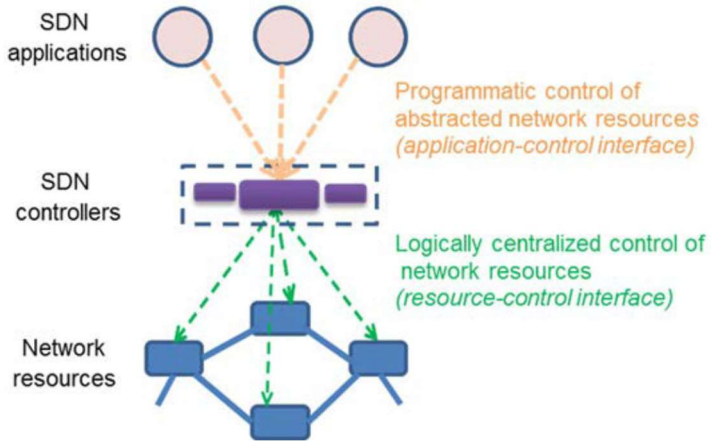

Fig 2 Concept of SDN

When SDN executes on an NFV infrastructure, SDN forwards data packets from one network device to another. At the same time, SDN's networking control functions for routing, policy definition and applications run in a VM or container somewhere on the network. Thus, NFV provides basic networking functions, while SDN controls and orchestrates them for specific uses. SDN further allows configuration and behavior to be programmatically defined and modified.

SDN can be incorporated in the NFV framework by positioning SDN resources and SDN controllers in different ways.

2. NFV Architectural Framework: The NFV architectural framework has been developed to standardize the NFV components and their service interfaces so as to ensure compatibility between different vendor implementations. ETSI has developed the NFV framework, the high level view of which is shown in Fig 3. ETSI identified three working domains in the NFV architecture.

1. **Virtual Network Functions (VNF)** - software implementation of network function that runs over a NFVI.
2. **NFV Infrastructure (NFVI)** - this includes the physical resources and how these can be virtualized. NFVI supports the execution of the VNFs.
3. **NFV Management and Orchestration (MANO)** - it includes the orchestration and lifecycle management of the physical resources and/or the software resources that support the virtualisation of the infrastrucure and the life cyle management of VNFs. MANO comprises of the Virtualized Infrastructure Manager (VIM), Virtualized Network Function Manager (VNFM) and NFV Orchestrator (NFVO).

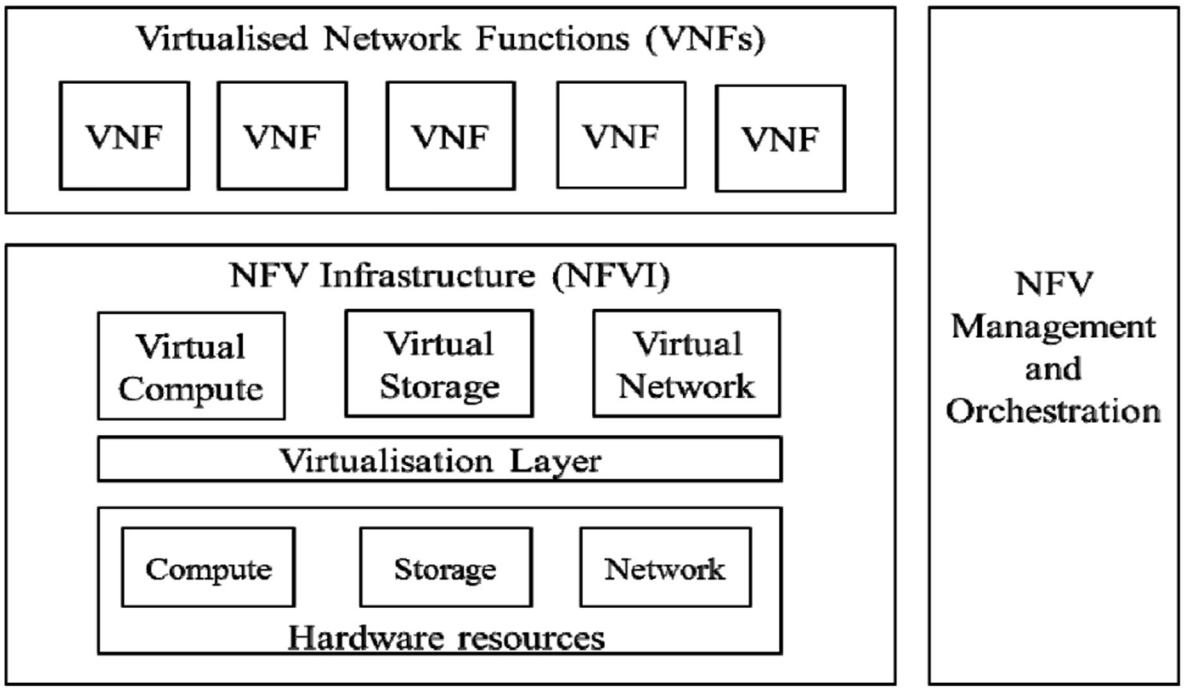

Figure 3 High level NFV Framework

The initial release of the ETSI NFV specification was predominantly dependent on hypervisor-based virtual machines (VMs) for virtualization. After the introduction of cloud native NFV, an adaptation is made in some areas as shown in the Fig 4. The cloud native here indicates the various micro services implemented as Container to realize a network services. The components of this architecture are

1. **NFV Infrastructure (NFVI):** The NFVI consists of all the hardware and software components that are contained within the environment in which VNFs are deployed. It provides virtualized computing, storage, and networking.
2. **OSS/BSS** - Operation Support System and Business Support System of the operator.
3. **Element Management System (EMS)**: It is responsible for the configuration, fault management, accounting, and collection of performance measurement results for the network functions provided by the VNF.
4. **Hardware Resources:** In NFV, the physical hardware resources include computing, storage and networks that provide processing, storage, and connectivity to VNFs through the virtualization layer (Host OS, Hypervisor, CIS).
5. **Virtualized Network Function (VNF):** An implementation of an NF that can be deployed on a network function virtualization infrastructure (NFVI). VNFs are built from one or more VNF components (VNFC).
6. **Virtualized Network Function Component (VNFC):** It is an internal component of a VNF that provides a VNF provider with a defined subset of that VNF's functionality. Its main characteristic is that a single instance of this component maps 1:1 against a single instance of an atomic deployable unit.
7. **Virtualization layer:** It consists of two sub layers: a host OS and hypervisor (for VMs) and CIS (for containers).
8. **Container Infrastructure Service (CIS):** the cloud-native equivalent of hypervisor is container infrastructure service (CIS), which provides all the runtime infrastructural dependencies for one or more container virtualization technologies.
9. **Container:** It is a virtualization container using a shared operating system (OS) kernel of its host. Containers can host a VNF component (VNFC) for instance. VM-based components within NFV
10. **Hypervisor:** It is a piece of software which partitions the underlying physical resources and creates virtual machines, and isolates the VMs from each other. It is running either directly on top of the hardware (bare metal hypervisor type 1) or running on top of a hosting operating system (hosted hypervisor type 2).
11. **Virtual Machine (VM):** It has all the ingredients (processor, memory/storage, interfaces/ports) of a physical computer or server and is generated by a hypervisor, which partitions the underlying physical resources and allocates them to VMs. Virtual machines can host a VNF component (VNFC) for instance.
12. **NFV Orchestrator (NFVO)** - It is in charge of orchestration and management of the NFVI and software resources. It also takes care of network services in the NFVI.
13. **VNF Manager (VNFM)** - It is responsible for lifecycle management of VNFs (e.g. Instantiation, update, scaling, query, termination). There may be scenarios that can have multiple VNFMs may be deployed, VNFM may be deployed for each VNF or VNFM may serve multiple VNFs.

14. **Virtualized Infrastructure Manager (VIM)** - It comprises the functionalities that are used to control and manage the interaction of VNF with computing, storage and network resources under its authority.
15. **Container Infrastructure Service Management (CISM):** is a functional block that manages one or more container infrastructure services. The CISM provides mechanisms for lifecycle management of the managed container infrastructure objects, which are hosting application components as services or functions. It is a cloud-native equivalent of virtualized infrastructure manager (VIM). Kubernetes - K8s(for cloud native NFs) is a possible solution for CISM.
16. **NFV Security Manager (NFV SM/NSM):** NFV SM is a function that applies security policy to a virtualized network based on both predefined default policy and active analysis of information provided through security monitoring

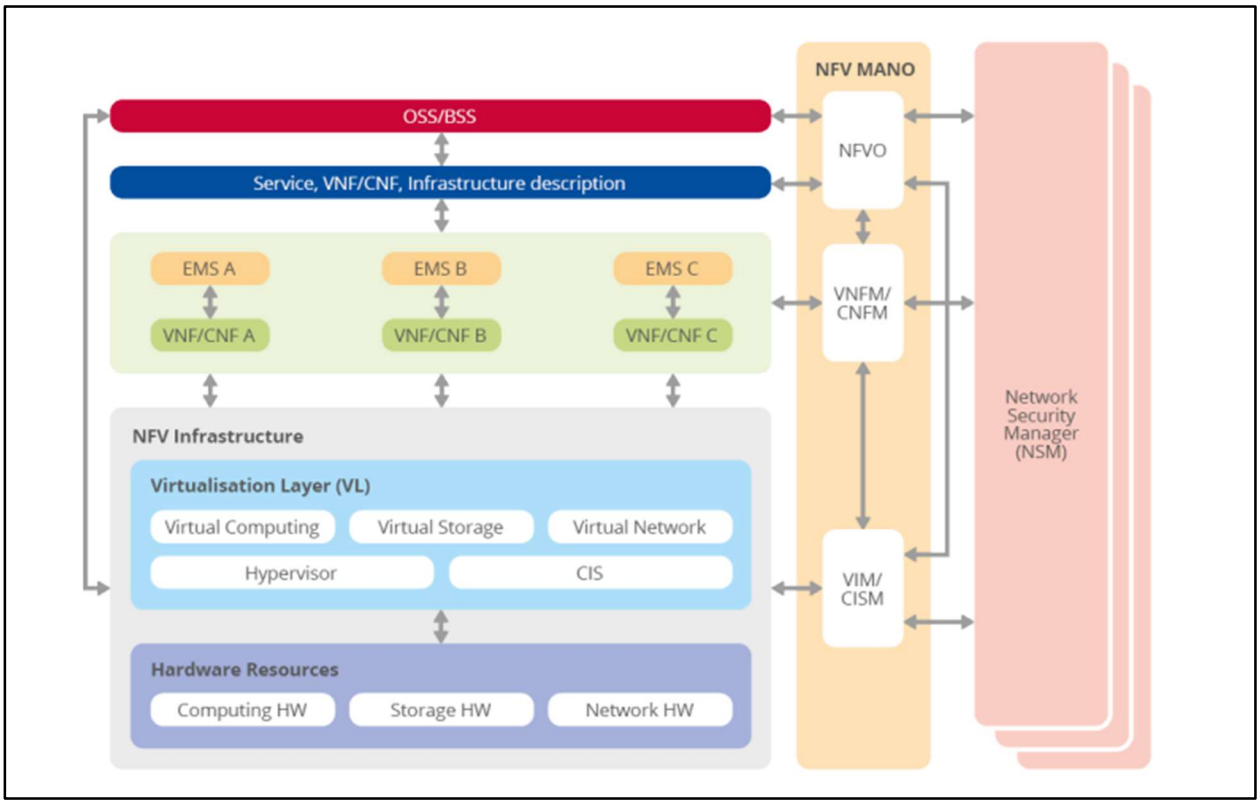

Fig 4 Adapted NFV architecture

3.NFV Security. Network Functions Virtualization will leverage modern technologies such as those developed for cloud computing to deliver end-end network services using the NFVI. Network function virtualization increases the attack surface. In a traditional telecom environment, it is sufficient to secure the hosts (with their operating systems), the applications running on these hosts, and the communication between these applications. With network function virtualization, it is also necessary to protect the hypervisor/CIS and its communication with the management infrastructure, and employ strict identity and access management. An unsecure hypervisor/CIS will impede adequate isolation of VMs/Containers running on the same host, inadequate identity and access management will result in compromises of the whole NFV infrastructure. With that, unauthorized parties may maliciously or accidentally impact the lifecycle of virtual machines.

A result of network function virtualization is extensive use of APIs. If as much as control of the NFV infrastructure is done programmatically, there shall be strict API access control. In particular, it is essential that there be adequate security control in place when APIs are used to provide orchestration and interaction between virtualized network functions and the underlying infrastructure.

Data protection is an essential aspect of NFV security. It covers data confidentiality, data integrity, and access control. Various data protection techniques can be deployed based on use cases.

The security requirement for NFV is covered in the subsequent chapters.

Chapter 2 – Common Security Requirements

(Applicable to NFV infrastructure(platform), NFV, SDN and MANO components. All these are denoted as system here)

Section 1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:

The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.

Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for management and maintenance.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

The management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.4]

2.1.3 Role-based access control policy

Requirement:

The system shall support Role-Based Access Control (RBAC). A role-based access control system uses a set of controls that 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 (e.g View, Modify, Execute). The system shall support RBAC with minimum of 3 user roles, in particular, for OAM privilege management for System Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

[Reference TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.2]

2.1.4. User Authentication – Local/Remote

Requirement:

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute 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 all the accounts from misuse. An exception to this requirement is local access and machine accounts where atleast one authentication attribute shall be supported.
The same authentication credentials must not be reused on different components of platform, SDN, NFV and MANO.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

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

[Reference TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.6]

2.1.6 Authorization Policy

Requirement:
The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.
Authorizations to 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 shall not be executed with administrator or system rights.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts removal

Requirement:

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Sections 4.2.3.4.1.2]

2.1.8 Operators must ensure that they use an out-of-band (OOB) management network that is not accessible from the internet so management interfaces are secured from remote access. If an operator allows for remote access into the OOB for employees and/or OEM support, the operator must ensure that they use a multi-factor authentication (MFA), at a minimum, for any type of VPN access. An MFA VPN combined with zero-trust greatly improves secure remote access to protect the 5GC Network.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T08]

Section 2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:
The usage of a system function without successful authentication on basis of the user identity and at least two authentication attribute (e.g. password, certificate) shall be prevented. For machine accounts and local access 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: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

Requirement:
If the system supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services) then the communication between system and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only.

2.2.3 Protection against brute force and dictionary attacks

Requirement:
A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in system.
Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.
Various measures or a combination of the following measures can 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 and an attacker can force this to deactivate accounts and make them unusable.
(iii) Using an authentication attribute blacklist to prevent vulnerable passwords.
(iv) Using 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 System. An exception to this requirement is machine accounts.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:
(a) The configuration setting shall be such that a system 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 system). 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. @;!$.)

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 system.
e) When a user is changing a password or entering a new password, system /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.).
Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

Additionally, pepper may be included to increase the complexity i.e password hash is a function of password, salt and pepper.

IETF draft-ietf-kitten-password-storage-04-BCP
[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3]

2.2.5 Inactive Session timeout

Requirement:
An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.
The system 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: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:
If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it shall be possible to implement this function on this system.
Password change shall be enforced after initial login. (after successful authentication)

System shall enforce password change based on password management policy.
In particular, the system shall enforce password expiry. System 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 system shall store at least the three previously set passwords. The maximum number of passwords that the system 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.

The system 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 System.

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 based on key events including, not limited to
• Indication of compromise (IoC)
• Change of user roles
• When a user leaves the organization

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.2]

CIS Password Policy Guide

2.2.7 Protected Authentication feedback

Requirement:

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 "*".

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:
Predefined or default authentication attributes shall be deleted or disabled**. (**or changed**)**
Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, OEM or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the OEM provides instructions on how to manually change it.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.3]

2.2.9 Logout function

Requirement:

The system 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. The network product 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.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.1]

2.2.10 Policy regarding consecutive failed login attempts

Requirement:

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

[Reference TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.5]

2.2.11 Suspend accounts on non-use:
It shall be possible for the system to automatically suspend an account after 'X' days without a valid login.

Note: X may be specified by operator.

Ref: CIS Password Policy Guide

Section 3: Software Security

2.3.1 Secure Update

Requirement:
For software updates, the system shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.
To this end, the system 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.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

(i) The system's Software package integrity shall be validated in the installation /upgrade stage.

(ii) The system shall support software package integrity validation via cryptographic means, e.g., digital signature, code signing certificate (valid and not time expired), and using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only. To this end, the System has 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.

(iii) Tampered software shall not be executed or installed if the integrity check fails.

(iv) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in (ii) above.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:
a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).
b) Also, OEM shall submit the undertaking as below:
(i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the system Software which includes OEM developed code, third party software and opensource code libraries used/embedded in the system.
(ii)System software shall be free from CWE top 25, OWASP top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security

weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.
(iii) The binaries for system and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

Note: Code signing (valid and not time expired) also allowed.

2.3.4 Known Malware and backdoor Check

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

2.3.5 No unused software

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:
The system 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. The system 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
- 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 system and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:

The system can boot only from the memory devices intended for this purpose.

[Reference– TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section-4.2.3.3.2]

2.3.8 Secure Time Synchronization

Requirement:
The reliable time and date information shall be provided through NTP/PTP server. All elements/functions which require time stamp shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" with NTP/PTP server.
Audit logs shall be generated for all changes to time settings.

In 5G networks, high precision time synchronization within microseconds will be required. 5G will not only provide personal mobile service, but also massive machine type communications (MTC) and services where latency and reliability are critical. These critical services require trusted and protected time sources.

ETSI GR NFV-SEC 016 (Draft specification - work in progress) is a study on how the location of sensitive VNFs (e.g., LI functions, VNFs handling data with restrictions on the location where data protection is handled and network security functions) can be attested. The study considers using trusted locstamp and timestamp information derived from global navigation satellite systems (GNSS), such as Galileo. The study also considers other binding solutions for physical location. The report outlines several solutions for timestamp-time synchronization and distribution (e.g. White Rabbit Network, IEEE® 1588-2019, based on trusted GNSS/ LEOs), for timestamp datacenter time protocol (DTP) and for locstamp (e.g. based on binding a trusted hardware 's ID with the location of a vertical hierarchy, indoor positioning such as RFID tagging and trusted GNSS positioning.

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

2.3.9 Restricted reachability of services

Requirement:
The system 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 shall 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: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.2]

2.3.10 Self Testing

Requirement:

A 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. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

Section 4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:
Unused functions i.e the software and hardware functions which are not needed for operation or functionality of the system shall be deactivated in the system'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 system.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:
OEM to ensure that the system shall not contain software and hardware components that are no longer supported by them or their 3rd Parties including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be given by system.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.5]

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

System shall not contain any wireless access mechanism which is unspecified or not declared.

An undertaking shall be given by the OEM as follows:

"The system does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

Section 5: User Audit

2.5.1 Audit trail storage and protection

Requirement:
The security event log shall be access controlled (file access rights) such that only privilege users have access to the log files.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:
The system shall log all important Security events with unique System Reference details as given in the Table below.
System 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 below:

Event Types (Mandatory or optional)	**Description**	**Event data to be logged**
Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the system.	Username
		Source (IP address and ports) if remote access
		Outcome of event (Success or failure)
		Timestamp
Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username,
		Timestamp,
		Length of session
		Outcome of event (Success or failure)
		Source (IP address &port) if remote access
Account administration (Mandatory)	Records all account administration activity, i.e.	Administrator username,
		Administered account,

	configure, delete, copy, enable, and disable.	Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
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 (Threshold Exceeded)
		Timestamp
Configuration change (Mandatory)	Changes to configuration of the network device	Change made
		Timestamp
		Outcome of event (Success or failure)
		Username
Reboot/shutdown/crash (Mandatory)	This event records any action on the network device/system that forces a reboot or shutdown OR where the network device/system has crashed.	Action performed (boot, reboot, shutdown, etc.)
		Username (for intentional actions)
		Outcome of event (Success or failure)
		Timestamp
Interface status change (Mandatory)	Change to the status of interfaces on the network device/system (e.g. shutdown)	Interface name and type
		Status (shutdown, down missing link, etc.)
		Outcome of event (Success or failure)
		Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	Administrator username,
		Administered account,
		Activity performed (group added or removed)
		Outcome of event (Success or failure)

		Timestamp.
Resetting Passwords (Optional)	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
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update (Optional)	Attempt to initiate manual update, initiation of update, completion of update	User identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	Old value of time
		New value of time
		Timestamp
		origin of attempt to change time (e.g.IP address)
		Subject identity
		Outcome of event (Success or failure)
		User identity
Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of	User identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)

	an interactive session.	Subject identity
		Activity performed
		Type of event
Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators (Optional)	Initiation, Termination and Failure of trusted Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
Audit data changes (Optional)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure)
		Subject identity
		User identity
		origin of attempt to change time (e.g.IP address)
		Details of data deleted or modified
User Login (Mandatory) and Logoff	All use of Identification and authentication mechanisms.	User identity
		Origin of attempt (IP address and port)
		Outcome of event (Success or failure)
		Timestamp

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:
(I) (a) The system shall support (preferably immediate) forwarding of security event logging data to an external system available in redundant configuration by push or pull mechanism through redundant links.

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

(III) 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

It is recommended that all audit logs are transferred to log management platform outside the system (NFV/SDN/MANO/Platform) to maintain their integrity and remove the risk of tampering.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.2]

2.5.4 Logging access to personal data

Requirement:
In some cases, access to personal data in a 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.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.5]

2.5.5 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

2.5.6 Audit Logs

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 must be logged
   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 Powershell on windows system.

GSMA NG 133 Cloud Infrastructure Reference Architecture ver 2.0

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

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

Section 6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:

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

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

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the system (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 system (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".

2.6.3. Cryptographic Algorithms implementation Security Assurance

Requirement:
Cryptographic algorithm implemented inside the Crypto module of system shall be in compliance with the respective 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 algorithm implemented inside the Crypto module of system is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the System)"

2.6.4. Protecting data and information – Confidential System Internal Data

Requirement:
a) When system is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear text to users and administrators.
b) Access to maintenance mode shall be restricted only to authorised privileged user.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.2.]

2.6.5. Protecting data and information in storage

Requirement:
a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of system that are needed for the functionality shall be protected

against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" 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 in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.
(iii)Stored files in the system: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:
a) Without authentication and except for specified purposes, system 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.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**
a) System 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 overt channels such as, HTTPS, IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the System.
Session logs shall be generated for establishment of any session initiated by either user or system.

---

2. 6.8 Protection against Data Exfiltration - Covert Channel

Requirement:
a) system 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 DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the System.
c) Session logs shall be generated for establishment of any session initiated by either user or system.

Section 7: Network Services

2.7.1: Traffic Filtering – Network Level Requirement:

The system shall provide a mechanism to filter incoming IP packets on any IP interface.
In particular the system 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 shall 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 source IP, destination IP and port addresses of protocol header.

(v) To reset the accounting.

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

[Reference– TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.1]

2.7.2 Traffic Separation

Requirement:

The system shall support the physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 for further information.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.5.1].

2.7.3: Traffic Protection –Anti-Spoofing:

Requirement:

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.3.1.1]

2.7.4 GTP-C Filtering (when 5GC is interworking with EPC)

Requirement:

The following capability is conditionally required:

- For each message of a GTP-C-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.
- At least the following actions shall be supported when the check is satisfied:
- Discard: the matching message is discarded.
- 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.

This requirement is conditional in the following sense: It is required that at least one of the following two statements holds:

- system supports the capability described above, and this is stated in the product documentation.
- The systems documentation states that the capability is not supported and that the System needs to be deployed together with a separate entity that provides the capability described above.

[Reference– TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.3]

2.7.5 GTP-U Filtering

Requirement:
The following capability is conditionally required:
- For each message of a GTP-U-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.
- At least the following actions shall be supported when the check is satisfied:
- Discard: the matching message is discarded.
- 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.
This requirement is conditional in the following sense: It is required that at least one of the following two statements holds:
- System supports the capability described above, and this is stated in the product documentation.
- The system's product documentation states that the capability is not supported and that the system needs to be deployed together with a separate entity which provides the capability described above.

[Reference– TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.4]

2.7.6 Network security:

Topology hiding
All internal interfaces between VNF elements, supporting MANO platforms and IT elements (mediation, provisioning) that are not required to publicly communicate outside the operators network, shall use private IP addresses.
It is recommended that all external interfaces are NAT through a firewalling function to provide additional protection of the identity of the elements
within the VNFI.

VNF network security profile

Each VNF supporting VNFC functions shall have a predefined network security profile describing its requirements for vNICs, ports, port group, VLANs and the requirement for internal VXLAN connections.
The security profile shall also define the vNIC firewall rules related to protocols (port numbers) that need to be supported on each VLAN or VXLAN connection. It is expected that vendors will provide a security profile for their applications, which will have to be aligned with the operators' zoning guidelines.

Note: there shall never be a requirement for all ports to be open, particularly on external standard-based interfaces (e.g. GTP).

Deploy NFVs with separate dedicated interfaces
Ideally, separate physical interfaces shall be implemented to maintain different traffic segregation in line with security zoning and X.805 principles. However, if this is not supported by a vendor then a separate logical interface and VLAN must be used to maintain security zoning.

Production and O&M traffic separation
O&M interfaces shall not share the same physical NIC, vNIC, distributed port group (DPG) or port group with other production traffic types (e.g. BSS, User Plane or Signalling Connectivity from management to production cluster Any connectivity between the operation and management (MANO) cluster and the production cluster shall pass through a firewall. If a virtual firewall is implemented, it shall be implemented within the management cluster.

Note: it is expected that MANO systems would not share the same hypervisor or CIS environment as production NFV elements.

Network resource pools
To prevent a VM or container causing a DoS by monopolising system and network resources, it is recommended that network resource pools shall
be configured.
Internal virtual switching control
The internal hypervisor or CIS controlled virtual IP network (vSwitch/VDS) shall be controlled to ensure a policy of positive enabling and must not support default connectivity or 'any to any' functionality.
Virtual network monitoring
In some deployments, internal network monitoring functions can be installed on the virtualization layer. If these are installed, the functions must be restricted to the administrator only and shall not provide a mechanism for compromising the security of the hypervisor or CIS or other VMs or containers.

Additionally, any operation of this type of monitoring functionality shall generate an alarm to the VIM and be recorded in the audit logs.

VLAN and VXLAN zoning

A comprehensive set of common VLAN and VXLANs must be created across each NFVi to ensure traffic separation and security zoning requirements.

Note: VLAN and VXLAN zoning shall ensure that clear vendor separation is maintained.

Only VLAN and VXLANs necessary to support VNFs hosted on a cluster shall be configured on the 'leaf' and 'spine' switching layers. The VLAN IP infrastructure shall follow existing segmentation and zoning rules with the use of firewalls or other security controls to provide protection between zones.

Existing hardware firewall appliances can continue to be used to provide boundary protection when connecting to untrusted or semi-trusted networks (e.g. internet or GRX). However, it is recognized that virtualized security appliances may be used in the future.

Use of VPNs Where possible, VPNs shall be created between VNFs and both internal and external non-VNF environments, e.g. interconnectivity between P-GW and Mediation for EDR transfer or HLR/HSS provisioning interfaces with the BSS Provisioning platform.

Dedicated network infrastructure

If a third party XaaS provider is being used then it is recommended that dedicated local 'leaf' switching infrastructure supporting only the operator VNFs is provided to ensure segregation from other tenants.

Additionally, it is also recommended that dedicated spine switches be provided also but this may not always be practical.

Protect all OAM traffic

Link security can be provided through the use of native traffic encryption such as HTTPS, SFTP, SMNP v3 or using TLS or IPsec tunnelling protocols.

Note: it is recommended this control shall be applied in addition to any security protection provided if, for example, OAM traffic is carried over an IPsec tunnel.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T21]

2.7.7 Networking Security Zoning

Network segmentation is important to ensure that applications can only communicate with the applications they are supposed to. To prevent a workload from impacting other

workloads or hosts, it is a good practice to separate workload traffic and management traffic. This will prevent attacks by VMs or containers breaking into the management infrastructure. It is also best to separate the VLAN traffic into appropriate groups and disable all other VLANs that are not in use. Likewise, workloads of similar functionalities can be grouped into specific zones and their traffic isolated. Each zone can be protected using access control policies and a dedicated firewall based on the needed security level.
Recommended practice to set network security policies following the principle of least privileged, only allowing approved protocol flows. For example, set 'default deny' inbound and add approved policies required for the functionality of the application running on the NFV Infrastructure.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.6.3]

2.7.8 Network interfaces shall be locked down so that they only accept a restricted number of expected protocols.

2.7.9 Reliance on static identifier such as network IP addresses in a traditional perimeter-based security model is impractical. Virtual security appliances like Firewall, IDS/IPS shall be implemented either within VM/Container or Standalone VM/Container or in the virtualization layer.

Section 8: Attack Prevention Mechanisms

2.8.1 Network Level and application-level DDoS

Requirement:
The system shall have protection mechanism against Network level and Application-level DDoS attacks.
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:

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process

- Prioritizing processes
- Limiting of amount or size of transactions of an user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.1]

2.8.2 Excessive Overload Protection

Requirement:
The system shall act in a predictable way if an overload situation cannot be prevented. 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 System cannot reach an undefined and thus potentially insecure, state.

OEM shall provide a technical description of the System's Over Load Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements e.g. RAN)

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.3]

2.8.3 Manipulated packets that are sent to an address of the network device shall not lead to an impairment of availability.

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

Examples of such packets are:

- Mass-produced TCP packets with a set SYN flag to produce half-open TCP connections (SYN flooding attack).

- Packets with the same IP sender address and IP recipient address (Land attack).

- Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).

- Fragmented IP packets with overlapping offset fields (Teardrop attack).

- ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IPv4 packets (Ping-of-death attack).

- Uncorrelated reply packets (i.e. packets which cannot be correlated to any request).

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.6.2.2]

Section 9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.4]

2.9.2 Port Scanning

Requirement:

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:

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

Sl 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 withing three months
4	0.1-3.9	Low	To be patched withing a year

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.3]

Section 10: Operating System

2.10.1 Growing Content Handling

Requirement:
a) Growing or dynamic content shall not influence system functions.
b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop the system from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:
Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the system.
system shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter	Permitted	N/A

		Problem		
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 system shall not respond to, or process (i.e., do changes to configuration) under any circumstances certain ICMP message types as marked in the 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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.2.]

2.10.3 Authenticated Privilege Escalation only

Requirement:

The system shall not support a 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.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:
Each system account shall have a unique identification with appropriate non-repudiation controls.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.2.2]

2.10.5 OS Hardening - Minimized kernel network functions

Requirement:
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:

1. IP Packet Forwarding between different interfaces of the network product.
2. Proxy ARP
3. Directed broadcast
4. IPv4 Multicast handling
5. Gratuitous ARP messages

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.2]

2.10.6 No automatic launch of removable media

Requirement:
The system shall not automatically launch any application when a removable media device is connected.
[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.3]

2.10.7 Protection from buffer overflows

Requirement:

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.5]

2.10.8 External file system mount restrictions

Requirement:
If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in the system 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.

[Reference– TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.6]

2.10.9 File-system Authorization privileges

Requirement:
The system 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: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.2.7]

2.10.10 SYN Flood Prevention

Requirement:
The system shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.4]

2.10.11 Handling of IP options and extensions

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.2.4.1.1.3]

2.10.12 Restrictions on running Scripts / Batch-processes

Requirement:
Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, System 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.

2.10.13 Restrictions on Soft-Restart

Requirement:
The system 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 11: Web Servers

This entire section of the security requirements is applicable if the system supports **web management interface.**

2.11.1 HTTPS

Requirement:
The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.1]

2.11.2 Webserver logging

Requirement:
Access to the webserver (for both successful as well as failed attempts) shall be logged by system.
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 shall be included whenever possible.
- Status code of web server response

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.2]

2.11.3 HTTPS input validation

Requirement:
The system shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.
System 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: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.4]

2.11.4 No system privileges

Requirement:
No system web server processes shall run with system privileges.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:
HTTPS methods that are not required for system operation shall be deactivated.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:
All optional add-ons and components of the web server shall be deactivated if they are not required for system operation.

In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.4]

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

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.5]

2.11.8 No CGI or other scripting for uploads

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

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.6]

2.11.9 No execution of system commands with SSI

Requirement:
If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.
[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:
Access rights for system's web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.8]

2.11.11 No default content

Requirement:

Default content that is provided with the standard installation of the system's web server shall be removed.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.9]

2.11.12 No directory listings

Requirement:
Directory listings (indexing) / "Directory browsing" shall be deactivated.
[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.10]

2.11.13 Web server information in HTTPS headers

Requirement:
The HTTPS header shall not include information on the version of the system's web server and the modules/add-ons used.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.11]

2.11.14 Web server information in error pages

Requirement:
User-defined error pages and Error messages shall not include version information and other internal information about the system web server and the modules/add-ons used.
Default error pages of the system web server shall be replaced by error pages defined by the OEM.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:
File type or script-mappings that are not required for system operation shall be deleted.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.13]

2.11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the system web server's document directory.
In particular, the system web server shall not be able to access files which are not meant to be delivered.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.14]

2.11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:

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: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.15]

2.11.18 HTTP User session

Requirement:
To protect user sessions, system shall support the following session ID and session cookie requirements:
1. The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
2.The session ID shall be unpredictable.
3.The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
4.In addition to the Session Idle Timeout, system 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.
5.Session IDs shall be regenerated for each new session (e.g., each time a user logs in).
6.The session ID shall not be reused or renewed in subsequent sessions.
7.The system 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.
8.Where session cookies are used the attribute 'HttpOnly' shall be set to true.
9.Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
10.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.
11.The system shall not accept session identifiers from GET/POST variables.
12.The system shall be configured to only accept server generated session ID.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.3]

2.13.1 Remote Diagnostic Procedure – Verification

Requirement:

If the system 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

2.13.2 No System Password Recovery

Requirement:

No provision shall exist for System / Root password recovery.

2.13.3 Secure System Software Revocation

Requirement:

Once the system 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.

System shall support a well-established control mechanism for rolling back to previous software image.

2.13.4 Software Integrity Check –Installation

Requirement:

System shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

Tampered software shall not be executed or installed if integrity check fails.

2.13.5 Software Integrity Check – Boot

Requirement:

The system 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 Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" to the expected reference value.

2.13. 6 Unused Physical and Logical Interfaces Disabling

Requirement:

System 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.

2.13.7 No Default Profile

Requirement:

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

Chapter 3 Specific Security Requirements

Part I NFV Infrastructure

This part presents the NFV infrastructure(platform) specific security requirements. Kindly refer to Fig 5 below for different security domains

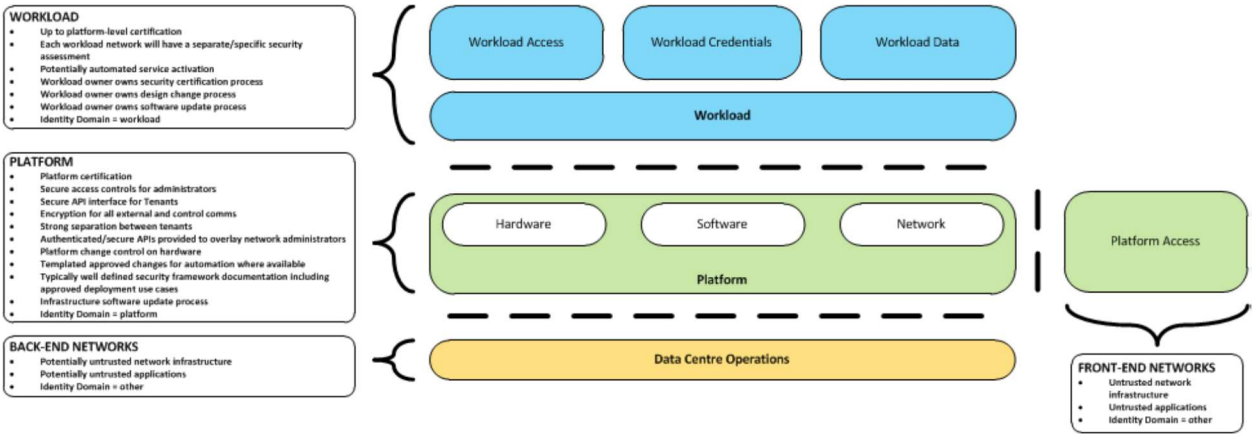

Fig 5 Security Domain

Cloud Infrastructure: A generic term covering NFVI, IaaS and CaaS capabilities - essentially the infrastructure on which a Workload can be executed.
Platform here include hardware, software and network that supports workloads i.e cloud infrastructure with all its hardware and software components.
Workload: An application (for example VNF, or CNF) that performs certain task(s) for the users. In the Cloud Infrastructure, these applications run on top of compute resources such as VMs or Containers.
Front-End Networks: to get access from internet and virtual/physical network used by carriage networks
Back-end networks: Datacenter operations access to the platform and subsequently, workloads.

1) Firmware/UEFI updates shall be applied in a timely manner to protect against hardware bugs and security flaws, including those which are newly found.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.8]
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T18]

---

2)The hypervisor that is launched shall be part of a platform and an overall infrastructure that contains:
(a) hardware that supports an Measured Launch Environment (MLE) with standards-based cryptographic measurement capabilities and storage devices and
(b) an attestation process with the capability to provide a chain of trust starting from the hardware to all hypervisor components. Moreover, the measured elements shall include, at minimum, the core kernel, kernel support modules, device drivers, and the hypervisor's native management applications for VM Lifecycle Management and Management of Hypervisor. The chain of trust shall provide assurance that all measured components have not been tampered with and that their versions are correct (i.e., overall boot integrity). If the chain of trust is to be extended to guest VMs, the hypervisor shall provide a virtual interface to the hardware-based MLE.

Reference: NIST SP 800-125A REV. 1 SECURITY RECOMMENDATIONS FOR SERVER-BASED HYPERVISOR PLATFORMS

---

3) CPU Pinning:

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

GSMA NG.133 - Cloud Infrastructure Reference Architecture

---

4)Workload Placement:

Affinity Rule: It specifies workloads that shall be hosted on the same computer node.
Non-Affinity Rule: It specifies workloads that shall not be hosted on the same computer node. It shall be possible to segregate workloads based on server groups (affinity and non-affinity groups)

---

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

---

6)The physical management interfaces like Baseband Management Controller, integrated lights out (iLO) etc shall use a dedicated network which is separate from virtualization fabric network.

---

7)The ToR switches shall be programmed to limit the VLAN/VXLANs used by hosts within the rack to only those virtual networks made accessible to the hosts.

---

8) Hardware-Based Root of Trust (HBRT)
The host system shall include an HBRT or TPM as Initial Root of Trust. The HBRT shall be based on hardware-based TPM or equivalent hardware root of trust (e.g., Secure Element including TPM functionalities, HSM including TPM functionalities).
The host system HBRT shall be able to provide isolated instances of the HBRT capabilities for individual workloads.
The host system HBRT shall include a hardware-based compute engine to be used by the workloads for cryptographic and security functionality.

ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 8.10

---

9) Hardware-Based Root of Trust (HBRT)

-The HBRT shall be both physically and electronically tamper-resistant.
- The HBRT shall be both physically and electronically tamper-evident.
- The HBRT physical and software interfaces between the HBRT and other hardware components of the host system to which it directly communicates shall be protected from eavesdropping, manipulation, replay or similar attacks.
- The level of resistance against attacks of the HBRT shall be verifiable and trustable using a certification process.

- It shall be possible to restrict the booting procedure if assistance from the HBRT is not available or the HBRT currently does not contain valid cryptographic material.
- Any tampering to the HBRT shall lead to detectable degradation of its function.
- The HBRT shall be physically protected such that any attempts to remove or replace the HBRT shall cause physical damage to both the HBRT and host system hardware to which the HBRT is attached, rendering both inoperable.

- The HBRT shall be (physically and/or logically) bound to the host system, so that any attempt to remove the HBRT will be detected and prevent normal operation of the host system.
- The HBRT shall include an Immutable Unique Identification value physically linked to the physical root of trust that can be used as identification of the platform. This value shall be stored in a shielded location protected from unauthorized use and disclosure.
- The HBRT shall provide capabilities to allow itself to be part of an attestation function.
- The host system shall have a mechanism to discover the tampered/non-tampered status of the HBRT.
- The host system shall have an interface to provide authorized external services with information about the tampered/non-tampered status of the HBRT.
- The host system shall provide a mechanism to report to authorized external services when tamper events occur.
ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 5.1

---

10)Chain of Trust: (CoT)

The *chain of trust (CoT)* is a method for maintaining valid trust boundaries by applying a principle of transitive trust. Each firmware module in the system boot process is required to measure the next module before transitioning control. Once a firmware module measurement is made, it is recommended to immediately extend the measurement value to a root of trust for storage, such as an HSM register, for attestation at a later point in time.

Static Root of Trust for Measurement (SRTM) begins with measuring and verifying the integrity of the BIOS firmware. It then measures additional firmware modules, verifies their integrity, and adds each component's measure to an SRTM value. The final value represents the expected state of boot path loads. SRTM stores results as one or more values stored in PCR storage. In SRTM, the CRTM resets PCRs 0 to 15 only at boot.
The host system shall support static root-of-trust measurement for hardware-based remote attestation.

In Dynamic Root of Trust for Measurement (DRTM), the RTM for the running environment are stored in PCRs starting with PCR 17. The host system shall support dynamic root-of-trust measurement for hardware-based remote attestation.

The chain of trust rooted in hardware shall be extended to the OS kernel and its components to enable cryptographic verification of trusted boot, system images, container runtimes and container images and so on. Chain of trust across hardware, operating system, hypervisor, VM, and container shall be ensured. Using a Trusted Platform Module (TPM), as a hardware root of trust, measurements of platform components, such as firmware, bootloader, OS kernel, shall be securely stored and verified.

---

11) Remote attestation

The remote attestation (RA) technique can be used to remotely verify the trust status of an NFV platform. ETSI suggests leveraging hardware security module (HSM), trusted platform module (TPM) and virtual TPM/HSM (vTPM/vHSM) to provide trusted protection for VNFs. These modules are used to shelter integrity measurements (i.e. hash values), cryptographic keys and certificates that are required to empower remote attestation of VNF components. Indeed, remote attestation guarantees the integrity of VNF instances at load time.
It shall be possible to attest a VNF through the full attestation chain from the hardware layer through the virtualization layer to the VNF layer.

Attestation of a platform's integrity shall be linked to the application layer and possible for other functions to query. If platform attestation fails, the VNF shall not be allowed to run.
Attestation of the VNF shall be performed prior to deployment or network integration and during operations.
Scenarios aimed to establish specific trust between NFV stakeholders:

(1) measurement of VM during launch,
(2) protected VM launch on a trusted NFVI,
(3) measurement of VM during launch and while in use,
(4) remote attestation of secret storage,
(5) secure VM migration between two trusted NFVIs.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T9]

---

12) Asset Tagging and Trusted Location

It shall be possible to assign specific labels for each server in the cloud infrastructure to enforce isolation of critical workloads and remotely attest each server's measurement and label against policies, feeding the results into a policy orchestrator to report, alert, or enforce rules based on events.

NISTIR 8320A HARDWARE-ENABLED SECURITY

---

13)Trusted computing technologies: To provide a trusted hardware platform, the hardware (blade servers) shall support Intel TXT, SGX, AMD SEV or ARM Trustzone silicon-based security functionality implemented with a TPM that stores measurements of the entire hypervisor or CIS stack and boot process.

This measure shall be applied to:

-blade clusters supporting VNF that support security critical functions; for example, lawful interception, customer access credential (HSS), security key management (AuC) or that have external traffic interfaces directly accessed by third parties or customers (Internet, GRX);
-all other MANO and VNF blade clusters to improve base platform security and reduce the complexity of affinity rules and hardware cluster of differing security trust levels.

A mechanism shall be in place to identify any attempt to physically remove the TPM from a system board. If physical tampering has been identified the blade server shall be considered compromised and no longer be used to support VNFs. For example, on HP blades any attempt to remove an installed TPM from the system board breaks or disfigures the TPM security rivet.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T15]

---

14) Hardware security:

If hardware is provided by a third-party cloud provider, then a dedicated cluster supporting only the operator's VNFs shall be provided to ensure physical, not logical, segregation from other tenants.
It is also recommended that separate dedicated hardware is used to provide independent NFV management (MANO) and service clusters (NFV).
In addition, separated clusters shall be used to provide MANO and NFVI.

The use of HW secure enclave technologies, such as AMD SEV and Intel TDX provide stronger tenant isolation from the cloud provider. The general commercial off-the-shelf (COTS) hardware may have varying levels of security functionality, such as hardware rooted secure storage, unique hardware identities, secure boot with software integrity check, and trusted execution environment (TEE), built-in depending on the manufacturer.
TEE refers to a technique of storing or running code in a protected memory area where no other applications or the host have access. An example is secure enclaves that can be used as a hardware root-of-trust for secure storage of secrets and running sensitive code. A HSM or TPM can be used to provide hardware rooted protection of keys.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T16]

---

15) Platform Node Integrity:
Servers, storage, and network devices form the cloud infrastructure platform on which the cloud native 5G core is deployed. These devices have low level firmware running on variety of critical components such as BIOS, disk drive controller firmware, baseboard management controller firmware, SmartNICs, packet processing chips, crypto off load engines and miscellaneous micro controllers required for operation of the devices. Such firmware shall be updated frequently.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

---

16) Local or removable blade storage – SAN protection:

Local storage protection

If local blade storage is supported, then it shall not store sensitive information such that its theft or removal would enable an attacker to gain a copy of the stored data.

Mutual authentication between VMs or containers and SAN

Mutual authentication shall be implemented between each VM or container and its associated SAN storage using CHAP (e.g. DH-CHAP, FCPAP).

SAN data protection in transit

The operator shall consider protecting sensitive data in transit between NFV and SAN using encapsulated security payload (ESP), as specified by the fibre channel protocol (FC-SP) or equivalent.

SAN physical blade interface

It is recommended that a separate physical interface module is used on each blade or rack mounted server for connectivity to the SAN. It is not recommended for any SAN connectivity to share common IP interface with other operational traffic.

SAN storage protection

The SAN storage shall protect against tampering and any ability to create unauthorized local copies of any of the stored data.
In the event of tampering or unauthorized copying, an alarm and log event shall be generated recording what data has been copied and which user initiated the action.

Note: it is expected that the SAN security (including backup management) will be addressed through existing IT security controls for the operation, access, backup and availability of the SAN.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T20]

---

17) Key Management System

The host system shall implement a key management system which includes key generation, key storage, key deletion and cryptographic processing with the following requirements:
- The cryptographic material shall be stored in a shielded location, protected against eavesdropping and physical and environmental tampering.
- The key generation processing shall be protected against eavesdropping and physical and environmental tampering.
- The key management system shall include an access right management to the sensitive data.
- The key management system shall ensure a complete deletion of outdated keys under deletion request.
- The key management system shall be scalable and ensure a high availability service.

- The key management system shall be remotely manageable to allow evolution, security strengthening, and countermeasure deployment of the system.
The host system shall provide cryptographically separated secure environments to different applications.
ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 5.1

---

18)Server boot hardening

Requirement:

The server boot process must be trusted. For this purpose, the integrity and authenticity of all BIOS firmware components must be verified at boot. Secure Boot based on Unified Extensible Firmware Interface must be used. By verifying the signatures of all BIOS components, Secure Boot will ensure that servers start with the firmware expected and without malware insertion into the system.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture managed by OpenStack v1.0 Section: 6.3.1.1]

---

19)Entropy and random numbers

Requirement:

The host system shall provide a means by which the designed and actual availability (quality and available bandwidth) of entropy on the system can be queried by an authorized party.
The host system shall implement a random number generator.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 6.4]

---

20)De-provisioning workloads

Requirement:

The host system shall provide:

- the capability to perform a secure wipe of storage at the request of authorized external services.
- a mechanism by which authorized external services can confirm the completion of the secure wipe operation.
- a mechanism to ensure that storage which is in the process of a secure wipe cannot be re-allocated until that operation is successfully completed.
- a mechanism to perform a secure wipe, at the time of de-provisioning, of any and all files associated with a workload.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 6.7]

---

21)Dealing with failure

Requirement:

The host system shall be booted with debug options off by default. It shall make a record when debug options are turned on, and a specific log entry shall be created. This record shall be unalterable without a power-off or reboot of the host system. It shall have an interface to provide authorized external services with information about the state of its debug options, including their historical state since boot. It shall provide a mechanism to report to authorized external services when a change in debug status occurs.
On failure:
- The host system shall have an interface to provide authorized external services with information related to failures or replacement of its components.
- The host system shall provide a mechanism to report to authorized external services when failures occur.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 6.8]

---

22)Access controls

Requirement:

The host system shall implement mandatory Attribute-Based Access Control (ABAC). The host system shall extend ABAC to restrict the capabilities available to the superuser/root administrative user.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 8.5]

---

23)Direct access to memory

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

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

---

24)Function and Software

Requirement:
Infrastructure must be implemented to perform at least the minimal functions needed to operate the Cloud Infrastructure.

Regarding software:
1. Only that software which is required to support the functions shall be installed.
2. Any unnecessary software or packages shall be removed.
3. Where software cannot be removed, all services to it shall be disabled.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture managed by OpenStack v1.0 section: 6.3.1.4]

---

25)System Hardening

1) The Platform must maintain the specified configuration.
2) All systems part of Cloud Infrastructure must support password ruled defined in Chapter 2.
3) All servers part of Cloud Infrastructure must support a root of trust and secure boot.
4) The Operating Systems of all the servers part of Cloud Infrastructure must be hardened by removing or disabling unnecessary services, applications and network protocols, configuring operating system user authentication, configuring resource controls, installing and configuring additional security controls where needed, and testing the security of the Operating System
5) The Platform must support Operating System level access control.

6) The Platform must support Secure logging. Logging with root account must be prohibited when root privileges are not required.
7) All servers part of Cloud Infrastructure must be Time synchronized with authenticated Time service.
8) All servers part of Cloud Infrastructure must be regularly updated to address security vulnerabilities.
9) The Platform must support Software integrity protection and verification and must scan source code and manifests.
10) The Cloud Infrastructure must support encrypted storage, for example, block, object and file storage, with access to encryption keys restricted based on a need to know. Controlled Access Based on the Need to Know.
11) The Cloud Infrastructure shall support Read and Write only storage partitions (write only permission to one or more authorized actors).
12) The Operator must ensure that only authorized actors have physical access to the underlying infrastructure.
13) The Platform must ensure that only authorized actors have logical access to the underlying infrastructure.
14) All servers part of Cloud Infrastructure shall support measured boot and an attestation server that monitors the measurements of the servers.
15) Any change to the Platform must be logged as a security event, and the logged event must include the identity of the entity making the change, the change, the date and the time of the change.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.1]

---

26) Platform and Access

1) The Platform must support authenticated and secure access to API, GUI and command line interfaces.
2) The Platform must support Traffic Filtering for workloads (for example, Fire Wall).
3) The Platform must support Secure and encrypted communications, and confidentiality and integrity of network traffic.
4) The Cloud Infrastructure must support authentication, integrity and confidentiality on all network channels.
5) The Cloud Infrastructure must segregate the underlay and overlay networks.
6) The Cloud Infrastructure must be able to utilize the Cloud Infrastructure Manager identity lifecycle management capabilities

7) The Platform must implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control).
8) The Platform must be able to assign the Entities that comprise the tenant networks to different trust domains
9) The Platform must support creation of Trust Relationships between trust domains.
10) For two or more domains without existing trust relationships, the Platform must not allow the effect of an attack on one domain to impact the other domains either directly or indirectly.
11) The Platform must not reuse the same authentication credential (e.g., key-pair) on different Platform components (e.g., on different hosts, or different services).
12) The Platform must protect all secrets by using strong encryption techniques, and storing the protected secrets externally from the component.
13) The Platform must provide secrets dynamically as and when needed
14) The Platform shall use Linux Security Modules such as SELinux to control access to resources.
15) The Platform must not contain back door entries (unpublished access points, APIs, etc.).
16) Login access to the platform's components must be through encrypted protocols such TLS v1.2 or higher
17) The Platform must provide the capability of using digital certificates that comply with X.509 standards issued by a trusted Certification Authority.
18) The Platform must provide the capability of allowing certificate renewal and revocation.
19) The Platform must provide the capability of testing the validity of a digital certificate (CA signature, validity period, non-revocation, identity).
20) The Cloud Infrastructure architecture shall rely on Zero Trust principles to build a secure by design environment

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.2]

---

27) Workload Security

1) The Platform must support Workload placement policy.
2) The Cloud Infrastructure must provide methods to ensure the platform's trust status and integrity (e.g. remote attestation, Trusted Platform Module).
3) The Platform must support secure provisioning of workloads.

4) The Platform must support Location assertion (for mandated in-country or location requirements).
5) The Platform must support the separation of production and non-production Workloads.
6) The Platform must support the separation of Workloads based on their categorisation (for example, payment card information, healthcare, etc.).
7) The Operator shall implement processes and tools to verify NF authenticity and integrity.

Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.4]

---

28) Image security on cloud Platform

Requirement:
In order to maintain Images securely the following requirements shall be followed

- Images must be scanned to be maintained free from known vulnerabilities.
- Images must not be configured to run with privileges higher than the privileges of the actor authorized to run them.
- Images must only be accessible to authorized actors.
- Image Registries must only be accessible to authorized actors.
- Image Registries must only be accessible over secure networks that enforce authentication, integrity and confidentiality.
- Image registries must be clear of vulnerable and out of date versions.
- Images must not include any secrets. Secrets include passwords, cloud provider credentials, SSH keys, TLS certificate keys, etc.
- CIS Hardened Images shall be used whenever possible.
- Minimalist base images shall be used whenever possible.

[Reference:_GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.5]

---

29)Lifecycle management Security on cloud

Requirement:
The following aspects of lifecycle management shall be fulfilled

- The Platform must support Secure Provisioning, Availability, and Deprovisioning (Secure Clean-Up) of workload resources where Secure Clean-Up includes tear-down, defence against virus or other attacks.
- Cloud operations staff and systems must use management protocols limiting security risk such as SNMPv3, SSH v2, ICMP, NTP, syslog and TLS v1.2 or higher.
- The Cloud Operator must implement and strictly follow change management processes for Cloud Infrastructure, Cloud Infrastructure Manager and other components of the cloud, and Platform change control on hardware
- The Cloud Operator shall support automated templated approved changes.
- Platform must provide logs and these logs must be regularly monitored for anomalous behaviour.
- The Platform must verify the integrity of all Resource management requests.
- The Platform must be able to update newly instantiated, suspended, hibernated, migrated and restarted images with current time information.
- The Platform must be able to update newly instantiated, suspended, hibernated, migrated and restarted images with relevant DNS information.
- The Platform must be able to update the tag of newly instantiated, suspended, hibernated, migrated and restarted images with relevant geolocation (geographical) information.
- The Platform must log all changes to geolocation along with the mechanisms and sources of location information (i.e. GPS, IP block, and timing).
- The Platform must implement Security life cycle management processes including the proactive update and patching of all deployed Cloud Infrastructure software.
- The Platform must log any access privilege escalation.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.6]

---

30)Audit and Monitoring on cloud infrastructure

Requirement:

In general, it is a good practice to have the same security monitoring and auditing capabilities in both production and non-production environments. However, we distinguish between requirements for Production Platform (Prod-Platform) and Non-production Platform (NonProd-Platform) as some of the requirements may in practice need to differ. when a requirement mentions only Prod-Platform, it is assumed that this requirement is optional for NonProd-Platform. If a requirement does not mention any environment, it is assumed that it is valid for both Prod-Platform and NonProd-Platform. The following are the requirements that shall be considered

- The Prod-Platform and NonProd-Platform must provide logs. The logs must contain the following fields: event type, date/time, protocol, service or program used for access, success/failure, login ID or process ID, IP address and ports (source and destination) involved.
- The logs must be regularly monitored for events of interest.
- Logs must be time synchronised for the Prod-Platform as well as for the NonProd-Platform.
- The Prod-Platform and NonProd-Platform must log all changes to time server source, time, date and time zones.
- The Prod-Platform and NonProd-Platform must secure and protect all logs (containing sensitive information) both in-transit and at rest.
- The Prod-Platform and NonProd-Platform must Monitor and Audit various behaviours of connection and login attempts to detect access attacks and potential access attempts and take corrective actions accordingly
- The Prod-Platform and NonProd-Platform must Monitor and Audit operations by authorized account access after login to detect malicious operational activity and take corrective actions.
- The Prod-Platform must Monitor and Audit security parameter configurations for compliance with defined security policies.
- The Prod-Platform and NonProd-Platform must Monitor and Audit externally exposed interfaces for illegal access (attacks) and take corrective security hardening measures.
- The Prod-Platform must Monitor and Audit service for various attacks (malformed messages, signalling flooding and replaying, etc.) and take corrective actions accordingly.
- The Prod-Platform must Monitor and Audit running processes to detect unexpected or unauthorized processes and take corrective actions accordingly.
- The Prod-Platform and NonProd-Platform must Monitor and Audit logs from infrastructure elements and workloads to detected anomalies in the system components and take corrective actions accordingly.
- The Prod-Platform and NonProd-Platform must Monitor and Audit Traffic patterns and volumes to prevent malware download attempts.
- The monitoring system must not affect the security (integrity and confidentiality) of the infrastructure, workloads, or the user data (through back door entries).
- The Monitoring systems shall not impact IaaS, PaaS, and SaaS SLAs including availability SLAs.
- The Prod-Platform and NonProd-Platform must ensure that the Monitoring systems are never starved of resources and must activate alarms when resource utilisation exceeds a configurable threshold.

- The Prod-Platform and NonProd-Platform Monitoring components shall follow security best practices for auditing, including secure logging and tracing.
- The Prod-Platform and NonProd-Platform must audit systems for any missing security patches and take appropriate actions
- The Prod-Platform, starting from initialization, must collect and analyse logs to identify security events, and store these events in an external system.
- The Prod-Platform's and NonProd-Platform's components must not include any authentication credentials, e.g., password, in any logs, even if encrypted.
- The Prod-Platform's and NonProd-Platform's logging system must support the storage of security audit logs for a configurable period of time.
- The Prod-Platform must store security events locally if the external logging system is unavailable and shall periodically attempt to send these to the external logging system until successful.
-

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.7]

---

31)Confidentiality and Integrity protection on Platform

Requirement:
The following requirements shall be fulfilled for Confidentiality and Integrity protection on Platform

- The Platform must support Confidentiality and Integrity of data at rest and in transit.
- The Platform shall support self-encrypting storage devices.
- The Platform must support Confidentiality and Integrity of data related metadata.
- The Platform must support Confidentiality of processes and restrict information sharing with only the process owner (e.g., tenant).
- The Platform must support Confidentiality and Integrity of process-related metadata and restrict information sharing with only the process owner (e.g., tenant).
- The Platform must support Confidentiality and Integrity of workload resource utilization (RAM, CPU, Storage, Network I/O, cache, hardware offload) and restrict information sharing with only the workload owner (e.g., tenant).
- The Platform must not allow Memory Inspection by any actor other than the authorized actors for the Entity to which Memory is assigned (e.g., tenants owning the workload), for Lawful Inspection, and by secure monitoring services.
- The Cloud Infrastructure must support tenant networks segregation.
- For sensitive data encryption, the key management service shall leverage a Hardware Security Module to manage and protect cryptographic keys.
- The monitoring system must not affect data confidentiality of the infrastructure, workloads or the user data.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.3]

[Reference– NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021)

---

32)Protection of data in transit

Requirement:

1. Where there are multiple hosting facilities used in the provisioning of a service, network communications between the facilities for the purpose of backup, management, and workload communications shall be cryptographically protected as prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" Only.
2. Systems transmitting data shall use protocols as prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" Only. Mutual authentication must be performed before encrypted data is sent from one system to another.
3. It must be ensured that all forms of data in transit are protected using strong cryptographic algorithms with strong integrity protection as prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" Only.
4. These mitigations require the use of key and certificate management systems (preferably global or federated, rather than ad hoc) between organizations sending and receiving this encrypted data.
5. Multiple cloud-based Hardware Security Modules (HSMs) shall be employed where practical and shall be required as a Root-of-Trust for high-risk or high-value data transmissions. This will also aid availability, data security monitoring, and governance.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021), Section-Protection of Data-in-transit]

---

33)Protection of data at rest

Requirement: The following requirements shall be met

1. All data persisted to primary, replica, or backup storage shall be encrypted.
2. Ensure all forms of data at rest are protected using strong cryptographic algorithms with strong integrity protection as prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" Only.
3. Cryptographic keys used to protect data, shall be refreshed periodically, atleast once a year.
4. Best practice is to secure the workload volumes by encrypting them and storing the cryptographic keys at multiple safe locations.
5. The hypervisor shall be configured to securely erase the virtual volume disks in the event of application crashes or is intentionally destroyed to prevent it from unauthorized access.
6. All subscriber data removed from the data at rest storage shall be cleaned
7. The Platform shall support self-encrypting storage devices.
8. Perform security-related testing and auditing of environments that store data at rest to ensure the effectiveness of the protection scheme and the protection of all sensitive and confidential data.
9. Ensure that access, Identity and Access Management (IAM), to data at rest is secured in a manner that strictly controls access to the data at rest according to the role, or access needs, required by the accessor.
10. Ensure that access to data is traceable by ensuring that all accessors of data are uniquely identifiable.
11. Ensure the availability of the data by performing real-time or near real-time back-ups of the data in order to protect from attacks (e.g., Ransomware attacks) and facilitate recovery from successful attacks.
12. User authentication related to access to data at rest shall use multi-factor authentication or Public Key Infrastructure (PKI) based certificate authentication.
13. Ensure that tools are in place to detect data integrity impacting events and processes exist that define recovery procedures.
14. All forms of storage related to data at rest, such as primary, replica, and backup, must meet the minimum requirements in terms of securing the data.
15. Backup storage can incorporate data integrity protection measures like a write once and read many approaches.
16. The Platform must support Secure Provisioning, Availability, and Deprovisioning (Secure Clean-Up) of workload resources where Secure Clean-Up includes tear-down, defense against virus, or other attacks. Note: Secure clean-up: tear-down, defending against virus or other attacks, or observing of cryptographic or user service data.
17. Multiple cloud-based Hardware Security Modules (HSMs) shall be employed where practical and shall be required as a Root-of-Trust for high-risk or high-value data

transmissions. This will also aid availability, data security monitoring, and governance.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021), Section-Protection of Data-at-rest]

---

34)Protection of data in use

Protecting and securing cloud data while *in use*, also referred to as *confidential computing*, utilizes hardware-enabled features to isolate and process encrypted data in memory so that the data is at less risk of exposure and compromise from concurrent workloads or the underlying system and platform.

A *trusted execution environment (TEE)* is an area or enclave protected by a system processor. Sensitive secrets like cryptographic keys, authentication strings, or data with intellectual property and privacy concerns can be preserved within a TEE, and operations involving these secrets can be performed within the TEE, thereby eliminating the need to extract the secrets outside of the TEE. A TEE also helps ensure that operations performed within it and the associated data cannot be viewed from outside, not even by privileged software or debuggers. Communication with the TEE is designed to only be possible through designated interfaces, and it is the responsibility of the TEE designer/developer to define these interfaces appropriately. A good TEE interface limits access to the bare minimum required to perform the task.

A hardware-mediated execution enclave is defined as an area of process space and memory within a system environment within a computer host which delivers confidentiality and integrity of instructions and data associated with that enclave. This enclave is protected from eavesdropping, replay and alteration attacks as the programs within the enclave are executed. An enclave is considered capable of executing processes, and executable code can be loaded into it. Encrypted data and code in the TEE is unavailable to other applications, the BIOS, operating systems, kernels, administrators, cloud vendors, and hardware components except CPUs. TEE-based confidential computing collaborates with sandboxed containers to isolate malicious applications and protect sensitive data.

Requirement: The following requirements shall be met

1. Implement Source Code Analysis of Code prior to load into TEE.
2. Perform regular updates/patching of Systems & Firmware for latest security fixes.

3. Leverage secure design guidance for code developed for TEE uses.
4. Verify and validate code before load into TEE using cryptographic methods such as Signature or hash checking.
5. The host system shall provide workloads access to hardware-mediated execution enclaves.
6. The host system shall make use of hardware-mediated execution enclaves when protecting its own sensitive processes
7. The host system shall provide the ability for authorized actors to perform a secure wipe of sections of memory in the HMEE.
8. The host system shall provide workloads with isolated enclaves.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021), Section-Protection of Data-in-use]

ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 8.9

---

35)Workload Provisioning:

1) The host system shall have an interface to provide authorized external services with information about its ability to prohibit host or hypervisor memory deduplication techniques that allow for sharing of memory pages between workloads.
2) The host system shall provide a mechanism to disable host or hypervisor memory deduplication techniques that allow for sharing of memory pages between workloads.
3) The host system shall disable host or hypervisor memory deduplication techniques that allow for sharing of memory pages between workloads by default. Where a capability is disabled, it shall not be possible re-enable it without a host system reboot.
4) The host system shall allow appropriately authorized parties to specify that certain memory types or locations (e.g. volatile vs non-volatile, on-blade vs off-blade) are not used for particular workloads.
5) The host system shall allow appropriately authorized parties to specify that only certain memory types or locations (e.g. volatile vs non-volatile, on-blade vs off-blade) are used for particular workloads
6) The host system shall provide the ability to prohibit local caching of binary images for workloads.
7) The host system shall have an interface to provide authorized external services with information about its ability to prohibit binary image caching.

8) The host system shall have an interface to provide authorized external services with information about its ability to provide perform secure provisioning of workloads.
9) The host system shall have an interface to provide authorized external services with information about its ability to provide secure de-provisioning of workloads.
10) The host system shall have an interface to provide authorized external services with information about its ability to block migration of workloads.
11) The host system shall provide secure provisioning of workloads.
12) The host system shall provide secure de-provisioning of workloads.

ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 6.2

---

36) Run Time Check
The integrity of a running system beyond its initial stages of provisioning, boot and software-loading may be checked by employing

• Integrity checking of running processes by local agents.
• Periodic checking of executable and binary file integrity by local agents.

ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 6.3

Infrastructure as a Code

Infrastructure as a Code (IaaC) (or also called Infrastructure as Code, IaC) refers to the software used for the declarative management of cloud infrastructure resources.

37) Secure Design and Architecture

Requirement:
a) Threat Modelling methodologies and tools shall be used during the Secure Design and Architecture stage triggered by Software Feature Design trigger. Security Control Baseline Assessment shall be performed during the Secure Design and Architecture stage triggered by Software Feature Design trigger.

b) Security Control Baseline Assessment shall be performed during the Secure Design and Architecture stage triggered by Software Feature Design trigger

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.9]

---

38)Secure Code Stage

Requirement:

The code shall be secured by adhering to the below mentioned requirements

- Static Application Security Testing must be applied during the Secure Coding stage triggered by Pull, Clone or Comment trigger.
- Software Composition Analysis shall be applied during Secure Coding stage triggered by Pull, Clone or Comment trigger
- Source Code Review shall be performed continuously during the Secure Coding stage.
- Integrated SAST via IDE Plugins shall be used during the Secure Coding stage triggered by Developer Code trigger.
- SAST of Source Code Repo shall be performed during the Secure Coding stage triggered by Developer Code trigger.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.10]

---

39)Continuous Build, Integration and Testing Stage

Requirement:
Following requirements shall be met during Build, Integration and Testing Stage

- Static Application Security Testing shall be applied during the Continuous Build, Integration and Testing stage triggered by Build and Integrate trigger.
- Software Composition Analysis shall be applied during the Continuous Build, Integration and Testing stage triggered by Build and Integrate trigger.
- Image Scan must be applied during the Continuous Build, Integration and Testing stage triggered by Package trigger.
- Dynamic Application Security Testing shall be applied during the Continuous Build, Integration and Testing stage triggered by Stage & Test trigger
- Fuzzing shall be applied during the Continuous Build, Integration and testing stage triggered by Stage & Test trigger.
- Interactive Application Security Testing shall be applied during the Continuous Build, Integration and Testing stage triggered by Stage & Test trigger.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.11]

---

40)Continuous Delivery and Deployment Stage

Requirement:
Following requirements shall be met during Delivery and Deployment Stage

- Image Scan must be applied during the Continuous Delivery and Deployment stage triggered by Publish to Artifact and Image Repository trigger.
- Code Signing must be applied during the Continuous Delivery and Deployment stage triggered by Publish to Artifact and Image Repository trigger.
- Artifact and Image Repository Scan shall be continuously applied during the Continuous Delivery and Deployment stage.
- Component Vulnerability Scan must be applied during the Continuous Delivery and Deployment stage triggered by Instantiate Infrastructure trigger.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.12]

---

41)Runtime Defense and Monitoring

Requirement:
Following requirements shall be met during runtime

- Component Vulnerability Monitoring must be continuously applied during the Runtime Defence and Monitoring stage and remediation actions must be applied for high severity rated vulnerabilities.
- Runtime Application SelfProtection shall be continuously applied during the Runtime Defence and Monitoring stage.
- Application testing and Fuzzing shall be continuously applied during the Runtime Defence and Monitoring stage.
- Penetration Testing shall be continuously applied during the Runtime Defence and Monitoring stage.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.13]

42)Software integrity protection and verification

Requirement:

The host system shall verify the provenance and integrity of all instances and versions of software components before installing them. It shall refuse to install all software that fails verification against the policies held by the host system. It shall verify the integrity of software components before execution.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 6.7]

43)Communications security

Requirement:

The host system shall use one or more of the following methods for communications security:

- TLS (minimum version 1.2) and IPSec, employing cryptographic primitives prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)", with client and server authentication required.
- The host system shall not use any of the following methods for communications security: SSL (any version), TLS 1.0, or TLS 1.1.
- The host system shall not employ anonymous TLS.
- The host system shall, when employing TLS or IPSec, use the latest approved version non-draft available.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 8.6]

44)Cryptographic primitives

Requirement:

The host system shall support the largest key length within an algorithm family, (refer Table1 of the latest document, "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)") in order to increase the resistance to emerging and anticipated threats.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 6.5]

---

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

Requirement:

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

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

---

46)UUID Generation

Requirement:
Support for the generation of UUID shall be provided as an alternative to the PKI.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.3]

---

47)Identity API Access Control

Requirement:
API access shall have some policy-based mechanism to maintain access control.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.8]

---

48)Time Synchronization

Requirement:

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

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.10]

---

49)Compute Isolation

Requirement:
The compute hosts in an availability zone can be further organized in terms of aggregates. The compute hosts in the same aggregate share a set of attributes (such as a tenant or a hardware capability) defined by administrators.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 11]

---

50)Re-evaluating trust

Requirement:
Many of the issues that need to be addressed revolve around establishment, re-establishment or revocation of trust. The requirement to re-evaluate trust may be prompted by a variety of different events, including time-based contexts such as a time-out or set frequency.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 Section 5.1.3]

---

51)Re-establishing trust

Requirement:

Re-establishing trust is defined here as the process of recreating a trust relationship between entity A and entity B which has previously existed, but which has, for whatever reason, failed.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 Section 5.1.5]

52)Assurance checks from Management and Operations domain

Requirement:
The Management and Operations domain which will have control over the service catalog holding the VNF Package, and it most likely to be in a position to make assurance checks on it.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 5.2.3.1.1]

53)Lifetime of entities

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

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

54)Provisioning/Deployment

Requirement:
Regarding the provisioning of servers, switches, routers and networking, tools must be used to automate the provisioning eliminating human error. The deployment tool is a sensitive component storing critical information (deployment scripts, credentials, etc.). The following rules must be applied:
1. The boot of the server or the VM hosting the deployment tool must be protected
2. Integrity of the deployment images must be checked, before starting deployment
3. Deployment must be done through dedicated network (e.g., VLAN)
4. When the deployment is finished, the deployment tool must be turned-off, if the tool is only dedicated to deployment. Otherwise, any access to the deployment tool must be restricted.
[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture managed by OpenStack v1.0 Section: 6.3.6.1]

55)Confidentiality and Integrity of communications

It is essential to secure the infrastructure from external attacks. To counter this threat, API endpoints exposed to external networks shall be protected by either a rate-limiting proxy or web application firewall (WAF), and shall be placed behind a reverse HTTPS proxy. Attacks can also be generated by corrupted internal components, and for this reason, it is security best practice to ensure integrity and confidentiality of all network communications (internal and external) by using Transport Layer Security (TLS) protocol.

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

---

56)Securing 3rd Party Hosting Environments:

Requirement:

Sensitive information of virtualized NFs shall be confidentiality protected when using a 3rd party environment (e.g., NFVI).
Third party hosting environments that support virtualized 3GPP NFs shall meet 3GPP virtualization security requirements and to enable operators to meet legal/regulatory requirements.
The system shall be able to monitor the attestation of 3rd party hosting environments.

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

---

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

Requirement: -

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

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

---

58) Front end access Security: Front-end network security at the application level will be the responsibility of the workload, however the platform must ensure the isolation and integrity of tenant connectivity to front-end networks.

GSMA NG 126 Ver 3.0 Section 7.4.3

---

59) Backend access Security: The integrity of resources management requests coming from a higher orchestration layer to the Cloud Infrastructure manage shall be validated and verified.

GSMA NG 126 Ver 3.0 Section 7.4.2

Part II Virtualization Security

(Applicable both to Hypervisor based VM and CIS based Container)

1) Application of hardening policies: The following shall be met
   The hypervisor or CIS shall be hardened to allow only the minimum services and processes necessary to operate VMs or containers, and all other services shall be removed by default. As a minimum, the following configuration changes must be made among others:
   a) remove all unused features;
   b) when a VM or container is deleted the virtual disk shall be zeroed to prevent an attacker reconstructing the contents of the VM or container disk;
   c) disable the ability to connect external devices to VMs or containers (e.g. CD, serial and parallel ports);
   d) make sure a VM does not have the ability to run with the full OS privilege level and can only operate at guest level; this can be controlled using Intel VT-x and AMD-V extensions;
   e) make sure each VM or container has a predefined set of restricted resources to ensure one VM or container cannot impact the resources
      and performance of another in the same hypervisor or CIS;
   f) disable the ability of a VM to initiate 'disk shrinking';
   g) enable persistent disk mode;
   h) restrict the visibility of one VM or container to detect another VM or container existing on the same host;
   i) use zoning and LUN masking to segregate SAN activity with each VM having unique authentication credentials;
   j) remove direct access to the O&M functionality of the hypervisor or CIS for management only through a secure connection from the VIM; however, this may not always be operationally feasible, so the hypervisor or CIS installation shall limit access to the hypervisor or CIS 'root' operating system to either:
      i) a dedicated O&M interface supporting a secure protocol (e.g. TLS 1.2 or above) with only an IP address,
      ii) ACL restriction on which domain can connect successfully;
   k) only allow 'root' access from the local terminal (LMP);
   l) where a hardware manufacturer provided monitoring tools that are implemented on the hypervisor or CIS or they utilise embedded support for industry standard protocols such as Common Information Model (CIM), these functions must be installed and operated on the hypervisor or CIS with limited privileges.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P12]

---

2) Strong password policy: A strong complex password shall be configured for each hypervisor or CIS 'root' account and secured in a safe location with physical and procedural controls on its access and use. It is recommended that the 'root' account is only used in exceptional operational circumstances by the hypervisor or CIS administrator and that separate user accounts are configured with less privilege for day-to-day operational management. Note: in the virtual environment hypervisor or CIS 'root' password has a greater significance as it controls multiple VMs or containers and provides access to security sensitive information.

   [Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P09]

---

3) Use and ownership of 'root' administration credentials:

   It is recommended that:
   a) each hypervisor or CIS has a single 'root' admin account that is used for local administration and to connect the host to VIM;
   b) to avoid sharing this common 'root' account, across the whole NFVI, at least one local named user account be created and assigned full admin privileges, and this account shall be the primary account for operating the hypervisor or CIS;
   c) strong access controls, account privileges and security logging are enabled;
   d) the hypervisor or CIS is configured to support multiple administration roles, and as a minimum there must be an admin role (highest privilege) and a separate operational role with minimal privileges to complete normal operational support;
   e) delegated administrator roles be used, with the global administrator role only being used in exceptional cases, e.g., to add permissions for other high-level administrators;
   f) all administration login attempts and critical operations must be logged and audited.

   [Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T18]

---

4) Hypervisor/CIS protection:

Hypervisor or CIS introspection can be used to scrutinize software running inside VMs or containers to find abnormal activities. It acts as a host based IDS that has access to the states of all VMs or containers, so that the root kit and boot kit inside VMs or containers cannot hide easily. Using introspection capabilities, the hypervisor's or CIS's functionalities are enhanced, enabling it, among other things, to monitor network traffic, access files in storage, and to execute read memory. Hypervisor or CIS introspection APIs are powerful tools to perform deep VM or container analysis and potentially increase VM or container security. However, they can also be used as an exploit that makes it possible to break and bypass the isolation between VMs or containers and the hypervisor or CIS.

The hypervisor or CIS must enforce network security policies. This includes, but is not limited to, ensuring that;

a) VMs or containers are isolated from each other,
b) VMs or containers are prevented from accessing each other's memory spaces,
c) keys used to encrypt memory are also under hypervisor or CIS control,
d) hypervisors or CISs are not allowed to write directly to memory,
e) hypervisors or CISs are not allowed to bypass normal memory access controls and security within the VM or container,
f) hypervisors or CISs are not allowed to change data within a VNF at run-time

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T07]

---

5) VNF shall include a secure boot process.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.19]

---

6) The VNF shall synchronize with trusted time source.
[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.20]

---

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

Requirement: -

The NFVI shall provide security isolation to minimize the impact of and detect hypervisor/VM breakout on a virtualized 3GPP NF.
The NFVI and VNFs shall be patched regularly.

The system shall prevent and detect attacks that breakout from an attacked VNF through the virtualization layer to any other VNF or any other location.

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

---

8) Data synchronicity through network

Requirement:

In a virtualized environment, flexible and low cost (both in money and resource terms) security monitoring agents can be easily inserted around multiple VNFs across the network, which could allow an attacker to identify the different messages making up a single procedure.

The virtualized 3GPP NFs shall be protected from distributed monitoring attacks. The system shall dynamically assign VNF resources (e.g. memory address) to prevent long-term data leakage and exposure and protect network resources.

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

---

9) Image Snapshot and VNF Mobility

Requirement:

-Migration of a VNF from a trustworthy environment to an untrustworthy environment shall not be possible, e.g., the access to virtualization management operations, like starting, stopping, pausing, restarting, live migration of a VNF, shall be subject to authentication and authorization.
-VNF data shall be confidentiality protected when stored as part of a VNF snapshot or during migration of the VNF to another execution environment.
-Where VNF sub-components are in different trust domains, the snapshot shall maintain security and isolation requirements for each trust domain within the snapshot of the VNF.
-The ability of a VNF to verify the trustworthiness of another VNF shall not be impeded by pausing, stopping, restarting, or migrating a VNF.

-All VNF Snapshot and VNF mobility operations shall preserve the persistent state of the VNF in order to prevent forking or roll-back attacks.
-It shall be possible to protect and prevent sensitive VNF or VNF-components from being subject to snapshot or migration without explicit authorization.
-All system snapshots events shall be subject to secure logging.
-Snapshots shall be securely deleted, once they are no longer required or after a specified maximum snapshot age has been reached.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.30]

---

10)VNF Protection

Protection of VNFs

It shall be possible to deploy a VNF to a host that provides specific security resources (e.g. HMEE, secure compute, secure memory) in order to bind a VNF to a specific host or group of hosts.
Binding shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.
The system shall manage (e.g. assign or log bindings) key storage and confidential data in a manner that provides protection against data compromise.
Sensitive data shall only be decrypted or handled in an unencrypted format in VNFs on trusted and well-known hosts.
It must be possible to control whether untrusted or less trusted VNFs are allowed to run on the same host as VNFs in a higher trust domain.
It must be possible to further restrict VNFs on a single host depending on whether they handle decrypted sensitive data.
The system shall prevent and detect unauthorized or unintended data manipulation and leakage (e.g. modification of VNF images, instantiating parallel VM(s) or container(s) on the same physical CPU).

Securing internal VNF communication

Where a NFV is composed on multiple VNFs the vendor shall demonstrate how it protects the internal communication of its NFV, as it transits between VMs or containers.

Protection of stored data

NFV vendors shall ensure that any security critical (including LI), customer privacy or confidentiality related information is stored securely on any shared or local storage (e.g. SAN, SSD).

Vendors shall be able to clearly state the security mechanisms used to protect this data using industry standard best practice (e.g. encryption).

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T19]

---

11) VNF integration with authentication and authorization services

Requirement:

The VNF shall integrate with the operator's authentication and authorization services, e.g., IDAM (Identity Access Management). Limiting the number of repeated failed login attempts (configurable) reduces the risk of unauthorized access via password guessing (Bruce force attack). The restriction on the number of consecutive failed login attempts ("lockout_failure_attempts") and any actions post such access attempts (such as locking the account where the "lockout_duration" is left unspecified) shall abide by the operator's policies.

[Reference: ONAP - VNF API security requirements, October 2022]
[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture managed by OpenStack v 1.0 section: 6.3.2.2]

---

12) VNF Host Spanning

Requirement:

All control plane data in transit between hosts shall be sent over an encrypted and authenticated channel using the protocols as prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR).". User plane traffic between hosts may be protected. The system shall prevent and detect unauthorized VNF host spanning.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.15]

---

13) VNF Image validation and protection

A VNF Package is composed of several components such as, for example, VNFD, software images, scripts, etc. During the on-boarding of the VNF package, a validation of the package shall be performed. The validation shall be a procedure that verifies the integrity of the VNF package. A package is certified by performing acceptance testing and full functional testing against the VNF including configuration, management, and service assurance.

It is easy to tamper with VNF images. It requires only a few seconds to insert some malware into a VNF image file while it is being uploaded to an image database or being transferred from an image database to a compute node. Luckily, VNF images can be cryptographically signed and verified during launch time. This can be achieved by setting up some signing authority and modifying the hypervisor or CIS configuration to verify an image's signature before they are launched.

The software package and the artefacts within the package of a VNF shall have their integrity protected by the vendor's signature. The software package and the artefacts within the package of a VNF and the software catalogue holding its image shall have their integrity protected after onboarding. The software package and the artefacts within the package of a VNF containing sensitive information must support the protection of confidentiality.

Software package and artefacts within the package of a VNF must be bound to a specific network after onboarding, such that unauthorized software cannot be instantiated even if it has a valid vendor certificate.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T2]

---

14) The IDAM (Identity and Access Management) must be implemented in the 5G Cloud

Requirement:

5G networks shall assign unique identities to all elements that will communicate to other elements in the 5G network.

Before allowing access to a resource, each network element shall authenticate and authorize the entity requesting access.

Where possible, identities shall be assigned using Public Key Infrastructure X.509 certificates from a trusted certificate authority (CA) rather than username/ password combinations.

If username/password is used, multi-factor authentication (MFA) shall be enabled to reduce the risk of compromise.

The 5G network shall provide automated mechanisms for credential management.

Where possible, use certificate pinning or public key pinning to provide additional identity assurance when authentication is dependent upon multiple CAs.
All access to resources shall be logged.
Analytics for detecting potentially malicious resource access attempts shall be deployed and run regularly.
Applications and workloads shall be explicitly authorized to communicate with each other using mutual authentication. Due to the ephemeral nature of cloud computing, key rotation and lifespan need to be frequent and short to maintain the demands of high-velocity capabilities and control and limit the blast radius in case of credential compromise.

For the client and server to bi-directionally verify identity via cryptography, all workloads must leverage mutual/two-way transport authentication.
Authentication and authorization must be determined independently (decision point) and enforced (enforcement point) within and across the environment.

Authorization for workloads are granted based on attributes and roles/permissions for which they have been assigned. It is strongly recommended organizations use both Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) to provide granular authorization enforcement in all environments and throughout their workload lifecycle. Such a posture can enable defense in- depth, where all workloads are able to accept, to consume, and to forward the identity of the end user for contextual or dynamic authorization. This can be achieved through the use of identity documents and tokens.
It is critical to note, application or service identity is also essential in the context of microservices, where the identities of apps are primarily subject to be spoofed and impersonated by a malicious service. Utilization of a strong identity framework and service mesh can help overcome these issues.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part I: Prevent and Detect Lateral Movement (2021)]

---

15) The 5G Cloud Software shall be kept up-to-date and free from known vulnerabilities

Requirement:

Software repositories for known vulnerabilities and out-of-date versions shall be regularly scanned using one or more software scanning tools or services.

Third-party applications and libraries that are integrated into the network-slicing infrastructure shall be regularly monitored for publicly reported vulnerabilities.

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.

Sl 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 practically possible.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part I: Prevent and Detect Lateral Movement (2021)]

---

16)Availability

Requirement:

The user shall be able to replicate its virtual machine/ containers into various zones and clusters to achieve high availability.

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

---

17)Function and capability authorization control for VNFs

Requirement:

There are many functions and capabilities that will be provided by various parts of a VNF and various different entities within NFV may request that these functions and capabilities are employed. It is not always appropriate to provide authorization for an entity to access these, even when the same entity has previously done so.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 4.2.1.1]

---

18) Authorization

Identity Services shall support the notion of groups and roles. A user belongs to groups and each group has a list of roles that permits certain actions on certain resources.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture managed by OpenStack v 1.0, Feb 2022]

---

19) Token Generation

Requirement:

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

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

---

20) Token Verification

Requirement:

Validation of the received token shall be carried out before the provision of the requested service.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.2.3]

---

21) Token Transport

Requirement:

Token in transit to the authentication manager need to be protected.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.6]

---

22)Identity Federation

Requirement:

Through identity federation, it shall be possible to outsource identity management to an external provider known as an identity provider.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.7]

---

23)The software package must be checked for integrity during installation

Requirement:

Each individual artifact in a VNF Package shall have a cryptographic signature when it is stored in the NFV-MANO catalogue(s):

i) -The VNF provider's signature on individual artifacts in a VNF Package shall be stored by NFV-MANO.
ii) -Additionally, if the service provider policy mandates to sign an artifact, this service provider's signature on this individual artifact(s) shall be stored as well

[Reference: ETSI NFV-SEC021v2.6.1 VNF - GS, Section 5.1]

---

24)Input validation

Requirement:

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

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

---

25)Key Management and security within cloned images

Requirement:

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

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

---

26)Key Management and security within migrated images

Requirement:
When images are migrated, regardless of the vehicle for accomplishing the migration, they shall possess the same MAC addresses, CPU ID, and other hardware signatures that they possessed prior to the migration.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 Section 4.4.3.3.2]

---

27)Vulnerabilities within the runtime software

Requirement:

Organizations shall use tools to look for Common Vulnerabilities and Exposures (CVEs) vulnerabilities in the runtimes deployed, to upgrade any instances at risk, and to ensure that orchestrators only allow deployments to properly maintained runtimes.

[Reference: NIST Special Publication 800-190 [September 2017]]

---

28)Secure Logging

Requirement:

Creation of entries which are confidential from other parties: in general steps shall be taken to ensure there is no long-term requirement for confidential logging or storage of Retained Data information (i.e. the details of previous requests or responses).

[Reference: ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.2]

---

29)Post-incident analysis

Requirement:

It is important that post-incident analysis shall be performed as it helps to identify whether any stores of material have been affected, which may subsequently be used as evidence.

[Reference: ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.4]

---

30)Logging

Requirement:

The module shall provide standard features, such as a common set of logging levels for classifying the logged events, log file rotation, and runtime logging configuration.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 10.1]

---

31)Event Notification

Requirement:

Generation of event notifications shall be provided as it can serve as a basis for purposes such as accounting, security monitoring, troubleshooting, and auditing.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 10.2]
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T17]

---

32)Encrypted Storage

Requirement:
Persistent Volumes and Ephemeral volumes shall be kept encrypted.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 7.1]

---

33)Volume Sanitization

Requirement:

Secure deletion of the volumes shall be provided as it gives assurance that deleted data in shared storage cannot be recovered.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 7.2]

---

34)Policies for workload placement in Retained data

Requirement:

Retained Data collection, storage and query shall only take place in a geographic location compatible with national legislation for Retained Data.

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

---

35)Sensitive authentication data in workloads

Requirement:

NFV workloads routinely possess sensitive authentication data used for authenticating the workload, its processes and users. This sensitive authentication data can consist of passwords, private keys, cryptographic certificates, tokens and other secrets. This data

shall be protected during all phases of the NFV security and trust lifecycle and shall be considered highly dynamic in nature, with updates likely during instantiation, hibernation/suspension, and VNF retirement.

[Reference– ETSI GS NFV-SEC 003 V1.1.1 4.2.1.1]

---

36)Platform backup

Requirement:

The storage for backup must be independent of storage offered to tenants.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture managed by OpenStack v 1.0 Section: 6.3.6.3]

---

37)Validating the Topology of Virtualized Network Functions

Requirement:

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

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

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

---

38)Ensure disconnectedness between many parts of an infrastructure network

Requirement:

Without any Virtualized forwarding Functions running, there must not be any connectivity between each partitioned network (core or customer networks).

[Reference– ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.1.1]

---

39)Security Groups

Requirement:

Security groups mechanism shall be present that tenants can use to control network traffic from and to virtual machines or network interfaces. A security group is defined by a set of rules. A rule consists of specific conditions (mainly pertaining to the type, source, and destination of traffic) and the action (e.g., drop, reject, or accept) to be taken if the conditions are satisfied.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.1]

---

40)Anti-Spoofing

Requirement:

Support to anti-spoofing of MAC addresses, IP addresses, ARP messages, and DHCP messages shall be present.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.2]

---

41)Network Address Translation

Requirement:

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

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

---

42)Network Isolation

Requirement:

Traffic separation of various tenants shall be ensured.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.4]

---

43)Firewall-as-a-Service

Requirement:

FWaas shall be supported with cloud infrastructure as on-premise firewalls have limited capabilities.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.5]

---

44)Valid MIME type

The VNF MUST implement the following input validation control on APIs: Validate that any input file has a correct and valid Multipurpose Internet Mail Extensions (MIME) type. Input files shall be tested for spoofed MIME types.

[Reference: ONAP: VNF API security requirements, October 2022]

---

45)OS-level access control

Requirement:

OS-level access controls need to be implemented to provide mechanisms for supporting access control security policies on Operating System processes.

[Reference: ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.3]

---

46) The networking within the 5G cloud shall be securely configured

Requirement:

Security groups per cluster shall be created, this will make it easy to achieve network security compliance by running applications with varying network security requirements on shared compute resources.
Private networking shall be used for connecting network functions.
Default firewall rules shall be configured that determines which outbound or inbound connections are permitted.
Use Service Meshes to protect node-to-node traffic.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part I: Prevent and Detect Lateral Movement (2021)]

---

47) Lock down communications among isolated network functions

5G networks shall ensure that all communication sessions on an NF's control plane, user plane, management plane, and through the cloud infrastructure are authenticated using the identities provisioned from the Identity and Authorization session. For example, these sessions could use mutually-authenticated TLS v1.2+ where the X.509 certificates are the identities that are authenticated.

Policies shall be created and deployed that enforce the separation of network resources in the same security group based on secure authentication and authorization.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part I: Prevent and Detect Lateral Movement (2021)]

---

48) Develop and deploy analytics to detect sophisticated adversarial presence

Stakeholders at all layers of the 5G cloud stack shall leverage an analytic platform to develop and deploy analytics that process relevant data (cloud logs and other telemetry) available at that layer. The analytics shall be capable of detecting known and anticipated threat, but also be designed to identify anomalies in the data that could indicate unanticipated threat.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part I: Prevent and Detect Lateral Movement (2021)]

---

49)VNF Deployment:

Minimum baseline security controls and hardening measures shall be configured for new VNF deployments. This can be done in many ways such as using pre-hardened golden images, deployment time configuration, etc. Such controls include fully implemented access control rules and ensuring that any unused ports, features, insecure protocols, or services are disabled

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T04]

---

50)Cryptography:

Secure key management must be implemented to manage all the steps of a key lifecycle: key generation using an appropriate level of entropy from a reliable source, secure key storage, key rotation and revocation, secure key destruction, etc.

It is also recommended establishing PKI infrastructure for secure admin access and protecting your network against external access, especially in a cloud environment.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T06]

---

51)Software compliance and integrity preservation

1) A software checksum (hash or signature) shall be created by the vendor during NFV and a supporting NFVI (e.g., host OS, hypervisor or CIS, SDN Controllers) software compilation that can be validated with a corresponding checksum created during any testing and validation process operated by the operator or a third party.

(2) TEE is an important enabler for that goal. Tamper-proofing techniques enable the preservation of software integrity by causing an altered software to fail.

(3) The concept of trusted execution and the associated technologies (e.g. Intel SGX enclave) that make certain that even a malicious host OS or operator cannot tamper or inspect any managed payload memory space.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T10]

---

52)Security segmentation and isolation between network functions

To prevent a VM or container from impacting other VMs, containers or hosts, it is a best practice to separate VM or container traffic and management traffic. This will prevent attacks by VMs or containers tearing into the management infrastructure. It is also a good idea to separate the VLAN traffic into groups and disable all other VLANs that are not in use. Likewise, VMs or containers of similar functionalities can be grouped into specific zones and their traffic shall be isolated. Each zone can be protected using access control policies and a dedicated firewall based on security level it needs. One example of such zones is a demilitarized zone (DMZ). Due to differing security requirements, a separate virtual environment using separate clusters shall be setup for VNFs and MANO.

Physical and/or logical separation shall be applied to keep sensitive control plane sub-components within a VNF (e.g. key material or billing data) away from lower security sub-functions or other general user plane traffic handling sub-functions.

Best practices include:

1)Linux kernel security: in virtualized platforms, the kernel of the host systems is a highly important component that provides isolation between the applications. The SELinux module is implemented in the kernel and provides robust isolation between the tenants when virtualization technology is used over the host. Secure virtualization (sVirt) is a new form of SELinux, developed to integrate mandatory access control security with Linux based hypervisors. sVirt provides isolation between VM processes and data files. Beyond these tools, other kernel hardening tools can be useful to secure the Linux kernel. A notable example is hidepd, which can be used to prevent unauthorized users from seeing the process information of other users. Another example is GRSecurity, which provides protection against attacks on corrupted memory.
(2) Best practices are to avoid co-hosting, on the same hardware, VNFs that have very different levels of sensitivity or very different levels of vulnerability to influence by an attacker.
(3) The trust domains of network functions shall be identified. Each trust domain shall be managed separately. Security policies for each trust domain shall be managed independently.

(4) Delegated administrator roles must be used, with roles which could give a user or administrator the ability to inspect the memory of functions only in exceptional circumstances.
(5) Confidentiality protection shall be provided to protect information traveling between memory locations in a single or multiple logical memory block.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T11]

---

53) Encrypting VNF volume/swap areas: The best practice to secure the VNF volumes is by encrypting them and storing the cryptographic keys at safe locations. TPM or HSM modules can be used to securely store these keys.
In addition, the hypervisor or CIS shall be configured to securely wipe out the virtual volume disks in the event a VNF is crashed or intentionally destroyed to prevent it from unauthorized access.

VM or container swapping is a memory management technique used to move memory segments from the main memory to disk, which is used as a secondary memory in order to increase system performance in case the system runs out of memory. These transferred memory segments can contain sensitive information such as passwords and certificates. They can be stored on the disk and remain persistent even after system reboot. This enables an attack scenario whereby a VM or container swap is copied and investigated to retrieve any useful information. One way to avoid this kind of attack is to encrypt VM or container swap areas. Linux based tools such as dm-crypt can be used for this purpose

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T14]

Other Security Requirements:

54) Security By Design: The security-by-design concept shall be used to address the protection of NFV resources and components at design time through the integration of security mechanisms. This shall concern the hardware layer, the virtualization layer, MANO and VNFs.

Secure software development lifecycle (SDLC) principles shall be used to avoid vulnerabilities and thus contribute to developing NFV software applications and services in a secure manner.

The use of DevSecOps methodology shall be promoted. The DevSecOps process aims at merging the security discipline within DevOps, thus considering security in every stage of the development process. By having security and development teams working together early in the development lifecycle, security naturally finds itself in the product by design.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P14]

---

55) Software Bill of Material (SBOM): A SBOM is a formal record containing the details and supply chain relationships of various open source and commercial software components, libraries and modules used in building software. Complex systems such as the 5G NFV might include hundreds or even thousands of software components that software development and cybersecurity teams must track through all stages of the lifecycle.
An SBOM shall be made which provides those who produce, purchase and operate software with information that enhances their understanding of the supply chain, which enables multiple benefits, most notably the potential to track known and newly emerged vulnerabilities and risks.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P16]

---

56) Open-Source Software:

Requirement:
Open-source code must be inspected by tools with various capabilities for static and dynamic code analysis
The CVE (Common Vulnerabilities and Exposures) must be used to identify vulnerabilities and their severity rating for open-source code part of Cloud Infrastructure and workloads software.
Critical and high severity rated vulnerabilities must be fixed in a timely manner. Refer to the CVSS (Common Vulnerability Scoring System) to know a vulnerability score and its associated rate (low, medium, high, or critical).

A dedicated internal isolated repository separated from the production environment must be used to store vetted open-source content.
[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.8]

---

57) Life cycle Management: Secure software development principles for VNFs shall incorporate the following industry best practices:
    a. validating the removal of unused software modules and execution paths;
    b. validating the disabling of unused protocols and the closure of unused ports; Run VM or container image and software package scanning to find known vulnerabilities and fix them before release;
    c. using container-specific host OSs to reduce risk by limiting the attack surface,
    d. enforcing Centre for Internet Security (CIS) benchmarks for K8S, docker, and Linux to establish a hardened baseline;
    e. ensuring that the software supplier practices proper due diligence when using commercial third-party and open-source software in their projects
    f. validating application performance on the hardened infrastructure.

    [Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P15]

---

58) Resources inventory management system and database:

    Hardware inventory: It is expected a hardware (blade) for hypervisor or CIS and bare metal installation for inventory shall exist to support operational management. However, in addition, to providing the ability to complete security investigations and meet possible local regulatory or legal requirements, it is recommended that the inventory stores: 1. the location of each blade server (e.g. country, datacenter, rack, shelf); 2. mapping VNF to hypervisor or CIS and blade server showing the current and historic records; 3. information as to whether any native installations are sharing the same blade server chassis, associated resources and network infrastructure.

    Software inventory: A mechanism shall exist to identify all VNFCs running in each VM or container within each hypervisor or CIS. It shall also be possible to identify which hardware, datacenter, location and country is being used and the assigned IP addresses and types of communication flows, routing tables and effective security policies and filtering rules are in place. In addition, automatic validation shall be

completed against the VIM and EMS platforms to ensure only authorized VNFC applications are running and installed.

Open-source inventory: Organizations must set up accurate inventories of open-source software dependencies used by their various applications, or a process to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open-source. Data integrity shall be maintained between the NFVi and SDN controller layers and the resource inventory through a robust mechanism implemented during deployment. Such mechanism must have the capability to check the SDN and NFV configuration against the one stored on the resource inventory. It must also have the capability to validate the security policies to ensure they are still being applied correctly, e.g. verifying firewall rules on the orchestration interface or check location of any VNF. A detection or audit mechanism must be implemented to identify where a workflow has been initiated requesting changes to the NFV or SDN environment but where no acknowledgement has been received on its success or failure. Upon detection of such changes an alarm must be raised so the operational team can investigate the incident

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P11]

---

59) Supply Chain Security: Trustworthy equipment (all supply chain), resilient system and verification must all be based on standards. Devising the required standards must be a collaborative effort between private (industry, SME, and research) and public (policy makers, regulators) parties, as no single vendor, operator or government can do it alone.

Stakeholders shall implement effective supply-chain and procurement controls to ensure the services they operate and provide comply with legal requirements and manage supply-chain threats. Processes shall be in place to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process.

Zero trust principles shall be implemented to identify supply chain weaknesses across product creation, manufacturing, testing, and delivery — without the need for disruptions that ultimately can halt operations.

Cybersecurity audits and certifications shall be conducted by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance.

Through collaboration, a shared responsibility model, zero trust principles, and security assurance, supply chains will strengthen as security improves.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P10]

---

60) Defense In depth: Operators need to use all the layers of security (defense-in-depth) to protect the NFV platforms including firewalls, access control lists, IP tables, rate limiting, closing all unnecessary ports, disabling all unnecessary services (for example, TLS and remote access service may not be needed all the time, so therefore it would be a good idea to enable these services only when needed), using strong confidential integrity algorithms, and so forth.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P08]

---

61) Zero Trust: Treat 5G infrastructure as an untrusted environment and explicitly authenticate and authorize interactions between all assets in all areas - both inside and outside the network - prior to allowing access. Secure and limit interactions to the minimum necessary, and continuously monitor asset security posture, adjusting access rights accordingly.
Zero trust represents an overarching access security model that deliberately avoids assuming implicit trust between elements in a network. This is particularly important in 5G as various external stakeholders may need to access infrastructure components or services for management, maintenance or monitoring purposes. For example, enterprise users may need to select access to 5G slice management services. Third party vendors may need access to select components for configuration or troubleshooting. Properly implemented, zero trust can provide appropriate stakeholder access while securing 5G services against misuse.
Strong digital identities with digital signing from a certificate authority (CA) establishes a root of trust for VNFs while mutual authentication using transport layer security (TLS) or datagram TLS (DTLS) with public-key infrastructure and X.509 (PKIX) and strong cipher suites ensures trust between network functions, between

the network and NFV, and between application clients and server. (D)TLS with X.509 digital certificates provide automation and security to ensure that only trusted devices are permitted access to a trusted network and application.

A zero-trust architecture includes automated security configuration for control policies over user access with visibility, monitoring and logging for alerting and auditing. Multifactor authentication (MFA), an important component of zero trust, shall be used to ensure secure human access to management interfaces and applications in the 5G NFV. NFV components shall be assumed to be untrusted and be able to establish trust through the process of certificate based mutual authentication. Any of the NFV entities or components shall have a certificate and an associated and protected private key to execute cryptographic security functions with other terminating entities.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P01]

---

62) Vulnerability handling & patch management: NFV/MANO software components will need to be monitored for vulnerabilities and patched as quickly as possible to address evolving risks and ensure security and functionality.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P03]

---

63) Security Testing and Assurance: Regular penetration and vulnerability testing shall be performed across the NFVI and MANO production environment to identify any known vulnerabilities or compromise of the network zoning rules.
It is recommended that testing shall be carried out if new infrastructure or IP based interconnect elements have been deployed or as a minimum on an annual basis.
It is recommended to use certified components (e.g. hypervisors, OSs, TEE, TPM, etc.) according to a recognized scheme such as Common Criteria.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P04]

---

64) Incident Management: Implement defensive security controls and continuous monitoring backed by machine learning capabilities and establish incident response operations to detect and mitigate threats.

Key capabilities include the following.

Vulnerability management: adopt internationally-accepted standards and best practices on the coordinated disclosure of vulnerabilities and handling to effectively identify, mitigate, and remediate security vulnerabilities (e.g. software patching) in a timely manner

- Denial-of-service defense systems: monitor network traffic to detect and mitigate network flooding attacks.

Intrusion detection and prevention systems: monitor network traffic to detect and mitigate unauthorized access or attempts to exploit system vulnerabilities.

Malicious traffic filtering systems: monitor network traffic to block malicious or unwanted traffic such as spam or attempts to interact with malicious domains and websites.

Anti-malware systems: monitor network traffic and endpoint and server devices to detect and block malware files or malware execution.

Security operations center: establish a centralized security monitoring, incident response, and threat intelligence organization responsible for rapidly detecting and mitigating security breaches. Adopt integrated cybersecurity capabilities and automation tools that simplify and streamline security operations.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P05]

---

65) Secure update management: The process must consider the ability to update the cryptographic algorithms and to adapt to upcoming 5G security challenges. Updates must be applied in a timely manner to protect against hardware or software bugs and security flaws, including those which are newly found.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P06]

66) Restrictions on installing applications: It shall not be possible to install a VNF application into the operational NFV environment without validation and approval by the operator.
Note: this can be a manual control process but it is expected that additional technical security controls will be adopted that allow only signed code to be installed in the NFV infrastructure

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P07]

---

67) User Plane Security

Requirement:

Additional security controls are needed on the user plane as follows:

a. to protect NFV components from attacks sourced from the public internet and cloud;
b. to protect the network from attacks sourced from internally attached NFV components;
c. to protect the NFVI from attacks sourced from internally attached components and the internet.

Inline detection and mitigation functions in the network can be used at the internet edge to prevent volumetric DDoS attacks from the internet, including TCP SYN floods, UDP floods, and DNS floods, which can attack the availability of the network or service.
Threat detection or prevention and response using IDS/IPS shall also be used to effectively defend against or prevent malware and ransomware infections on NFVI and network functions.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T34]

---

68) OSS/BSS Protection:
The contrasting attributes of the legacy and virtualized infrastructures shall be considered from an overall management perspective. This will be particularly important during the migration phase while both types of infrastructure are running

in parallel. The OSS/BSS would, therefore, need to be adapted for near-real time operation and be able to support a hybrid network across SDN/NFV and non-SDN, non-NFV domains.

OSS systems shall be consistent with the ETSI NFV architectural framework and support the Os-Ma interface between the traditional OSS/BSS and the NFV management and orchestration (MANO) framework. OSS/BSS systems shall delegate fine-grained management of the NFV Infrastructure and the specific VNFs to the VIM and the VNFM, which in turn are orchestrated by the NFV orchestrator (NFVO). Thus, the OSS/BSS will be responsible for the high-level configuration of the infrastructure and network functions, but the NFV MANO framework will manage the dynamic aspects of infrastructure and services.

The integration with the SDN controller and applications will follow a similar approach. The OSS will manage the configuration of the SDN data plane, configure and set policies for the SDN controller and control SLAs for SDN applications, but the dynamic control of the SDN forwarding plane will be managed by the SDN controller and the SDN control to data-path interface (CDPI)1. Operators moving to deploy virtualized network architectures based on SDN and NFV are likely to evolve the OSS/BSS systems in stages. Existing operators have a significant installed base and it is unrealistic to replace all existing infrastructure. The new capability will be deployed first where it brings the most value or where the legacy network requires upgrades anyway.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T32

---

69) Redundancy and Back up:

Recovery

The system shall be deployed in such a way as to provide isolation and redundancy to increase the resiliency and defense against a single point of failure.

There are a variety of ways operators shall consider redundancy. Below are three ways the operator shall be thinking about redundancy when it comes to its recovery plan.

a. Network redundancy: network redundancy is the process of adding additional instances of network devices and lines of communication to help ensure network availability and decrease the risk of failure along the critical data path. Having redundancy by providing additional pathways through your

network via redundant routers or switches would ensure minimal downtime and complete continuity of NFV services.

b. Power redundancy: backup power supply (a generator, for instance) that specifically keeps critical NFV hardware running in colocation facilities.
c. Geographic redundancy: geographic redundancy is important for how sensitive data is backed up. Having a redundant backup in an entirely different location will allow quicker recovery with little downtime.
d. The recovery plan shall already identify a fail-over location for the NFV system in the event that the current location is inoperable.

Backup

Backups is the process of creating and storing copies of NFV data to protect against data loss. A backup involves duplicating important data like VNF code and data, configurations, cryptographic materials, network configurations, audit logs or anything that the NFV system needs to stay operational.

Regardless of the backup solution chosen, offsite backups are a must across all industries. Operators are required to store backups in a secure location, preferably an off-site facility, such as an alternate or backup site.

Having both backups and redundancy contributes to the NFV system running smoothly. Backups make sure that if something is lost, corrupted or stolen then a copy of the sensitive NFV data is available. Redundancy makes sure that if something fails, the NFV system is able to work regardless of the problem.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T30]

Common Security Requirements related to 3GPP (4G/5G) Network Functions:

70) Establishment of trust domains for Network Functions: The trust domains of 3GPP network functions shall be identified. Security policies shall be applied depending on those trust domains. The system shall manage each trust domain separately. The system shall manage (e.g., define, enforce) the security policies for each trust domain independently.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.2]

---

71) Confidentiality of sensitive data: The sensitive information of a virtualized 3GPP NF is not exposed through the virtualization layer. The system shall manage (e.g., define, enforce) the permission control at the virtualization layer between NFs and/or sub-NFs.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.3]

---

72) Availability of Network Functions: Virtualized 3GPP NFs, particularly those which are critical to the operation and security of the network, will have access to the required resources for their availability or functionality when sharing resources with other VNFs.
The system shall manage the utilization, traffic distribution, and overload control of the NFs and sub-NFs to ensure availability for key network processes.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.4]

---

73) Common Software Environment: The software vulnerability in one virtualized 3GPP NF does not affect other virtualized 3GPP NFs using the same software platform. Network interfaces shall be locked down so that they only accept a restricted number of expected protocols. Network management shall be secured and shall only be allowed from authorized devices and/or networks. Multi-factor authentication shall be used to log into administrator accounts.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.5]

---

74) Data Location and Lifecycle: The privacy sensitive information of a virtualized 3GPP NF is protected from being leaked out of its legal jurisdiction.

The sensitive information of a virtualized 3GPP NF is protected during its lifecycle process to avoid leakage of the information to other VNFs reusing the storage resource. All privacy sensitive data shall be encrypted when at rest and when in transit. Security policy which restricts where certain types of data can reside shall be defined and implemented by TSPs.

When VNF moves from one host to another or when VNF is terminated, the system shall ensure that resources, privacy sensitive data, and/or keys are fully cleared.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.6]

---

75) Function Isolation: The virtualization platform prevents one function from inspecting the memory of other functions.
Delegated administrator roles shall be used, with roles which could give a user or administrator the ability to inspect the memory of functions only used in exceptional circumstances
The system shall manage reference point-based security and service-based security between VNF functional "boxes".
Confidentiality protection shall be provided to protect information traveling between memory locations in a single or multiple logical memory block.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.7]

---

76) Test Isolation and Assurance: Security assurance testing of a virtualized 3GPP NF needs to be performed using a standardized NFVI environment used to test all VNFs. When testing security assurance of a virtualized 3GPP NF, the scope of testing shall be clarified, including defining the pre-conditions of the virtualized test environment/platform and defining assumptions made in the process. Where possible recreate these assumptions in the product deployment e.g. close ports which do not need to be open.
Both positive and common vulnerability testing (e.g negative testing) shall be carried out against virtualized 3GPP NF and the underlying virtualization and hardware layers. This is required to mitigate the increased attack surface which was partly addressed by physical security assurance protections in physical networks.
Virtualized 3GPP NFs shall be checked regularly to see if they are using out-of-date or insecure versions of a library and these libraries shall be updated if and when possible. This is required to mitigate the increased attack surface which was partly addressed by physical security assurance protections in physical networks.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.9]

---

77) Trust domain and Slice Isolation: The 5GC shall be configured so that NFs can only communicate with NFs which they have a valid reason to communicate with. The default shall be that functions are not able to communicate.

Delegated administrator roles shall be used and shall only give the user or administrator the minimum necessary privileges. The system shall manage slice isolation, security domains and trust domains.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.10]

---

78) Single Administrator Domain: In general, delegated administrator roles shall be used. The global administrator role shall only be used in exceptional cases, e.g. to add permissions for other high-level administrators
The highest security controls shall be applied to use of the global administrator role. In particular, all use of this role shall be logged and audited.
An alert shall be raised in the global administrator role is used, or if any account attempts a function, it is not meant to attempt.
All administration and management shall only be permitted from known, attested devices and multi-factor authentication shall be enforced.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.11]

---

79) Keys and Confidential Data: It shall be possible to deploy a VNF to a host that provides specific security resources (e.g. HMEE, secure compute, secure memory) in order to bind a VNF to a specific host or group of hosts.
Binding shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.
The system shall manage (e.g., assign/log bindings) key storage and confidential data in a manner that provides protection against data compromise.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.12]

---

80) Virtual Network Function Locations: It shall be possible to deploy a VNF to a host that provides specific security resources (e.g. HMEE, secure compute, secure memory) in order to bind a VNF to a specific host or group of hosts.
These controls shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated. The system shall manage the physical location of the VNFs

and sub-components and SDN routing to provide the attestation that the VNF/sub-components provided a commensurate level of security to match the requirements of the service or to meet legal/regulatory requirements.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.13]

---

81) Attestation at 3GPP Function level: It shall be possible to attest a virtualized 3GPP NF through the full attestation chain from the hardware layer through the virtualization layer to the VNF layer.
Attestation of a platform's integrity shall be linked to the application layer and possible for other functions to query. If platform attestation fails the virtualized 3GPP NF shall not be allowed to run.
Attestation of the VNF shall be performed prior to deployment/network integration and during operations.
Attestation of the VNF shall be done at the hardware, virtualization, and NF layers. The solution is inside and outside 3GPP.The system shall manage VNF attestation.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.14]

---

82) Encrypted Data Processing: Sensitive data shall only be decrypted or handled in an unencrypted format in VNFs on trusted and well-known hosts
It shall be possible to control whether untrusted or lower trusted VNFs are allowed to run on the same host as VNFs in a higher trust domain.
It shall be possible to further restrict VNFs on a single host depending on whether they handle decrypted sensitive data.
These controls shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.
The system shall prevent and detect unauthorized or unintended data manipulation and leakage (e.g., modification of VNF images, instantiating parallel VM(s) on same physical CPU).

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

---

83) Mixed Virtual and Legacy PNF Deployments: The 5GC shall be configured so that NFs can only communicate with NFs which they are specifically authorized to communicate with. These rules shall be applied irrespective of whether the NF is a PNF or a VNF. The default shall be for two NFs not to trust one another and to block communication.
The security policies enforced by the system shall complement each other in order to protect mixed PNF-VNF deployments.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.17]

---

84)Software Catalogue Image Exposure: The software package and the artefacts within the package of a virtualized 3GPP NF shall be integrity protected by the vendor's signature.
The software package and the artefacts within the package of a virtualized 3GPP NF and the software catalogue holding its image shall be integrity protected after its onboarding.
The software package and the artefacts within the package of a virtualized 3GPP NF containing sensitive information shall support confidentiality protection.
Software package and artefacts within the package of a virtualized 3GPP NF shall be bound to a specific network after onboarding, such that unauthorized software cannot be instantiated even if it has valid vendor certificate.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.18]

---

85)IP layer vs Application layer Security : The security mechanisms in upper layers higher than the common virtualization platform layer (e.g. hypervisor) can provide virtualized 3GPP NFs the same protection as in physical NFs.

The system shall be able to communicate security policies to the hypervisor(s) to protect NF resource selection.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.24]

---

86)Secure Management APIs:

Requirement:
The system shall be able to support a single 3GPP-defined security level, for all APIs (including the 3GPP layer, NFV layer, and NFVI layer) within a 3GPP network.

The system shall be able to support 3GPP-defined API access restrictions for specific NFs, NF components, and network slices.

[Reference 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.29]

Part II (A)Virtual Machine

This part presents the Virtual Machine specific security requirements.

1) GVNP Life Cycle Management Security

Requirement:

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

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

---

2)Secure executive environment provision

Requirement:

The VNF shall support comparing the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF can query the parsed resource state by the VNFM from the OAM. The VNF shall send an alarm to the OAM if the two resource states are inconsistent. This comparing process can be triggered periodically by the VNF, or the administrator can manually trigger the VNF to perform the comparing process.

[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.2]

---

3) Instantiating VNF from trusted VNF image

Requirement:

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

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

---

4)Traffic separation

Requirement:
The virtualized network product shall support logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains.
[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.8.5.1]

---

5)Inter-VNF and intra-VNF Traffic Separation

Requirement:

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

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

---

6) security functional requirements on virtualization resource management

Requirement:

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

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

---

7)Secure executive environment creation

Requirement:

When an attacker tampers a driver which provided by the hardware and used to create the executive environment, the virtualization layer shall alert the driver error to the administrator for checking the error and finding the attack at latter.

[Reference: 3GPP TS 33.818 v17.1.0 Section 5.2.5.6.7.3]

---

8)VM escape protection

Requirement:

To defend against the attack that an attacker utilizes a vulnerability of a VNF to attack a virtualization layer and then control the virtualization layer, the virtualization layer shall implement the following requirements: The virtualization shall reject the abnormal access from the VNF (e.g. the VNF accesses the memory which is not allocated to the VNF) and log the attacks.

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.6.7.4]

---

9) Secure hardware resource management

Requirement:
The VIM manages the hardware resource configuration and state information exchange. When the VIM is compromised to change the hardware resource configuration, an alert shall be triggered by the hardware. The administrator can check the alert and find the attack at latter.

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.7.7.2]

---

10) Secure hardware resource management information

Requirement:
When a compromised Virtualization layer tampers the hardware resource configuration which is received from the VIM to result in the configuration error of the hardware, the hardware shall trigger an alert. The administrator can check the alert and find the attack at latter.

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.7.7.3]

---

11) Trusted platform

Requirement:

The host system shall implement a Hardware-Based Root of Trust (HBRT) ((e.g. TPM, HSM)) as Initial Root of Trust. The trust state of the platform shall be measured and a trusted chain shall be built.

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.7.7.4]

---

12) VNF package and VNF image integrity

Requirement:

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

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

---

13) VNF Secure Boot

Requirement:

VNF shall include a secured boot process.

[Reference: 3GPP 33.848-17.1.0 V.0.11.0. Section 5.19]

---

14)Secure crash measures for VMs running on hypervisors

Requirement:

The following clauses must be satisfied:

1)Hypervisors need to ensure that in the event of the crash of a VNF component instance, all file references, hardware pass-through devices, and memory are safe from access by unauthorized entities.
This is expected behavior for most hypervisors.

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

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

3)In the event of a crash, the hypervisor must wipe the local storage that is no longer required. (e.g. the VNF Manager might instruct the Virtualization Infrastructure Manager to request this).

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

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

6) The hypervisor needs to ensure that it is not possible for a newly executing VNF component instance to adopt addresses that were recently used by a crashed instance. Otherwise, the new instance may be able to place itself in a position where it can adopt the privileges associated with a recently crashed instance.

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

---

15) Confidentiality protection of Cloned VM image

Requirement:

If an image contains sensitive information, it musto have confidentiality protection in addition to customary integrity protection and access control. In this case, secure key management is also necessary.

[Reference: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.8]

---

16) Proper image management of VM images must be done

Requirement:

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

1. Small number of images must be kept.
2. Images must be kept updated to avoid known vulnerability exploits.
3. Cryptographic checksum protection must be used to detect unauthorized changes to images and snapshots.
4. Strict control around access, creation and deployment of images/instances must be implemented. Such activities must be recorded for audit purposes.

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

---

17) Memory Introspection

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

Delegated administrator roles shall be used to ensure that administrators do not have the ability to inspect memory of functions except under exceptional circumstances.

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

a) VMs are isolated from each other
b) Applications shall be prevented from accessing each other's memory spaces,
c) VMs shall be prevented from accessing the memory of another VM,
d) Keys used to encrypt the memory shall be kept under hypervisor control,
e) Hypervisors shall not be allowed to write directly to memory,

f) Hypervisors shall not be allowed to bypass normal memory access controls and security within the VNF/VM,
g) Hypervisors shall not be allowed to change data within a 3GPP VNF at run-time.

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

---

18)Unnecessary hypervisor services and virtual hardware must be disabled.

Requirement:

Unused services must be identified and disabled. Disable all hypervisor services such as clipboard- or file-sharing between the guest OS and the host OS unless they are needed. Disconnect unused virtual hardware in each guest OS.

[Reference: ENISA Security Aspects of Virtualization (Feb 2017) HY-05, OS-06]

---

19) Hypervisor boot configuration choice

Requirement:

The hypervisor shall have a boot configuration choice to disallow the use of non-certified drivers.

[Reference: ENISA Security Aspects of Virtualization (Feb 2017), HY-14, Pg-63]

---

20)Hypervisor protection

Requirement:

The hypervisor shall be configured to securely erase the virtual volume disks in the event of application crashes or is intentionally destroyed to prevent it from unauthorized access.

[Reference– NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021), Section-Protection of Data-at-rest]

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T14]

---

21) VM Process Isolation

Requirement:

a) The hardware of the virtualized host shall provide assistance for virtualization for instruction sets and memory management using MMU since the hardware support provides the following security assurances that cannot be guaranteed with purely software-based virtualization:
   • Better memory management controls can prevent attacks such as buffer overflow.
   • The feature for re-mapping of DMA transfers in IOMMU provides better isolation of I/O devices. Further, the feature to directly assign I/O devices to a specific VM and enable direct access to those resources eliminates the need for providing emulated device drivers for that VM, thus reducing the size of trusted code.
   • Guest OS code and hypervisor code execute in different processor modes, providing better isolation.
   • Privilege-level isolation can provide better protection for device access mediation functions, and hardware-based memory protection can provide better VM-level protection.
   • By supporting full virtualization, COTS versions of OSs can allow for easier patching and updating than having to perform the same operations on modified or ported versions of OSs that are the only types that can be run on para-virtualized platforms.
   • Since many features of virtualization are now available in hardware, the size of the hypervisor code will be small, enabling better security attestation and verification.

b) The hypervisor shall have configuration options to specify a guaranteed physical RAM for every VM that requires it, as well as a limit to this value, and a priority value for obtaining the required RAM resource in situations of contention among multiple VMs. Further, the over-commit feature that enables the total configured memory for all VMs to exceed the host physical RAM shall be disabled by default.
c) The hypervisor shall have robust configuration features for provisioning virtual resources to all hosted VMs such that it does not exceed a key physical resource (e.g., number of CPU cores).
d) The hypervisor shall provide features to specify a lower and upper bound for CPU clock cycles needed for every deployed VM as well as a feature to specify a priority

score for each VM to facilitate scheduling in situations of contention for CPU resources from multiple VMs.

Reference: NIST SP 800-125A REV. 1 SECURITY RECOMMENDATIONS FOR SERVER-BASED HYPERVISOR PLATFORMS

---

22) Devices Mediation and Access Control

a) Because of the complexity of emulating a hardware device through software emulation, apart from suffering performance penalties, also increases the size of the TCB especially in situations where the guest OS has native device drivers and the device emulation code runs as a kernel module with the same privilege level as the hypervisor. Hence emulation shall only be used where complexity is manageable (e.g., USB host controller).

   In situations where para-virtualized device drivers are used in VMs, mediation of access to physical devices shall be enabled by running back-end device drivers (which control the physical device attached to the hypervisor host) in a dedicated VM rather than in the hypervisor.

   For situations where VMs need to be given dedicated access to DMA capable devices, the hypervisor platform shall include hardware support in the form of I/O Memory Management Unit (IOMMU) for validating and translating all device access to host memory.

b) It shall be possible to set up an Access Control List (ACL) to restrict the access of each VM process to only the devices assigned to that VM. To enable this, the hypervisor configuration shall support a feature to mark VMs (semantically, a set of tasks) and/or have a feature to specify a whitelist, or list of allowable of devices, for each VM.
c) shall be possible to set resource limits for network bandwidth and I/O bandwidth (e.g., disk read/write speeds) for each VM to prevent denial-of-service (DOS) attacks. Additionally, the proper use of resource limits localizes the impact of a DOS to the VM or the cluster for which the resource limit is defined.

   Reference: NIST SP 800-125A REV. 1 SECURITY RECOMMENDATIONS FOR SERVER-BASED HYPERVISOR PLATFORMS

---

23)Direct Execution of commands from Guest VMs

a) Gold standard must be defined for VMs of all types, and VM Images that do not conform to the standard shall not be allowed to be stored in the VM Image server or library. Images in the VM Image library shall be periodically scanned for outdated OS versions and patches, which could result in a drift from the standard.
b) Every VM Image stored in the image server shall have a digital signature attached to it as a mark of authenticity and integrity, signed using trustworthy, robust cryptographic keys.
c) Permissions for checking into and out of images from the VM Image library shall be enforced through a robust access control mechanism and limited to an authorized set of administrators. In the absence of an access control mechanism, VM image files shall be stored in encrypted devices that can only be opened or closed by a limited set of authorized administrators with passphrases of sufficient complexity.
d) Access to the server storing VM images shall always be through a secure protocol such as Transport Layer Security (TLS).

Reference: NIST SP 800-125A REV. 1 SECURITY RECOMMENDATIONS FOR SERVER-BASED HYPERVISOR PLATFORMS

---

24)VM Lifecycle Management

a) During VM live migration, a secure authentication protocol must be employed; the credentials of the administrator performing the migration are passed only to the destination host; the migration of memory content and processor state takes place over a secure network connection; and a dedicated virtual network segment is used in both source and destination hosts for carrying this traffic.
b) There shall be a mechanism for security monitoring, security policy enforcement of VM operations, and detecting malicious processes running inside VMs and malicious traffic going into and out of a VM. This monitoring and enforcement mechanism forms the foundation for building Anti-Virus (AV) and Intrusion Detection & Prevention System (IDPS) solutions.
c) Solutions for Security Monitoring and security policy enforcement of VMs shall be based outside of VMs and leverage the virtual machine introspection capabilities of the hypervisor. Generally, such solutions involve running a security tool as a Security Virtual Appliance (SVA) in a security-hardened or trusted VM.

d) All anti-malware tools (e.g., virus checkers, firewalls, and IDPS) running in the virtualized host shall have the capability to perform autonomous signature or reference file updates on a periodic basis.

Reference: NIST SP 800-125A REV. 1 SECURITY RECOMMENDATIONS FOR SERVER-BASED HYPERVISOR PLATFORMS

---

25) Management of hypervisor platform

a) VM configuration management tools shall have the capability to compile logs and alert administrators when configuration changes are detected in any VM that is being monitored.
b) The access control solution for VM administration shall have a granular capability, both at the permission assignment level and the object level (i.e., the specification of the target of the permission can be a single VM or any logical grouping of VMs based on function or location). In addition, the ability to deny permission to some specific objects within a VM group (e.g., VMs running workloads of a particular sensitivity level) in spite of having access permission to the VM group shall exist

Reference: NIST SP 800-125A REV. 1 SECURITY RECOMMENDATIONS FOR SERVER-BASED HYPERVISOR PLATFORMS

---

27)Hypervisor Security : The following must be met

a) Install all updates to the hypervisor as they are released by the vendor. Most hypervisors have features that will check for updates automatically and install the updates when found. Centralized patch management solutions can also be used to administer updates.
b) Restrict administrative access to the management interfaces of the hypervisor. Protect all management communication channels using a dedicated management network or the management network communications is authenticated and encrypted using Table 1 of secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only.
c) Synchronize the virtualized infrastructure to a trusted authoritative time server.
d) Disconnect unused physical hardware from the host system. For example, a removable disk drive might be occasionally used for backups, but it shall be

disconnected when not actively being used for backup or restores. Disconnect unused NICs from any network.

e) Disable all hypervisor services such as clipboard- or file-sharing between the guest OS and the host OS unless they are needed. Each of these services can provide a possible attack vector. File sharing can also be an attack vector on systems where more than one guest OS share the same folder with the host OS.
f) Consider using introspection capabilities to monitor the security of each guest OS. If a guest OS is compromised, its security controls may be disabled or reconfigured so as to suppress any signs of compromise. Having security services in the hypervisor permits security monitoring even when the guest OS is compromised.
g) Consider using introspection capabilities to monitor the security of activity occurring between guest OSs. This is particularly important for communications that in a non-virtualized environment were carried over networks and monitored by network security controls (such as network firewalls, security appliances, and network IDPS sensors).
h) Carefully monitor the hypervisor itself for signs of compromise. This includes using self-integrity monitoring capabilities that hypervisors may provide, as well as monitoring and analyzing hypervisor logs on an ongoing basis.

Reference: NIST Special Publication 800-125 Guide to security for full virtualization technologies

---

28)Guest OS Security

a) Follow the recommended practices for managing the physical OS, e.g., time synchronization, log management, authentication, remote access, etc.
b) Install all updates to the guest OS promptly. All modern OSs have features that will automatically check for updates and install them.
c) Back up the virtual drives used by the guest OS on a regular basis, using the same policy for backups as is used for non-virtualized computers in the organization.
d) In each guest OS, disconnect unused virtual hardware. This is particularly important for virtual drives (usually virtual CDs and floppy drives), but is also important for virtual network adapters other than the primary network interface and serial and/or parallel ports.
e) Use separate authentication solutions for each guest OS unless there is a particular reason for two guest OSs to share credentials.
f) Ensure that virtual devices for the guest OS are associated only with the appropriate physical devices on the host system, such as the mappings between virtual and physical NICs.

g) If a guest OS on a hosted virtualization system is compromised, that guest OS can potentially infect other systems on the same hypervisor. The most likely way this can happen is that both systems are sharing disks or clipboards. If such sharing is turned on in two or more guest OSs, and one guest OS is compromised, the administrator of the virtualization system needs to decide how to deal with the potential compromise of other guest OSs. Two strategies for dealing with this situation are:
-Assume that all guest OSs on the same hardware have been compromised. Revert each guest OS to a known-good image that was saved before the compromise.
- Investigate each guest OS for compromise, just as one would during normal scanning for malware. If malware is found, follow the organization's normal security policy.

Reference: NIST Special Publication 800-125 Guide to security for full virtualization technologies Section 4.2

---

29) Security Recommendations for Network Segmentation

a) In environments using virtual switches for network segmentation, it is strongly recommended that distributed virtual switches are used instead of standalone virtual switches for the following reasons: (a) to ensure consistency of configuration across virtualized hosts and reduce chances of configuration errors, and (b) to eliminate constraints on VM migration, since a distributed virtual switch (defined for a particular sensitivity level) by definition spans multiple virtualized hosts.

b) Isolation of the hypervisor's management network using virtual switches needs special configuration. In addition to dedicated virtual switches, the management traffic pathway shall have separate pNICs and separate physical network connections (besides the traffic itself being encrypted). Also, it is preferable that the dedicated virtual switch is a standalone virtual switch (so that it can be configured at the virtualized host level) instead of a distributed virtual switch. This is due to the close dependency between distributed virtual switches and the centralized virtualization management servers. Distributed virtual switches can only be configured using a virtualization management server (requiring high availability for these servers), and in some situations bringing up a virtualization management server may require distributed virtual switch modification.

c) In all VLAN deployments, the switch (physical switch connecting to virtualized host) port configuration shall be VLAN aware – i.e., its configuration shall reflect the VLAN profile of the connected virtualized host.

d) Large data center networks with hundreds of virtualized hosts and thousands of VMs and requiring many segments shall deploy overlay-based virtual networking because of scalability (Large Namespace) and virtual/physical network independence. However, it is highly advisable that the overall traffic generated by overlay-based network segmentation technique (e.g., VXLAN network traffic) is isolated on the physical network using a technique such as VLAN in order to maintain segmentation guarantees.

e) Large overlay-based virtual networking deployments shall always include either centralized or federated SDN controllers using standard protocols for configuration of overlay modules in various hypervisor platforms

Reference: NIST Special Publication 800-125BSecure Virtual Network Configuration for Virtual Machine (VM) Protection

---

30) Security Recommendations for Configuring Network Path Redundancy

a) It is preferable to use pNICs that use different drivers in the NIC team. The failure of one driver will only affect one member of the NIC team, and traffic will keep flowing through the other members.
b) If multiple PCI buses are available in the virtualized host, each pNIC in the NIC team shall be placed on a separate PCI bus. This provides fault tolerance against PCI bus failure in the virtualized host.
c) The network path redundancy created within the virtual network of the virtualized host shall also be extended to the immediate physical network links emanating from the virtualized host. This can be achieved by having the individual members of the NIC team (i.e., the two or more pNICs) connected to different physical switches.

Reference: NIST Special Publication 800-125BSecure Virtual Network Configuration for Virtual Machine (VM) Protection

---

31) Security Recommendations for Firewall Deployment Architecture

a) In virtualized environments with VMs running delay-sensitive applications, virtual firewalls shall be deployed for traffic flow control instead of physical firewalls, because in the latter case, there is latency involved in routing the virtual network traffic outside the virtualized host and back into the virtual network.
b) In virtualized environments with VMs running I/O intensive applications, kernel-based virtual firewalls shall be deployed instead of subnet-level virtual firewalls, since kernel-based virtual firewalls perform packet processing in the kernel of the hypervisor at native hardware speeds.
c) For both subnet-level and kernel-based virtual firewalls, it is preferable if the firewall is integrated with a virtualization management platform rather than being accessible only through a standalone console. The former will enable easier provisioning of uniform firewall rules to multiple firewall instances, thus reducing the chances of configuration errors.
d) For both subnet-level and kernel-based virtual firewalls, it is preferable that the firewall supports rules using higher-level components or abstractions (e.g., security group) in addition to the basic 5-tuple (source/destination IP address, source/destination ports, protocol).

Reference: NIST Special Publication 800-125BSecure Virtual Network Configuration for Virtual Machine (VM) Protection

---

32) Security Recommendations for VM Traffic Monitoring

a) VM traffic monitoring shall be performed for both incoming and outgoing traffic.
b) If traffic visibility is accomplished by setting the promiscuous mode feature, care shall be taken to see that this is activated only for the required VM port group and not for the entire virtual switch.
c) A port mirroring feature that provides choices in destination ports (either the virtual port or uplink port) facilitates the use of network monitoring tools in the physical network which are generally more robust and feature rich compared to VM-based ones.

Reference: NIST Special Publication 800-125BSecure Virtual Network Configuration for Virtual Machine (VM) Protection

---

Part II –(B) Container

This part presents the container specific security requirements.

1)Container Security

Requirement:

Appropriate restrictions on container placement and on the use of container caching shall include:
- user handling containers relative to network management containers within a VNF;
-separation of containers belonging to different NFs on different physical servers;
-special handling of containers implementing interfaces between different trust domains (intra-VNF and inter-VNF).
Security policy which restricts the placement and co-existence of containers belonging to different trust domains shall be defined and implemented by TSPs.

Security policy which restricts which sub-functions within an NF if implemented using containers may be cached within the general unencrypted container cache, or define security protection mechanisms for sensitive containers at rest within the cache, shall be defined and implemented by TSPs.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.26]
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022) BP-T31]

---

2)Container breakout

Requirement:

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

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

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.27]
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022) BP-T31]

---

3)Secrets in NF Container Image

Requirement:

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

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

---

4) Container Platform Integrity

Requirement:
The following best practices shall be implemented to ensure the integrity of the container platform

a) Harden and optimize operating system for running containers:
   Ensure that the node operating system that the container platform runs on is hardened against attacks from the container platform and from within the cloud. Follow best practice guidance on securely configuring the operating system, ensuring that the operating system is stripped down to reduce the attack surface and regularly patched to protect against known vulnerabilities. Consider using an operating system that is optimized for running container workloads. Regularly inspect hosts for exposures, vulnerabilities, and deviations from best practices.
b) Implement an immutable infrastructure and automate the replacement of worker nodes: Maintain services on nodes (virtualized hosts) in the development environment and update the service in the production environment by maintaining a golden (configured and clean) set of worker node images. Build the nodes from a common, hardened image. Replacing rather than updating the nodes in the production environment is key to an immutable infrastructure, which improves security by avoiding configuration drift and inconsistencies in deployed services. Integral to the concept of Infrastructure as Code, an immutable infrastructure enables deployments of pre-configured, grouped resources (compute, network, storage), key to secure automation. Combined with the attestation requirement, an immutable

infrastructure makes it more difficult for attackers to maintain persistence in the container stack.

Maintain a golden (configured and clean) set of worker node images and implement patches and updates on the golden images. Replace running nodes with the golden images when available, rather than patching/updating the nodes while they are in operation.

c) Harden Kubernetes clusters: Use configurations that hardens a K8s cluster against known attacks. Ensure that a container platform's K8s cluster is hardened by following security guidelines and by regularly running kube-bench against the cluster to detect when the cluster falls out of compliance
d) Minimize direct access to worker nodes: Opening up direct access to worker nodes greatly increases the risk of cluster compromise. Minimize this risk by disabling direct access (via SSH or other protocols) and using an agent-based system for node maintenance and troubleshooting.
e) Deploy worker nodes in private subnets unless external access is needed: Worker node subnets shall be on private subnets (no access to the Internet) unless explicitly required (e.g., web server). Exposing worker nodes to the Internet greatly increases the threat and attack surface against the container resources, opening opportunities for cyber actors to compromise the nodes and maliciously manage the container resources.
f) Container placement and orchestration based on container platform integrity
   Container platform information and verified firmware and configuration measurements that are retained within an attestation service can be used for policy enforcement in a variety of use cases. One example is orchestration scheduling. Cloud orchestrators, such as Kubernetes, provide the ability to label worker nodes in their database with key value attributes. The attestation services can publish trust and informational attributes to orchestrator databases for use in workload scheduling decisions. In addition, the orchestration system shall provide visibility into the attestation state of the machines.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

---

5) Launch Time Integrity

Requirement: The following shall be met

Before launching a container, we first ensure that the underlying container platform is still trusted. This verification also includes ensuring that monitoring and other runtime controls and policies are active. For example, a Trusted Execution Environment (TEE) with loadable container-specific policies may be provided and enabled by the platform. With the integrity of the container platform assured, the integrity of each container must be verified before launch. The first step is to assure that the container was loaded from a trusted source, such as a trusted images store.

Finally, the container is launched. At this point, the container's execution will be securely monitored according to the policies specific to the container and container platform. The stack shall be constantly monitored using analytics or other means that provide ongoing proof of the secure state of the stack as containers are launched and terminated.

a) Container encryption/decryption of images on Trusted Platforms

Requirement:

The ability for users to encrypt their workload images can provide at-rest cryptographic isolation to help protect consumer data and intellectual property. When the runtime node service receives the launch request, it can detect that the image is encrypted and make a request to retrieve the decryption key. This request can be passed through an attestation service to a key broker with proof that the platform has been attested. The key broker can then verify the attested platform report and release the key back to the Cloud Service Provider and node runtime services. At that time, the node runtime can decrypt the image and proceed with the normal workload execution. The disk encryption kernel subsystem can provide at-rest encryption for the workload on the platform.

b) It is recommended to consider running containers in TEEs to reduce the attack surface for containers, and to keep the Service providers and malicious insiders outside the Trusted Computing Base.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

---

6) Container Image Hygiene

Requirement:

The following best practices shall be implemented

a) Build images from scratch or create minimal de-fanged images:

Reducing the attack surface of a container image shall be a primary aim when building images. The ideal way to do this is by creating minimal images that are devoid of binaries that can be used to exploit vulnerabilities. As an example, if your container software has a mechanism to create images from scratch, it shall be used. Programming languages can create a static linked binary that can be directly referenced in the container file. Creating containers in this manner ensures that the image consists of only the application, greatly reducing extraneous attack surface.

If unable to build an image from scratch, developers shall still seek to reduce the attack surface inside a container by removing extraneous binaries from the container image. Inspecting container images using an application that allows the developer to see the contents of each image layer. Remove all binaries with setuid and setgid bits, as they can be used to escalate privilege, and consider removing all shells and utilities such as nc and curl that can be used for nefarious purposes.

Third-party software shall also undergo an enterprise security review that includes code inspection, threat modeling, and penetration testing to identify and mitigate risks.

b) Use multi-stage builds

Using multi-stage builds is a way to create minimal images. Oftentimes, multi-stage builds are used to automate parts of the Continuous Integration (CI) cycle. For example, multi-stage builds can be used to lint your source code or perform static code analysis. This affords developers an opportunity to get near immediate feedback instead of waiting for a pipeline to execute. Multi-stage builds are attractive from a security standpoint because they allow you to minimize the size of the final image pushed to your container registry. Container images devoid of build tools and other extraneous binaries improves your security posture by reducing the attack surface of the image.

c) Scan container images for vulnerabilities regularly

Container images can contain binaries and application libraries with vulnerabilities. The best way to safeguard against exploits is by regularly scanning images and quickly mitigating identified vulnerabilities. Additionally, knowing where images with vulnerabilities have been deployed can help forensic efforts when vulnerabilities are exploited.

d) Restrict access to container image repositories

Create policies that restrict development teams to access only to repositories with which each team shall interact.

e) Create a set of curated container images

Rather than allowing developers to create their own images, security administrators can create a set of vetted images providing different application stacks for developers. By doing so, developers can forego learning how to compose container specifications and concentrate on writing code. As changes are merged into a Master, a CI/CD pipeline can

automatically compile the asset, store it in an artifact repository, and copy the artifact into the appropriate image before pushing it to an image repository.

Alternatively, security administrators can create a set of base images from which developers create their own container images. Base images shall be vetted and regularly scanned for vulnerabilities. Additionally, administrators shall ensure that the image was published by a reliable entity such as the developer of a reputable product.

f) Add the USER directive to run as a non-root user

As mentioned in the pod security section, of Part II: Securely Isolate Network Resources of this series, avoid running container as root. While you can configure this as part of the podSpec, it is a good habit to use the USER directive. The USER directive sets the UID to use when running RUN, ENTRYPOINT, or CMD instruction that appears after the USER directive.

g) Lint your container images

Linting can be used to verify that a container image adheres to a set of predefined guidelines, such as the inclusion of the USER directive and image tagging. There are tools and resources available that can help to verify common best practices and administrator defined requirements. Linting can be incorporated into a CI pipeline to reject builds that violate the organization's policy.

h) Use immutable tags with your images

Some image repositories support immutable tags. This forces you to update the image tag on each push to the image repository. This can thwart an attacker from overwriting an image with a malicious version without changing the image's tags. Additionally, it gives you a way to identify an image easily and uniquely.

i) Sign your container images

As an example, Docker adds digests to the image manifest that allow an image's configuration to be hashed and the hash to be used to generate an ID for the image. When image signing is enabled, the container (Docker) engine verifies the manifest's signature of each layer, ensuring that the content was produced from a trusted source and no tampering has occurred. Image signing enhances supply chain security, through the verification of digital signatures. Kubernetes provides a dynamic admission controller to verify that an image has been signed.

j) Update the packages in your container images

You shall update the packages used in container images to ensure you have the most up-to-date and secure packages. As an example, include RUN apt-get update && apt-get upgrade in your Docker files to upgrade the packages in your images. Although upgrading requires you to run as root, this occurs during image build phase. The application doesn't need to run as root. You can install the updates and then switch to a different user with the USER directive. If your base image runs as a non-root user, switch

to root and back; don't solely rely on the maintainers of the base image to install the latest security updates.

Run apt-get clean to delete the installer files from /var/cache/apt/archives/. You can also run rm -rf /var/lib/apt/lists/* after installing packages. This removes the index files or the lists of packages that are available to install.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

---

7)The networking within the cloud shall be securely configured

Requirement:

a) Security groups per cluster shall be created, this will make it easy to achieve network security compliance by running applications with varying network security requirements on shared compute resources.
b) Private networking shall be used for connecting network functions.
c) Default firewall rules or default ACLs shall be configured that determines which outbound or inbound connections are permitted.
d) Service Meshes shall be used to protect node-to-node traffic.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part I: Prevent and Detect Lateral Movement (2021)]

---

8) Securely Isolate Network Resources (Pod Security)

Requirement:

a) Pods with containers configured to run as privileged shall be rejected using the technical controls and policies provided by the container orchestration platform.
b) Containers run as root by default. This could be problematic if an attacker is able to exploit a vulnerability in the application and gain arbitrary execution in the container. So containers shall not allow processes to run as root. The K8s PodSpec shall include a set of fields that will specify the user and/or group to run the application.

Alternatively, the Dockerfile USER directive shall instruct the engine to run the container as a non-root user. Container orchestration platforms provide technical controls and policies to mandate non-root execution.

c) Container orchestration platforms provide technical controls and policies to prevent privilege escalation.
d) Container orchestration platforms provide technical controls and policies to restrict directories used by hostPath and ensure that those directories are read only.
e) Cryptographically isolate critical Containers using TEEs

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part II: Securely Isolate Network Resources, 2021]

---

9)Runtime security

Requirement:

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

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part II: Securely Isolate Network Resources,2021]

---

10)Real-time threat detection and incident response shall be implemented

Requirement:

At boot and runtime, attestation technology can verify configuration policy and container metrics (e.g., hash of files, time to execute a module). Attestation technology takes a snapshot of current configurations or metrics, digitally signing that evidence. The evidence is verified against a protected set of expected policies and measurements. The Trusted Platform Module (TPM) or equivalent platform (or infrastructure) may serve as the Root of Trust or a hand-off to a TEE. Attestations can be performed against configuration settings individually or in groups. This method of attestation enables an allow-list approach centered on expected behaviors rather than a deny-list approach that leaves gaps.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part II: Securely Isolate Network Resources,2021]

---

11)Good container security hygiene shall be used to avoid contention and DoS

Requirement:

PodSpec shall be used to set limits to help minimize resource contention and mitigate the risk arising from poorly written or compromised applications that consume an excessive number of resources. Also setting a resource quota or creating a limit range can force the use of limits on a namespace.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part II: Securely Isolate Network Resources, 2021]

---

12) Incident response

Requirement:

The ability to react quickly to an incident can help minimize the damage caused by a breach. There shall be a reliable alert system that warns of suspicious behavior. When an incident does arise, the offending pod shall be identified and isolated for forensic investigation and root cause analysis. Responses shall minimally include:
- Pod with a network policy that denies all ingress and egress traffic to the Pod shall be isolated.
- The worker node shall be cordoned off.
- Impacted worker nodes shall enable termination protection.
- Volatile artifacts on the worker node shall be captured.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part II: Securely Isolate Network Resources,2021]

---

13) Software Catalogue Image Exposure

Requirement:

a) The software package and the artefacts within the package of a virtualized NF shall be integrity protected by the vendor's signature.
b) The software package and the artefacts within the package of a virtualized NF and the software catalogue holding its image shall be integrity protected after its onboarding.
c) The software package and the artefacts within the package of a virtualized NF containing sensitive information shall support confidentiality protection.
d) Software package and artefacts within the package of a virtualized NF shall be bound to a specific network after onboarding, such that unauthorized software cannot be instantiated even if it has valid vendor certificate.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.18]
[Reference: ETSI NFV-SEC021v2.6.1 VNF - GS, Section 5.1]

---

14)Container Image related

A) Image vulnerabilities: Organizations shall use tools that take the pipeline-based build approach and immutable nature of containers and images into their design to provide more actionable and reliable results . Key aspects of effective tools and processes include

1. Integration with the entire lifecycle of images, from the beginning of the build process, to whatever registries the organization is using, to runtime.

2. Visibility shall be centralized across the organization and provide flexible reporting and monitoring views aligned with organizations' business processes.

3. organizations shall be able to create "quality gates" at each stage of the build and deployment process to ensure that only images that meet the organization's vulnerability and configuration policies are allowed to progress.

B) Image Configuration:

1)Images shall be configured to run as non-privileged users.

2)All remote management of containers shall be done through the container runtime APIs which may be accessed via orchestration tools.

C) Embedded Secrets: Secrets shall be stored outside of images and provided dynamically at runtime as needed.

[Reference: NIST Special Publication 800-190 (September 2017)]

---

15)Registry Related

Requirement: The following shall be met

a) Insecure connections to registries: Organizations shall configure their development tools, orchestrators, and container runtimes to only connect to registries over encrypted channels. All data pushed to and pulled from a registry shall occur between trusted endpoints and shall be encrypted in transit.
b) Stale images in registries: The use of stale image shall be prevented
c) Insufficient authentication and authorization restrictions: All access to registries that contain proprietary or sensitive images shall require authentication. Any write access to a registry shall require authentication to ensure that only images from trusted entities can be added to it.

[Reference: NIST Special Publication 800-190 (September 2017)]

---

16) Orchestrator Related

Requirement: The following shall be met

a) Unbounded administrative access: orchestrators shall use a least privilege access model in which users are only granted the ability to perform the specific actions on the specific hosts, containers, and images their job roles require
b) Unauthorized access: Access to cluster-wide administrative accounts shall be tightly controlled as these accounts provide ability to affect all resources in the environment. Organizations shall use strong authentication methods, such as requiring multifactor authentication.
c) Poorly separated inter-container network traffic: Orchestrators shall be configured to separate network traffic into discrete virtual networks by sensitivity level.
d) Mixing of workload sensitivity levels: Orchestrators shall be configured to isolate deployments to specific sets of hosts by sensitivity levels. The best practice could be

to group containers together by relative sensitivity and to ensure that a given host kernel only runs containers of a single sensitivity level.

e) Orchestrator node trust: Orchestrators shall ensure that nodes are securely introduced to the cluster, have a persistent identity throughout their lifecycle, and can also provide an accurate inventory of nodes and their connectivity states.

[Reference: NIST Special Publication 800-190 (September 2017)]

---

17)Container related

Requirement: The following must be satisfied

a) Vulnerabilities within the runtime software: The container runtime must be carefully monitored for vulnerabilities, and when problems are detected, they must be remediated quickly
b) Unbounded network access from containers: Organizations shall use a combination of existing network level devices and more app-aware network filtering. App-aware tools shall be able to not just see the inter-container traffic, but also to dynamically generate the rules used to filter this traffic based on the specific characteristics of the apps running in the containers.
c) Insecure container runtime configurations: Organizations shall automate compliance with container runtime configuration standards. Organizations shall ensure that containers are run with the default profiles provided by their runtime and shall consider using additional profiles for high-risk apps.
d) App vulnerabilities: Organizations shall implement additional tools that are container aware and designed to operate at the scale and change rate typically seen with containers. These tools shall be able to automatically profile containerized apps using behavioral learning and build security profiles for them to minimize human interaction
e) Rogue containers: Separate environments for development, test, production, and other scenarios, each with specific controls to provide role-based access control for container deployment and management activities shall be used. All container creation shall be associated with individual user identities and logged to provide a clear audit trail of activity

[Reference: NIST Special Publication 800-190 (September 2017)]

---

18)Host OS related

Requirement:

a) Organizations shall use container-specific OS which is read only OS with other services disabled. If not possible, measures must be taken to reduce attack surface.
b) Shared kernel: Container workload shall be grouped onto host by its sensitivity level. Also, organizations shall not mix containerized and non-containerized workloads on the same host instance.
c) Host OS component vulnerabilities: Organizations shall implement management practices and tools to validate the versioning of components provided for base OS management and functionality. Organizations shall use tools provided by the OS vendor or other trusted organizations to regularly check for and apply updates to all software components used within the OS. The OS shall be kept up to date not only with security updates, but also the latest component updates recommended by the vendor. Host OSs shall be operated in an immutable manner with no data or state stored uniquely and persistently on the host and no application-level dependencies provided by the host. Instead, all app components and dependencies shall be packaged and deployed in containers.
d) Improper user access rights: All authentication to the OS shall have feature of audit, login anomalies shall be monitored, and any escalation to perform privileged operations shall be logged.
e) Host file system tampering: Ensure that containers are run with the minimal set of file system permissions required. In no case shall containers be able to mount sensitive directories on a host's file system, especially those containing configuration settings for the operating system.
f) To allow defense in depth, it is recommended to not allow disparate data sensitive workloads to be run on the same OS kernel.

[Reference: NIST Special Publication 800-190 (September 2017)]

---

19)Build Pipeline:
Continuous Integration (CI) servers shall be isolated and restricted to projects of a similar security classification or sensitivity. Infrastructure builds which require elevated privileges shall run on separate dedicated CI servers. Build policies shall be enforced in the CI pipeline and by the orchestrator's admission controllers.

Supply chain tools can gather and sign build pipeline metadata. Later stages can then verify the signatures to validate that the prerequisite pipeline stages have run.
It shall be ensured that the CI and Continuous Delivery (CD) infrastructure is as secure as possible

CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0

---

20)Container Application Manifest Scanning

Application manifests describe the configurations required for the deployment of containerized applications. It is vital to scan application manifests in the CI/CD pipeline to identify configurations that could potentially result in an insecure deployment posture.

CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0

---

21)Dynamic Analysis shall be carried out

Dynamic analysis of deployed infrastructure may include detecting Role-based Access Control (RBAC) and IAM configuration drift, validating the expected network attack surface, and ensuring that a SOC can detect unusual behavior in dedicated test environments to configure alerting for production. Dynamic analysis is considered to be a part of testing; however, it is expected to occur in a non-production runtime environment.

CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0

---

22)Container image authorization shall be implemented
When container image encryption is coupled with key management and runtime environment attestation and/or authorization and credential distribution, it is possible to require that a container image can only run on particular platforms. Container image authorization is useful for compliance use cases such as geo-fencing or export control and digital rights media management.

CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0

---

23)Resource Requests and Limits shall be implemented
Single misbehaving workload intentionally (e.g., fork bomb attack or cryptocurrency mining) or unintentionally (e.g., reading a large file in memory without input validation, horizontal

autoscaling) can cause exhaustion of node and cluster level resources. Applying different object level resource requests and limits via cgroups helps prevent such a scenario.

24)Audit Log Analysis shall be carried out

Cloud native architectures are capable of generating more granular audit configuration and filtering than traditional legacy systems for workloads. Additionally, the interoperability of cloud native logs allows for advanced filtering to prevent overloads in downstream processing. What is critical here, as with traditional log analysis, is the generation of actionable audit events that correlate/contextualize data from logs into “information” that can drive decision trees/incident response.

Non-compliant violations are detected based on a pre-configured set of rules that filter violations of the organization’s policies. To have the ability to audit actions of entities using the cluster, it is vital to enable API auditing that filters for a specific set of API Groups or verbs that are of interest to a security team or cluster administrators.

Immediate forwarding of logs to a location inaccessible via cluster-level credentials also defeats an attacker’s attempt to cover their tracks by disabling logs or deleting their activity logs. These systems processing alerts shall be periodically tuned for false positives to avoid alert flooding, fatigue, and false negatives after security incidents that were not detected by the system.

25)Control Plane Authentication and Certificate Root of Trust

The orchestrator administrators shall configure all orchestrator control plane components to communicate via mutual authentication and certificate validation with a periodically rotated certificate in addition to existing control plane hardening.

The Issuing Certificate Authority (CA) can be a default orchestrator CA or an external CA. Using an external CA may involve a non-trivial amount of work in maintaining the Certificate Authority Infrastructure, so this option shall be selected with caution. Particular attention shall be given by the administrators to protect the CA’s private key.

26)Service Mesh shall be implemented
A service mesh provides connectivity between the services that adds additional capabilities like traffic control, service discovery, load balancing, resilience, observability, security, and so on. A service mesh allows microservices to offload these capabilities from application-level libraries and allows developers to focus on differentiating business logic. To effectively ensure secure communications between services in cloud native environments, organizations shall implement a service mesh to eliminate implicit trust within and across workloads, achieved through data-in-motion encryption.

It is important to note that implementation of a service mesh can help reduce the attack surface of a cloud native deployment, and provide a key framework for building zero trust application networks.

27)Storage Cloud Native Storage covers a broad set of technologies that are bucketed into presented storage and accessed storage. Presented storage is storage made available to workloads such as volumes and includes block stores, file systems and shared file systems. Access storage is storage that is accessed via an application API, and includes object stores, key value stores, and databases.
Storage systems contain a data access interface that defines how applications or workloads store or consume data that is persisted by the storage system or service. This interface can be protected by access controls, authentication, authorization, and potentially encryption in transit.
Storage systems also contain a control plane / management interface which is typically an API protected by authentication and TLS, although finer grained access may be available. In general, the control interface is only accessed via a service account by an orchestrator or service broker.

CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0

28)DDoS Attack Prevention:
A distributed denial-of-service attack (DDoS attack) typically involves a high volume of incoming traffic flooding the cloud native application services or the upstream networks to which they depend. Typically, the attack is mounted from many sources. Volumetric attacks are mitigated by detecting and deflecting the attacks before they reach the cloud native application.

29)Threat Intelligence:
Threat intelligence in cloud native systems would make use of indicators observed on a network or host such as IP addresses, domain names, URLs, and file hashes which can be used to assist in the identification of threats. Behavioral indicators, such as threat actor tactics, techniques, and procedures can also be used to identify threat actor activity in cloud native components. The MITRE ATT&CK framework can be leveraged as a starting point for establishing and validating threat activity.

CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0

30)Least Privilege:
Mandatory Access Control (MAC) implementations (e.g. SELinux and AppArmor) can limit the privileges beyond those set to the container or namespace.

Additionally, they provide container isolation at the host level to prevent container breakout or pivoting from one container to another, to escalate privileges beyond those permitted by the access control in place.

CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0

Part III-SDN

This part presents the SDN specific security requirements.

1)Mutual authentication within SDN

Requirement:

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

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

---

2)Centralized Log Auditing

Requirement:

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

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

---

3) Software compliance and integrity preservation
Requirement:

A software checksum (hash or signature) shall be created by the vendor during SDN Controller software compilation that can be validated with a corresponding checksum created during any testing and validation process operated by the operator or a third party.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T10]

---

4) OS hardening

Requirement:

The OS of SDN elements shall be hardened to allow only the minimum services and processes necessary to operate and all other services shall be removed by default.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-P12]

---

5)Host Security

Requirement:

SDN elements shall be hosted on secure server.

---

6)SDN controller and associated SDN communications

Requirement:

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

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

---

7)Prevent attacks via forwarding plane

Requirement:

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

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

---

8)Prevent attacks via control network

Requirement:

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

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

---

9) Prevent attacks via SDN controller's Application Control Interface

Requirement:

There shall be mechanisms to mitigate attacks via the SDN Controller's Application Control Interface such as
- TLS 1.2 or higher shall be used to secure northbound communications and secure controller management.
-Secure coding practices for all northbound applications requesting SDN resources shall be used.
The SDN systems shall be configured to validate flows in network device tables against controller policy.

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

---

10)Prevent attacks via virtualized environment

Requirement:

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

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

---

11) Northbound Applications

Requirement:

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

---

12) SDN security management

Requirement:

a) The controls below shall be applied if message bus technology for communication between SDN elements is used.
   i) A strong mechanism to authenticate the integrity of messages must be deployed between the 'publisher' and 'producer' over the message bus.
   ii) No messages shall be accepted or processed by the message broker or 'consumer' systems from unknown, 'fake' or unauthenticated users.
   iii) The communications shall be secured using TLS 1.2 and above security or certificates where supported (e.g. Kafka).
   iv) The message bus shall be monitored for any unauthenticated messages or 'fake' or default usernames and a security alarm raised for investigation.

b) The security functionality shall be deployed that identifies potential attacks on any SDN elements. Any security functionality shall provide automated alarms and the ability to change the network or element configuration to mitigate the attack.
c) A high availability architecture shall be implemented for key SDN components (e.g. SDN Controllers) to ensure operational service is maintained. The design shall include primary and secondary IP links with, where possible, diverse routing to allow for single point of network failure.
d) Any changes to network, service and virtual environments shall be restricted to the orchestrator. The SDN Controller and the VNFM and VIM shall have additional controls applied to them to restrict such access for normal operation. Restricting the

SDN Controller and the VNFM and VIM will prevent the application of rules and changes that may break policy and rules during deployment of service templates.

e) For operational emergencies, a high-level administration account shall be created and stored in a safe physical location and such an account must not be available to support engineers or used during normal operations.
f) The orchestration layer and SDN must be architected so that SDN networks and NFV environments are not operationally dependent on the orchestration or MANO layer to maintain operating services under circumstances that may render the orchestration platform unavailable.

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

Part IV MANO

This part presents the MANO specific security requirements.

1)Authorized access to MANO

Requirement:

Access to the MANO shall be restricted to a limited number of administrators.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.19]
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP T8]

---

2)Instantiation of MANO components

Requirement:

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

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

---

3)Identity verification shall be done at the Receiver end in MANO Architecture

Requirement:

Relying parties shall not allow any actions from received data before successfully identifying and verifying the location of the relied upon party. The possible countermeasure is to deply the multi-attribute authentication and authorization schemes.

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

4)Monitoring in VIM

Requirement:

The VIM shall monitor stored images to determine if any unauthorized modification, deletion or insertion has occurred. The requirement calls for proof of integrity of the data stores used for VM images and when combined with the data transfer integrity services.

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

5)Message handling in MANO

Requirement:

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

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

6)Data Transfer in MANO

Requirement:

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

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

7)Identity verification in MANO

Requirement:

The receiving party shall not allow any actions from received data before successfully identifying and verifying the identity and location of the transmitting party. This requirement shall eliminate most elements of masquerade and when placed alongside access control schemes shall also eliminate most forms of privilege escalation.

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

---

8)The client and authorization servers shall mutually authenticate

Requirement:

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

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

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T23, BP-P1]

---

9)Authentication of the Request Originator

Requirement:

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

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

---

10)Requirements for client credentials

Requirement:

- The client credentials shall be stored in a secure and tamper-resistant location or stored encrypted with the key protected in a tamper-resistant location.

- The client credentials shall be generated with a minimum of 128 bits of entropy, using best practices for entropy sources, in order to mitigate the risk of guessing attacks.
- The client credentials shall not be included in the source code and software packages.
- The client credentials shall be installed in the client in a secure way, eliminating any possibility of gaining access to these credentials during installation.
- The client credentials shall be possible for the authorization server to revoke the client credentials.

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

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T23]

---

11)Access Token shall be signed

Requirement:

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

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

---

12)Format of Access Token

Requirement:

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

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

---

13)Access tokens shall have limited lifetimes

Requirement:

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

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

---

14)Access tokens shall be restricted to a particular number of operations

Requirement:

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

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

---

15)Access token shall be bound to the intended resource server.

Requirement:

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

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

---

16)Tokens shall be bound to the client ID

Requirement:

The access token shall include a claim for the NF Instance Id of the Service Consumer (subject) which is the "Client ID."

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

---

17)Token Revocation

Requirement:

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

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

---

18)Orchestrator node trust

Orchestration platforms shall be configured to provide features that create a secure environment for all the apps they run. Orchestrators shall ensure that nodes are securely introduced to the cluster, have a persistent identity throughout their lifecycle, and can also provide an accurate inventory of nodes and their connectivity states. Organizations shall ensure that orchestration platforms are designed specifically to be resilient to compromise of individual nodes without compromising the overall security of the cluster. A compromised node must be able to be isolated and removed from the cluster without disrupting or degrading overall cluster operations. Finally, organizations shall choose orchestrators that provide mutually authenticated network connections between cluster members and end-to-end encryption of intra-cluster traffic.

[Reference: NIST Special Publication 800-190 [September 2017]

---

19)Internal Health Checks in MANO Functions

Requirement:

MANO functions shall include internal health checks to detect potential intrusion and take protective action.

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

---

20)Logging in MANO

Requirement:

The receiver of a message shall be able to determine if any of modification, deletion, insertion, or replay has occurred. This requirement provides for a closed loop message and session integrity service.

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

---

21) MANO Access Control and Management

Requirement:

a) The MANO components shall support a high-level of role granularity to ensure appropriate levels of privilege can be assigned to all users to protect key processes and the integrity of data.
b) All OAM access shall be controlled through a centralized single sign-on or PAM solution with all access (success and failure) recorded in the audit log mechanism. Multi-factor authentication shall be used to log into administrator accounts.
c) All administration and management shall only be permitted from known, attested devices and multi-factor authentication shall be enforced.
d) The confidentiality and data integrity of all messages must be ensured, e.g. by using a transport-layer mechanism, such TLS 1.2 and above, on each interface.
e) The authorization server database used to authenticate the user and store associated user credentials, access tokens and refresh tokens must be stored in a tamper resistant location (e.g. HSM).

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T23]

---

22) Security Management and Orchestration

Requirement:
One best practice consists of designing a NFV orchestrator incorporating the security and trust requirements of the NFVI. The orchestration and management of security functions

requires integration by enabling interaction among the security orchestrator, the VNFM, and the element management systems (EMS). This type of protection can be achieved by setting scaling boundaries in the VNFD or network service descriptor (NSD), for example, and having the NFVO enforce these restrictions to protect from attacks such as a DNS amplification attack.

Secure management and administration of the NFVI and NFV-MANO is critical for the security of a virtualized network. The following describe the basic principles for such secure management which shall be met

a) Administration of the NFVI is only available over mutually authenticated, encrypted and integrity protected channels or APIs.

b) All channels or APIs are separated from each other and use separate credentials.

c) The number of privileged accounts for the NFVI is constrained to a minimal manageable number to meet the TSP's needs.

d) NFV-MANO and NFVI administrators do not have any privileged rights to other services within the TSP.

e) NFV-MANO and NFVI administrators are only provided with the privileges and accesses required to carry out their role.

f) NFV-MANO and NFVI administrators do not have access to workloads running within the virtualized environment.

g) NFV-MANO and NFVI administration access is limited to best practice configuration methods (e.g. authorized API calls).

h) Internal components within VNFs are not able to directly connect to entities or management functions outside of the network trust domain, except via interfaces that are explicitly part of the VNF security design.

i) NFV-MANO and NFVI administration is automated wherever possible.

j) Manual administration of the NFVI is by exception and raises a security alert.

k) Functions that manage the administration and security of the NFVI (e.g. MANO) are physically separate and do not run on the same NFVI as the NFs they manage.

l) Functions that support the administration and security of the NFVI are treated as security critical functions.

m) Ensure that there is physical/logical separation of the management network from other networks.

n) Management networks shall not pass through any virtualized Forwarding Functions.

[Reference: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.2]

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T8]

23) Hardware Security

Requirement:

Separate dedicated hardware shall be used to provide independent NFV management (MANO) and service clusters (NFV). In addition, separated clusters shall be used to provide MANO and NFVI.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T16]

---

24)Centralized log auditing

Requirement:

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

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

---

25) VIM connectivity to virtualization layer

Requirement:

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

Additionally, it is advised that any vendor defaults (e.g., self-signed certificates) be removed and replaced with operator generated certificates.

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

---

26)Recovery and reinstallation

Requirement:
Recovery mechanisms in NFV must ensure the following:

The NFVI must be restored completely, with all configurations and settings adjusted correctly. This includes controller nodes pointing to the right set of components, settings reloaded with correct parameters, and full inter-operability restored. Of particular importance is restoring the interoperation between NFV, SDN, and MANO systems, in an automated way, without the need for human intervention to reconfigure these systems to become functional again.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T25]

---

27) Deploying VM/Container of different trust levels

Requirement:

The VIM shall be configured to ensure that VMs or containers of differing trust levels are not deployed on the same physical host or blade and that VMs or containers requiring a 'hardware root of trust' cannot be installed on a physical host or blade that does not fully support trusted boot (e.g., Intel-TXT) and TPM.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T26]

---

28)NFVO Security Management

Requirement:
A mutual authentication mechanism shall exist between the NFVO, VIM and EMS platforms to provide a level of trust and to ensure only the authorized NFVO can make requests to the VIM and EMS platforms and vice versa.
The NFVO shall provide internal workflow rules to prevent accidental changes to the NFVI and NFV services that could have an impact on service delivery.
A mechanism shall exist to provide configuration roll-back in the event of any unauthorized or accidental service changes.

The NFVO shall create and maintain a comprehensive audit log of all service changes including the identity of the user making each change.
The NFVO shall implement robust transaction management for any NFV management for supporting NFVi changes to ensure that the opportunity for configuration integrity errors across the orchestration-controlled elements and service inventory is eliminated.
Best practice for provisioning platform controls for configuration roll-back and failure alarming must be implemented.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T27]

---

29)Redundancy

Requirement:

MANO functions shall include internal health checks to detect potential intrusion and take protective action.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T30]

---

30)Tracking VNF version changes

Requirement:
The orchestration and VNF management systems shall have the ability to keep track of multiple versions, multiple environments, multiple instances and allow the service provider team to perform updates or upgrades with clear expectations of service continuity based on metadata information including component dependencies.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T3]

---

31)VNF deletion or relocation

The NFVO may only relocate or retire a VNF after backup and storage of critical data such as encryption keys or subscriber information to ensure this data is not lost during migration or restructuring of the network. This also applies when a request to relocate or retire a VNF comes from the EMS.

The NFVO may only relocate or retire a VNF after having validated that the security and affinity policies can be and will be applied upon reintroduction of the element either in the same or a new location. This validation must take into account both operator and regulatory requirements.
The NFVO may only relocate or retire a VNF after its operational state is no longer depended upon by other VNFs. In the event of a VNF being attacked or compromised it shall be possible to isolate the VNF from the production environment and restore the VNF to a state prior to the attack.
It shall also be possible to take a snapshot of the affected VNF to allow for security investigation and analysis.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T5]

---

32) Secure hardware resource management

Requirement
The VIM manages the hardware resource configuration and state information exchange. When the VIM is compromised to change the hardware resource configuration, an alert shall be triggered by the hardware. The administrator can check the alert and find the attack later.

[Reference: 3GPP 33.818 v17.1.0 Section 5.2.5.7.7.2]

Annexure-I (Definition)

1. Anti-Spoofing: Anti Spoofing is a technique for identifying and dropping packets that have a false source address
2. Application Programming Interface: This interface can be thought of as a contract of service between two applications
3. Atomic deployable unit: An instance of an atomic deployable unit is represented by a single VM for hypervisor-based virtualization or represented by one or a set of OS containers for CIS (Container Infrastructure Service) based virtualization.
4. Availability: The network availability is the average percentage of time during which the network is performing its intended function.
5. ABAC: Attribute-based access control (ABAC), also known as policy-based access control for IAM, defines an access control paradigm whereby a subject's authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment attributes.
6. Confidentiality: The state of keeping or being kept secret or private.
7. Firewall: A firewall is a network security device that monitors traffic to or from your network.
8. Post-incident analysis: post-incident analysis is the checking of various logged measurements to establish details of the attack, i.e. the mode and method of attack, the time of the attack, the identities or locations of attackers.
9. PNF: Refers to the legacy network appliances on proprietary hardware. Physical Network Function
10. TEE: A Trusted Execution Environment (TEE) is an area in memory protected by the processor in a computing device. Hardware ensures confidentiality and integrity of code and data inside a TEE. The code that runs in the TEE is authorized, attested, and verified.
11. VNF Package: VNF Package is a ZIP file including VNFD, software images for VM, and other artifact resources such as scripts and config files
12. Relying Parties: An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.
13. Hypervisor: A software which acts as a bridge in between the Virtual Machines and the Host machine. It converts all the operations from the Virtual Machines so that they will be executable on the Host Machine CPU.
14. Host path: In Kubernetes, a host Path volume means mounting a file or a directory from the node's host inside the pod.
15. host system: collection of hardware, software and firmware making up the system which executes workloads

16. Virtual Machine: A virtual machine (VM) is an isolated computing environment created by abstracting resources from a physical machine.
17. VM Image: A Virtual Machine Image is a fully configured Virtual Machine used to create a VM for deployment
18. VNF Image: It is a fully configured Network Function which is used to deploy the network function in a virtualized environment.
19. Pods: Pods are the isolated environments used to execute 5G network functions in a 5G container centric or hybrid container/virtual network function design and deployment.
20. Pod Spec: PodSpec includes a set of fields that specify the user and/or group to run the application.
21. Worker nodes: Worker nodes within the Kubernetes cluster are used to run containerized applications and handle networking to ensure that traffic between applications across the cluster and from outside of the cluster can be properly facilitated.
22. syscall : The system call is the fundamental interface between an application and the Linux kernel.
23. hostpath : A Kubernetes hostpath is one of the volumes supported by Kubernetes.
24. Namespace: In Kubernetes, namespaces provide a mechanism for isolating groups of resources within a single cluster.
25. Network Functions Virtualization (NFV): principle of separating network functions from the hardware they run on by using virtual hardware abstraction
26. Network Functions Virtualization Infrastructure (NFVI): totality of all hardware and software components that build up the environment in which VNFs are deployed.
27. Network Functions Virtualization Infrastructure (NFVI) components: NFVI hardware resources that are not field replaceable, but are distinguishable as COTS components at manufacturing time.
28. Network Functions Virtualization Infrastructure Node (NFVI-Node): physical device[s] deployed and managed as a single entity, providing the NFVI Functions required to support the execution environment for VNFs.
29. Network Function Virtualization Infrastructure Point of Presence (NFVI-PoP): N-PoP where a Network Function is or could be deployed as Virtual Network Function (VNF)
30. Network Functions Virtualization Management and Orchestration (NFV-MANO): functions collectively provided by NFVO, VNFM, and VIM
31. Network Functions Virtualization Management and Orchestration Architectural Framework (NFV-MANO Architectural Framework): collection of all functional blocks (including those in NFV-MANO category as well as others that interwork with NFV-MANO), data repositories used by these functional blocks, and reference points and interfaces through which these functional blocks exchange information for the purpose of managing and orchestrating NFV.

32. Network Functions Virtualization Orchestrator (NFVO): functional block that manages the Network Service (NS) lifecycle and coordinates the management of NS lifecycle, VNF lifecycle (supported by the VNFM) and NFVI resources (supported by the VIM) to ensure an optimized allocation of the necessary resources and connectivity
33. Network Interface Controller (NIC): device in a compute node that provides a physical interface with the infrastructure network.
34. Network operator: operator of an electronics communications network or part thereof. An association or organization of such network operators also falls within this category.
35. Network Point of Presence (N-PoP): location where a Network Function is implemented as either a Physical Network Function (PNF) or a Virtual Network Function (VNF)
36. Network Service: composition of Network Function(s) and/or Network Service(s), defined by its functional and behavioral specification.
37. network service orchestration: subset of NFV Orchestrator functions that are responsible for Network Service lifecycle management
38. network service provider: type of Service Provider implementing the Network Service
39. Overlay Networks: A software-defined networking component included in most orchestrators that can be used to isolate communication between applications that share the same physical network
40. Physical Network Function (PNF): implementation of a NF via a tightly coupled software and hardware system
41. Physical Network Function Descriptor (PNFD): template that describes the connectivity requirements of Connection Point(s) attached to a Physical Network Function.
42. Platform: A computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run.
43. Chain of trust: It is used to infer trust in the measurement data of the software component that represents the last link of the chain.
44. Relying Party: An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.
45. Virtual Machine (VM): virtualized computation environment that behaves very much like a physical computer/server
46. virtual network: virtual network routes information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity
47. Virtualized Network Function (VNF): implementation of an NF that can be deployed on a Network Function Virtualization Infrastructure (NFVI)

48. Virtualized Network Function Instance (VNF Instance): run-time instantiation of the VNF software, resulting from completing the instantiation of its components and of the connectivity between them, using the VNF deployment and operational information captured in the VNFD, as well as additional run-time instance-specific information and constraints.
49. Virtualized Network Function Component (VNFC): internal component of a VNF providing a VNF Provider a defined subset of that VNF's functionality, with the main characteristic that a single instance of this component maps 1:1 against a single Virtualization Container
50. workload: component of the NFV architecture that is virtualized in the context of a particular deployment

Annexure-II(Acronyms)

5GC	-	5G Core Network
5GMM	-	5GS Mobility Management
5GS	-	5G System
5GSM	-	5G Session Management
ARP	-	Address Resolution Protocol
AUSF	-	Authentication Server Function
AUTS	-	Authentication failure message with synchronization failure
CIoT	-	Cellular Internet of things
CIS	-	Center for Internet Security
CLI	-	Command Line Interface
CP	-	Control Plane
DAST	-	Dynamic Application Security Testing
DDoS	-	Distributed Denial of Service
DHCP	-	Dynamic Host Configuration Protocol
DL	-	Downlink
EM	-	Element Manager
EPS	-	Evolved Packet Core
EPS	-	Evolved Packet System
EMM	-	Evolved Mobility Management
gNB	-	5G Next Generation base station
GTP-C	-	GPRS Tunneling Protocol Control Plane
GTP-U	-	GPRS Tunneling Protocol User Plane
GUI	-	Graphical User Interface
GUTI	-	Global Unique Temporary Identifier
HBRT	-	Hardware Based Root of Trust
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hypertext Transfer Protocol Secure
IaaC	-	Infrastructure as a Code
ICMP	-	Internet Control Message Protocol
IDE	-	Integrated Development Environment
IE	-	Information Element
IP	-	Internet Protocol
ISO-OSI	-	International organization of Standardization – Open System Interconnection
JSON	-	JavaScript Object Notation
MAC	-	Media access control
MANO	-	Management and Orchestration

NAS	-	Non-Access Stratum
N1A0	-	Null Security Algorithm
NF	-	Network Function
NFV	-	Network Function Virtualization
NFVI	-	Network Functions Virtualization Infrastructure
NFVO	-	Network Function Virtualization Orchestrator
NG	-	Next Generation
ng-eNB	-	Next Generation e-NodeB
NG-RAN	-	Next Generation Radio Access Network
O&M	-	Operations and Maintenance
OAM	-	Operations Administration Maintenance
OS	-	Operating System
OSS/BSS	-	Operation Support System/Business Support System
PDU	-	Protocol Data Unit
PKI	-	Public key infrastructure
PNF	-	Physical Network Function
RAM	-	Random Access Memory
RES	-	Response
RFC	-	Request For Comments
RRC	-	Radio Resource Control
S-NSSAI	-	Single - Network Slice Selection Assistance Information
SAML	-	Security Assertion Markup Language
SAST	-	Static Application Security Testing
SBI	-	Service Based Interfaces
SCA	-	Software Composition Analysis
SDN	-	Software defined networking
SEAF	-	Security Anchor Function
SMT	-	Simultaneous Multithreading
SUCI	-	Subscription Concealed Identifier
TEE	-	Trusted Execution Environment
UE	-	User Equipment
UL	-	Uplink
URL	-	Uniform Resource Locator
UUID	-	Universal Unique Identifier
VIM	-	Virtualized Infrastructure Manager
VM	-	Virtual Machine
VNF	-	Virtual Network Function
VNFD	-	Virtual Network Function Descriptor
VNFM	-	Virtual Network Function Manager

Annexure-III(List of Submissions)

Annexure-IV (References)

1. 3GPP TS 33.818 V17.1.0 (2021-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products (Release 17).
2. 3GPP TR 33.848 V0.11.0 (2022-02) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects; Study on Security Impacts of Virtualization (Release 17).
3. ETSI GS NFV-SEC 001 V1.1.1 (2014-10) "Network Functions Virtualization (NFV); NFV Security; Problem Statement"
4. ETSI GS NFV-SEC 002 V1.1.1 (2015-08) "Network Functions Virtualization (NFV); NFV Security; Cataloguing security features in management software"
5. ETSI GS NFV 003 V1.3.1 (2018-01) Network Functions Virtualization (NFV); Terminology for Main Concepts in NFV.
6. ETSI GS NFV-SEC 006 V1.1.1 (2016-04) Network Functions Virtualization (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns.
7. ETSI GR NFV-SEC 009 V1.2.1 (2017-01) Network Functions Virtualization (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration.
8. ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Network Functions Virtualization (NFV); NFV Security; Report on Retained Data problem statement and requirements.
9. ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Network Functions Virtualization (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components.
10. ETSI GS NFV-SEC 013 V3.1.1 (2017-02) Network Functions Virtualization (NFV) Release 3; Security; Security Management and Monitoring specification
11. ETSI GS NFV-SEC 014 V3.1.1 (2018-04) Network Functions Virtualization (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points.
12. ETSI GR NFV-SEC 018 V1.1.1 (2019-11) Network Functions Virtualization (NFV); Security; Report on NFV Remote Attestation Architecture.
13. ETSI GS NFV-SEC 021 V2.6.1 (2019-06) Network Functions Virtualization (NFV) Release 2; Security; VNF Package Security Specification.
14. ETSI GS NFV-SEC 022 V2.8.1 (2020-06) Network Functions Virtualization (NFV) Release 2; Security; Access Token Specification for API Access.
15. ETSI GS NFV-EVE 005 V1.1.1 (2015-12) Report on SDN Usage in NFV Architectural Framework.

16. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES “Part I: Prevent and Detect Lateral Movement 2021”
17. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES “Part II: Securely Isolate Network Resources”
18. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021)
19. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES (2021) “Part IV: Ensure Integrity of Cloud Infrastructure”
20. NIST Special Publication 800-125B (March 2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection.
21. NIST Special Publication 800-125 Guide to Security for Full Virtualization Technologies.
22. NIST Special Publication 800-190 Application Container Security Guide.
23. ONAP VNF API Security Requirements
24. ENISA Security aspects of virtualization FEBRUARY 2017.
25. ENISA NFV SECURITY IN 5G Challenges and Best Practices FEBRUARY 2022.
26. GSMA NG 133 Cloud Infrastructure Reference Architecture managed by OpenStack v 1.0, Feb 2022.
27. GSMA NG 126 Cloud Infrastructure Reference Model Version 3.0
28. CNCF _cloud-native-security-whitepaper-May2022-v2

-End of Document-