Best Current Practices/ सर्वोत्तम वर्तमान प्रथाएँ (स.व.प्र)

Network Function Virtualization (NFV)

(As applicable to Mobile Generation Technologies)

BCP Number: BCP404042308
BCP Name: NCCS/BCP/Customer Premises Equipment/Mobile Based Equipment/NFV

Date of Release: 28.08.2023 Version: 1.0.1
Date of Enforcement:

जारीकर्ता
Issued by
राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

About NCCS

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

Document History

Sr No .	Title	BCP No.	Version	Date of Release	Remark
1.	Network Function Virtualization (NFV)	BCP404042308	1.0.0	28.08.2023	First release

Table of Contents

Abstract

The purpose of the document is to present the practical and widely considered best practices and recommendations for the security assurance of Network Function Virtualization. The provisions in this document have been developed after reviewing the published standards, recommendations, guidance documents and white papers of various regional/ international standardization bodies viz 3GPP, ETSI, along with the publications of ENISA, NIST, CISA NGMN, GSMA, CNCF. The references indicated against each of the clauses imply that the respective clause has been adopted as it is or with certain modifications.

Scope

This document specifies the best current practices related to the security of NFV Infrastructure (Platform), Virtual Network Functions (both container and Virtual Machine based), Management and Network Orchestration (MANO) and Software Defined Networking (SDN). These best practices are recommended to be followed by all stakeholders i.e Original Equipment Manufacturer, Telecommunication Service Provider, Cloud Service Provider etc.

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.

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.

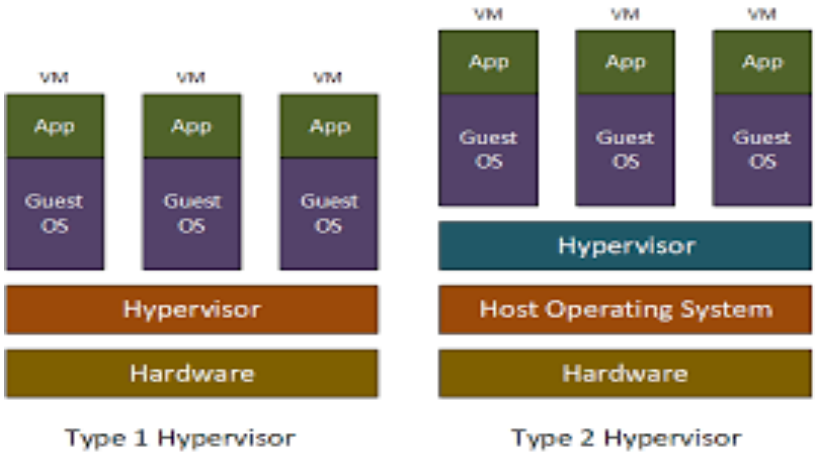

Fig 1 Type 1 and Type 2 Hypervisors

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.

i) 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)

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

iii) 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.

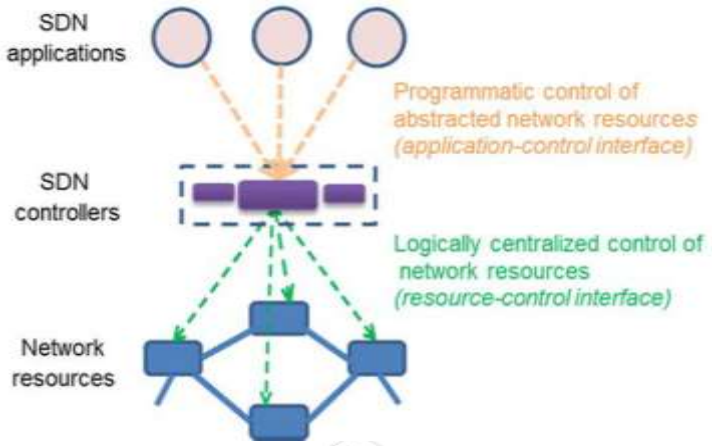

Fig 2 Concept of SDN

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.

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 identifies 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 virtualization of the infrastructure and the life cycle management of VNFs. MANO comprises of the Virtualized Infrastructure Manager (VIM), Virtualized Network Function Manager (VNFM) and NFV Orchestrator (NFVO).

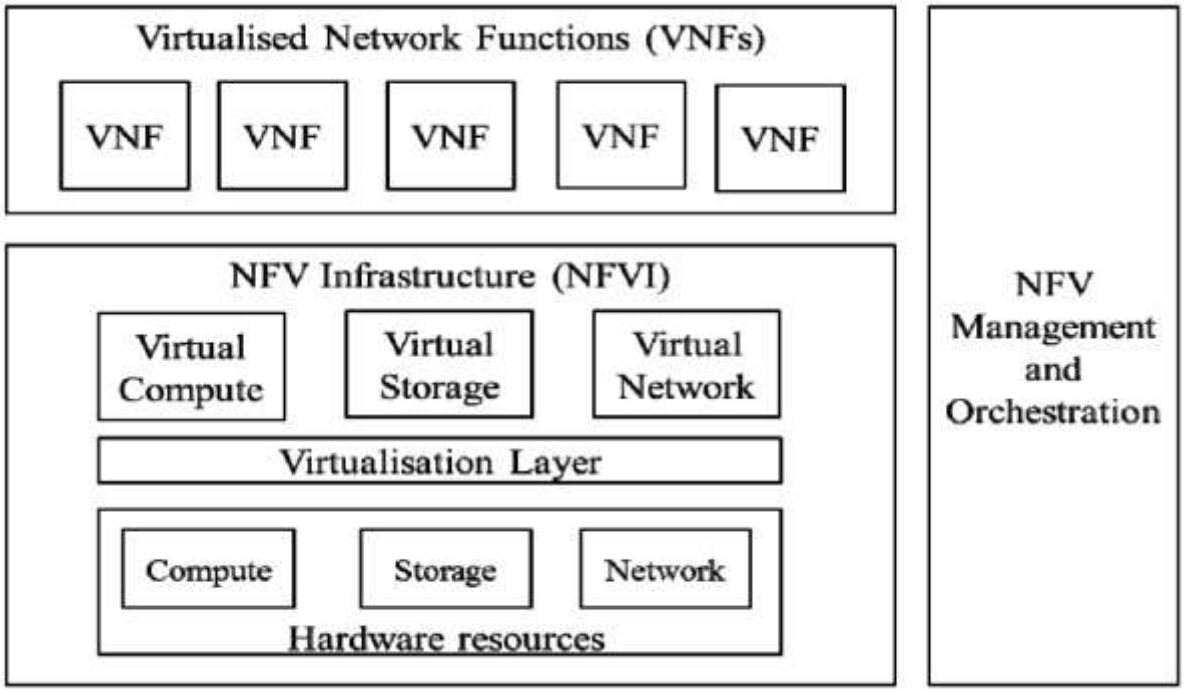

Figure 3 High level NFV Framework

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):** It 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.

1) **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

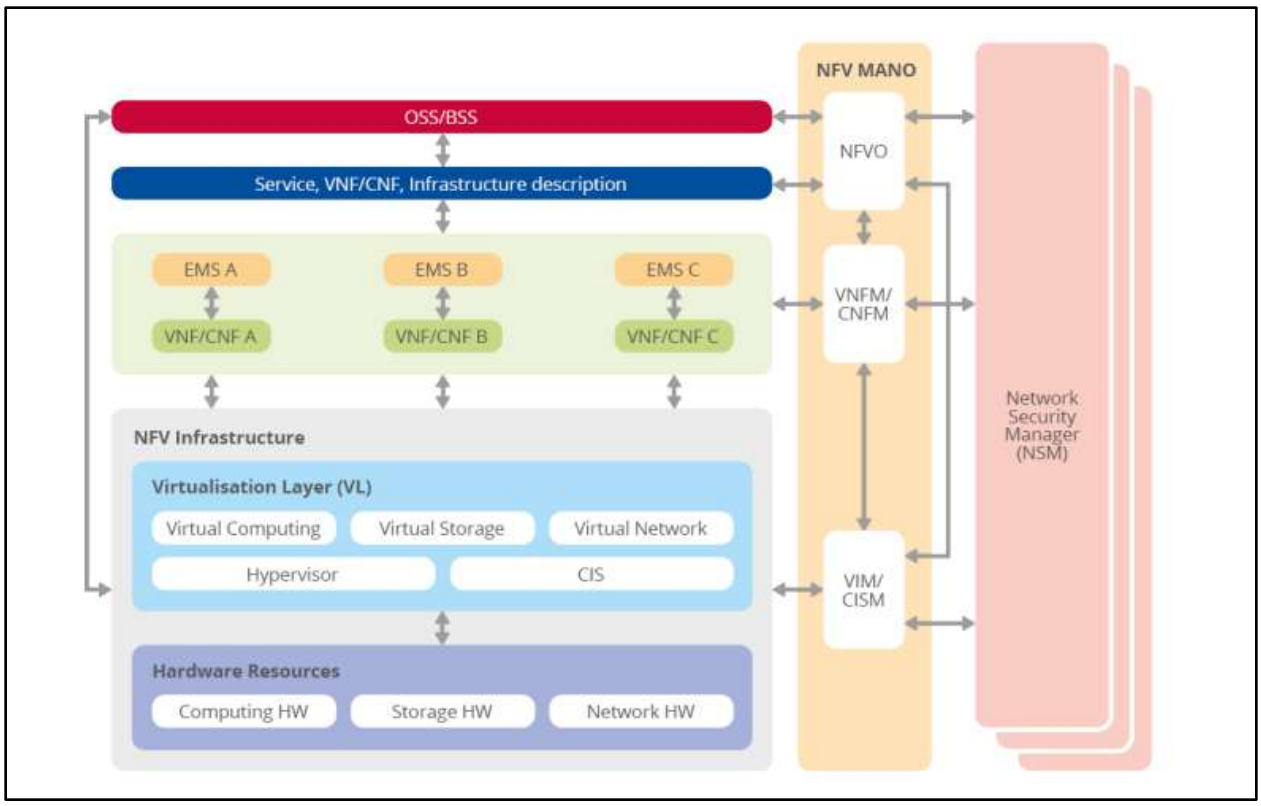

Fig 4 Adapted NFV architecture

Chapter 1 – Common Security Best Practices

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

Section 1: Network Services

1.1.1 Network security

Recommendation:

a) Topology hiding

Topology hiding: In a NFV environment, 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.

b) VLAN and VXLAN zoning

It is recommended that virtualized security appliances may be used in the future in place hardware security appliances to enable protection between zones.

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

1.1.2 Networking Security Zoning

Recommendation:

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 is 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]

1.1.3 Network Interfaces

Recommendation:

Network interfaces should be locked down so that they only accept a restricted number of expected protocols.
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T01]

1.1.4 Security Monitoring and Filtering

Recommendation:
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 should be implemented either within VM/Container or Standalone VM/Container or in the virtualization layer.

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

Section 2: Operating System

1.2.1 Restrictions on running Scripts / Batch-processes

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

1.2.2 Restrictions on Soft-Restart

Recommendation:
The system should 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.

Chapter 2 - Specific Best Practices

Part 1 NFV Infrastructure (Platform)

This part presents the NFV infrastructure(platform) specific security recommendations. NFV infrastructure, here does not include virtualization layer. Kindly refer to Fig 5 below for different security domains

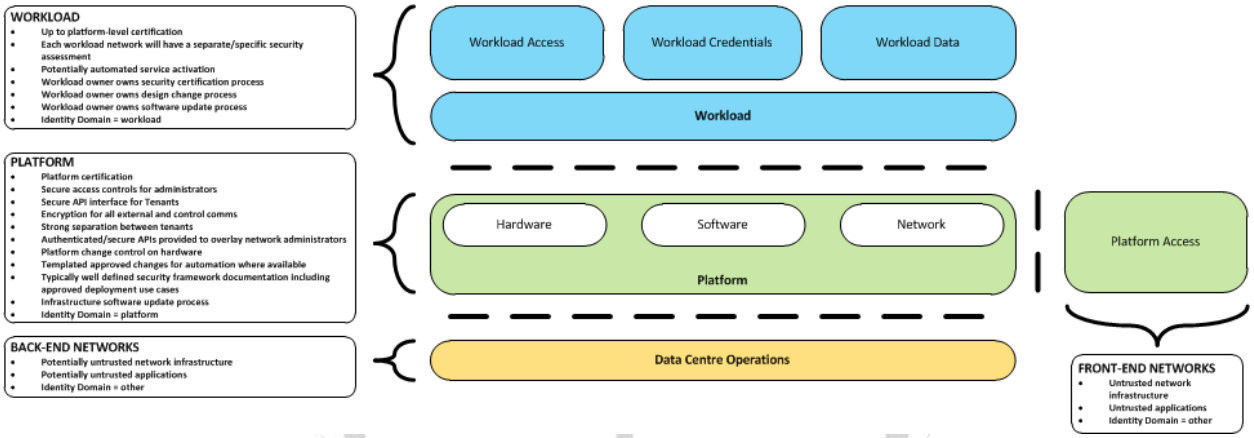

Fig 5 Security Domain

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.

2. 1.1 Regular Updates

Recommendation:

Firmware/UEFI updates should 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]

2.1.2 Hardware security

Recommendation:

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]

2.1.3 Platform Node Integrity

Recommendation:

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, Smart NICs, packet processing chips, crypto off load engines and miscellaneous micro controllers required for operation of the devices. Such firmware should be updated frequently.

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

2.1.4 Local or removable blade storage – SAN protection (applicable if SAN is used)

Recommendation:

SAN storage protection

SAN security (including backup management) should 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]

2.1.5 Entropy and random numbers

Recommendation:

(a) The host system should 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.
(b) The host system should implement a random number generator.

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

2.1.6 Access controls

Recommendation:

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

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

2.1.7 Workload Security

Recommendation:

The Operator should 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]

2.1.8 Audit and Monitoring on cloud infrastructure

Recommendation:

In general, it is a good practice to have the same security monitoring and auditing capabilities in both production and non-production environments. The logs should be regularly monitored for events of interest.

2.1.9 Confidentiality and Integrity protection on Platform

Recommendation:

The following should be considered for Confidentiality and Integrity protection on Platform

a) The platform should support self-encrypting storage devices
b) The monitoring system must not affect data confidentiality of the infrastructure, workloads, or the user data.

[Reference: 1) GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section7.10.3.
2) NSA CISA Security Guidance for 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (2021)

2.1.10 Protection of data in transit

Recommendation:

a) 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 should be cryptographically protected as prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" Only.
b) Systems transmitting data should 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.
c) 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.
d) 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.
e) Multiple cloud-based Hardware Security Modules (HSMs) should be employed where practical and should 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]

2.1.11 Protection of data at rest

Recommendation:

The following should be considered

a) Cryptographic keys used to protect data, should be refreshed periodically, at least once a year.
b) Best practice is to secure the workload volumes by encrypting them and storing the cryptographic keys at multiple safe locations.
c) The hypervisor should 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.
d) The Platform should support self-encrypting storage devices.
e) The Perform security-related testing and auditing of environments that store data at rest should ensure the effectiveness of the protection scheme and the protection of all sensitive and confidential data.
f) It must be ensured 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.
g) It must be ensured that access to data is traceable by ensuring that all accessors of data are uniquely identifiable.

a) It should be possible to 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.
b) It must be ensured that tools are in place to detect data integrity impacting events and processes exist that define recovery procedures.
c) Multiple cloud-based Hardware Security Modules (HSMs) should be employed where practical and should 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]

2.1.12 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 data like cryptographic keys, authentication strings, or data with intellectual property and privacy concerns can be preserved within a TEE, and operations involving these data 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.

Recommendation:
The following recommendations are to be considered

a) Implement Source Code Analysis of Code prior to load into TEE.
b) Perform regular updates/patching of Systems & Firmware for latest security fixes.
c) Leverage secure design guidance for code developed for TEE uses.
d) Verify and validate code before load into TEE using cryptographic methods such as Signature or hash checking.

[Reference: 1) NSA-CISA Security Guidance for 5G Cloud Infrastructures Part III: Data Protection (2021), Section-Protection of Data-in-use
2) ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 8.9]

2.1.13 Run Time Check

Recommendation:

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

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

[Reference: 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.

2.1.14 UUID Generation

Recommendation:

It is recommended to provide UUID generation as an alternative to the PKI
[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.3]

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

Recommendation:

The NFVI and VNFs should be patched regularly.
[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.22]

Part 2 Virtualization Security

(Applicable for both Hypervisor based VM with its VNF and CIS based Container with its CNF)

2.2.1 Strong password policy

Recommendation:

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.

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

2.2.2 Use and ownership of 'root' administration credentials

Recommendation:
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 should 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]

2.2.3 Hypervisor/CIS protection

Hypervisor or CIS introspection can be used to scrutinize software running inside VMs or containers to find abnormal activities. Using introspection capabilities, the hypervisors 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]

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

Recommendation:
The NFVI and VNFs should be patched regularly.
[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.22]

2.2.5 VNF Image validation and protection

Recommendation:
a) 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 should be performed. The validation should 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.
b) 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.
c) The software package and the artefacts within the package of a VNF should have their integrity protected by the vendor's (OEM's) signature. The software package and the artefacts within the package of a VNF and the software catalogue holding its image should 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.
d) 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]

2.2.6 The IDAM (Identity and Access Management)

Recommendation:
It is critical to note, application or service identity is also essential in the context of micro services, 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: 1) NSA-CISA Security Guidance for 5G Cloud Infrastructures Part I: Prevent and Detect Lateral Movement (2021)
2) CNCF Cloud Native Security Whitepaper Ver 2.0]

2.2.7 Function and capability authorization control for VNFs

Recommendation:

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]

2.2.8 Authorization

Recommendation:
Identity Services should 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 1.0, Feb 2022]

2.2.9 The software package must be checked for integrity during installation

Recommendation:
Each individual artefact in a VNF Package should have a cryptographic signature when it is stored in the NFV-MANO catalogue(s). Additionally, if the service provider policy mandates to sign an artifact, this service provider's signature on this individual artifact(s) should be stored as well

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

2.2.10 Vulnerabilities within the runtime software

Recommendation:

Operators should 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]

2.2.11 Secure Logging

Recommendation:

Creation of entries which are confidential from other parties; in general steps should 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]

2.2.12 post-incident analysis

Recommendation:

It is important that post-incident analysis should 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]

2.2.13 Firewall-as-a-Service

Recommendation:
F Was should be supported with cloud infrastructure as on-premise firewalls have limited capabilities.
[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.5]

2.2.14 The networking within the Mobile cloud should be securely configured

Recommendation:
a) Security groups per cluster should 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 should be used for connecting network functions.
c) Default firewall rules should be configured that determines which outbound or inbound connections are permitted.
[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part I: Prevent and Detect Lateral Movement (2021)]

2.2.15 Lock down communications among isolated network functions

Recommendation:
Policies should 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)]

2.2.16 Develop and deploy analytics to detect sophisticated adversarial presence

Recommendation:

a) Stakeholders at all layers of the mobile cloud stack should leverage an analytic platform to develop and deploy analytics that process relevant data (cloud logs and other telemetry) available at that layer. The analytics should 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)]

2.2.17 Cryptography

Recommendation:

a) It is also recommended establishing PKI infrastructure for secure admin access and protecting the network against external access, especially in a cloud environment.
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T06]

2.2.18 Security segmentation and isolation between network functions

Recommendation:

a) 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.
b) 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 should 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).
c) Due to differing security requirements, a separate virtual environment using separate clusters should be setup for VNFs and MANO.
d) Physical and/or logical separation should 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:

i) Linux kernel security: in virtualized platforms, the kernel of the host systems is a highly important component that provides isolation between the applications. The SEL inox 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 SEL inox, 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 GR Security, which provides protection against attacks on corrupted memory.
ii) 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.
iii) The trust domains of network functions should be identified. Each trust domain should be managed separately. Security policies for each trust domain should be managed independently.
iv) 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.
v) Confidentiality protection should 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]

Other Security Recommendations

2.2.19 Software Bill of Material (SBOM)

Recommendation:

a) 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 4G/5G NFV might include hundreds or even thousands of software components that software development and cyber security teams must track through all stages of the lifecycle.
b) An SBOM should 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]

2.2.20 Life cycle Management

Recommendation:

Secure software development principles for VNFs should incorporate the following industry best practices:

i) validating the removal of unused software modules and execution paths;
ii) 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;
iii) using container-specific host OSs to reduce risk by limiting the attack surface,
iv) enforcing Centre for Internet Security (CIS) benchmarks for K8S, docker, and Linux to establish a hardened baseline;
v) ensuring that the software supplier practices proper due diligence when using commercial third-party and open-source software in their projects
vi) validating application performance on the hardened infrastructure.

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

2.2.21 Resources inventory management system and database

Recommendation:

a) Hardware Inventory: It is expected a hardware (blade) for hypervisor or CIS and bare metal installation for inventory should exist to support operational management. However, in addition, to providing the ability to complete security investigations and meet regulatory

or legal requirements, it is recommended that the inventory stores: i) the location of each blade server (e.g. place, data centre, rack, shelf); ii) mapping VNF to hypervisor or CIS and blade server showing the current and historic records; iii) information as to whether any native installations are sharing the same blade server chassis, associated resources and network infrastructure.
b) Software inventory: A mechanism should exist to identify all VNFCs running in each VM or container within each hypervisor or CIS. It should also be possible to identify which hardware, data centre and location 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 should be completed against the VIM and EMS platforms to ensure only authorized VNFC applications are running and installed.
c) 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 should 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]

2.2.22 Defense In depth

Recommendation:
a) 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]

2.2.23 Vulnerability handling & patch management

Recommendation:

NFV/MANO software components should 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]

2.2.24 Security Testing and Assurance

Recommendation:

a) Regular penetration and vulnerability testing should be performed across the NFVI and MANO production environment to identify any known vulnerabilities or compromise of the network zoning rules.
b) It is recommended that testing should be carried out if new infrastructure or IP based interconnect elements have been deployed or as a minimum on an annual basis.

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

2.2.25 Incident Management

Recommendation:

The following should be met

a) Implement defensive security controls and continuous monitoring backed by machine learning capabilities and establish incident response operations to detect and mitigate threats.
b) Key capabilities include the following.

i) 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
ii) Denial-of-service defence systems: monitor network traffic to detect and mitigate network flooding attacks.
iii) Intrusion detection and prevention systems: monitor network traffic to detect and mitigate unauthorized access or attempts to exploit system vulnerabilities.
iv) 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.
v) Anti-malware systems: monitor network traffic and endpoint and server devices to detect and block malware files or malware execution.
vi) Security operations centre: 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]

2.2.26 User Plane Security

Recommendation:

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

vii) to protect NFV components from attacks sourced from the public internet and cloud;
viii) to protect the network from attacks sourced from internally attached NFV components;
ix) to protect the NFVI from attacks sourced from internally attached components and the internet.

b) 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.
c) Threat detection or prevention and response using IDS/IPS should 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]

2.2.27 OSS/BSS Protection

Recommendation:

The contrasting attributes of the legacy and virtualized infrastructures should 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.

a) The OSS/BSS would 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 should 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.
b) OSS/BSS systems should 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.
c) 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)

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

2.2.28 Redundancy and back up

Recommendation:

a) Recovery

The system should be deployed in such a way as to provide isolation and redundancy to increase the resiliency and defence against a single point of failure. There are a variety of ways operators should consider redundancy. Below are three ways the operator should be thinking about redundancy when it comes to its recovery plan.

1) 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 the network via redundant routers or switches would ensure minimal downtime and complete continuity of NFV services.
2) Power redundancy: backup power supply (a generator, for instance) that specifically keeps critical NFV hardware running in colocation facilities.
3) 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.
4) The recovery plan should already identify a fail-over location for the NFV system in the event that the current location is inoperable.

b) 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.

i. 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.

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

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

2.2.29 Test Isolation and Assurance

Recommendation:

a. 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 should 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.

b. Both positive and common vulnerability testing (e.g negative testing) should 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.
c. Virtualized 3GPP NFs should be checked regularly to see if they are using out-of-date or insecure versions of a library and these libraries should 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]

2.2.30 Single Administrator Domain

Recommendation:

a) In general, delegated administrator roles should be used. The global administrator role should only be used in exceptional cases, e.g. to add permissions for other high-level administrators

b) The highest security controls should be applied to use of the global administrator role. In particular, all use of this role should be logged and audited.

c) An alert should be raised in the global administrator role is used, or if any account attempts a function, it is not meant to attempt.

d) All administration and management should only be permitted from known, attested devices and multi-factor authentication should be enforced.

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

Part 2 (A)Virtual Machine

This part presents the Virtual Machine specific security best practices.

2.2A.1 VM Process Isolation

Recommendation:

a) The hardware of the virtualized host should 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:

i) Better memory management controls can prevent attacks such as buffer overflow.
ii) 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.

iii) Guest OS code and hypervisor code execute in different processor modes, providing better isolation.

iv) Privilege-level isolation can provide better protection for device access mediation functions, and hardware-based memory protection can provide better VM-level protection.

v) 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.

vi) 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 should 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 should be disabled by default.

c) The hypervisor should 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 should 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]

2.2A.2 Devices Mediation and Access Control

Recommendation:

a) Because of the complexity of emulating a hardware device through software emulation, apart from suffering performance penalties, also increases the size of the Trusted Computing Base (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 should only be used where complexity is manageable (e.g., USB host controller).

b) In situations where para-virtualized device drivers are used in VMs, mediation of access to physical devices should 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.

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

d) It should 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 should 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.
e) It should 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]

2.2A.3 VM Lifecycle Management

Recommendation:

a) There should 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.
b) Solutions for Security Monitoring and security policy enforcement of VMs should 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.
c) All anti-malware tools (e.g., virus checkers, firewalls, and IDPS) running in the virtualized host should 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]

2.2A.4 Network Segmentation

Recommendation:

a) Isolation of the hypervisor's management network using virtual switches needs special configuration. In addition to dedicated virtual switches, the management traffic pathway should 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.

b) In all VLAN deployments, the switch (physical switch connecting to virtualized host) port configuration should be VLAN aware – i.e., its configuration should reflect the VLAN profile of the connected virtualized host.
c) Large data center networks with hundreds of virtualized hosts and thousands of VMs and requiring many segments should 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.

[Reference: NIST Special Publication 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection]

2.2A.5 Configuring Network Path Redundancy

Recommendation:

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 should 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 should 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 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection]

2.2A.6 Firewall Deployment Architecture

Recommendation:

a) In virtualized environments with VMs running delay-sensitive applications, virtual firewalls should 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 should 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 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection]

2.2A.7 VM Traffic Monitoring

Recommendation:

a) VM traffic monitoring should be performed for both incoming and outgoing traffic.
b) If traffic visibility is accomplished by setting the promiscuous mode feature, care should 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 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection]

2.2A.8 Hypervisor Security

Recommendation:

The following must be met

a) 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.
b) Having security services in the hypervisor permits security monitoring even when the guest OS is compromised.

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

Part 2 (B) Container

This part presents the container specific security best practices

2.2B.1 Container Security

Recommendation:

a) Appropriate restrictions on container placement and on the use of container caching should include:

i) User handling containers relative to network management containers within a VNF;
ii) Separation of containers belonging to different NFs on different physical servers;
iii) Special handling of containers implementing interfaces between different trust domains (intra-VNF and inter-VNF).

b) Security policy which restricts the placement and co-existence of containers belonging to different trust domains should be defined and implemented by TSPs.

c) 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, should be defined and implemented by TSPs.

[Reference: 1) 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.26 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022) BP-T31]

2.2B.2 Container Platform Integrity

Recommendation:
The following should 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) Minimize this risk by disabling direct access (via SSH or other protocols) and using an agent-based system for node maintenance and troubleshooting.
d) 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 should 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)]

2.2B.3 Container Image Hygiene

Recommendation:

The following best practices should be implemented

a. Policies should be in place to restrict development teams to access only to repositories with which each team should interact.
b. 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 should be vetted and regularly scanned for vulnerabilities. Additionally, administrators should ensure that the image was published by a reliable entity such as the developer of a reputable product.

c) Lint 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.

d) Use immutable tags with images

Some image repositories support immutable tags. This forces 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 a way to identify an image easily and uniquely.

e) Sign 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.

f) Update the packages in the container images

The packages used in container images should be updated to ensure that the most up-to-date and secure packages.

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

2.2B.4 Secure Configuration of Networking within the cloud

Recommendation:

(a) Security groups per cluster should 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 should be used for connecting network functions.
(c) Default firewall rules or default ACLs should be configured that determines which outbound or inbound connections are permitted.
(d) Service Meshes should 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)]

2.2B.5 Incident response

Recommendation:

a) The ability to react quickly to an incident can help minimize the damage caused by a breach. There should be a reliable alert system that warns of suspicious behavior. When an incident does arise, the offending pod should be identified and isolated for forensic investigation and root cause analysis. Responses should minimally include:

i) Pod with a network policy that denies all ingress and egress traffic to the Pod should be isolated.
ii) The worker node should be cordoned off.
iii) Impacted worker nodes should enable termination protection.
iv) Volatile artifacts on the worker node should be captured.

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

2.2B.6 Container Image related

Recommendation:

a) Image vulnerabilities: Organizations should 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

i) Integration with the entire lifecycle of images, from the beginning of the build process, to whatever registries the organization is using, to runtime.
ii) Visibility should be centralized across the organization and provide flexible reporting and monitoring views aligned with organizations' business processes.
iii) Organizations should 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:

i) Images should be configured to run as non-privileged users.
ii) All remote management of containers should be done through the container runtime APIs which may be accessed via orchestration tools.
iii) Embedded Secrets: Secrets should be stored outside of images and provided dynamically at runtime as needed.

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

2.2B.7 Registry Related

Recommendation:

The following should be met

a) Insecure connections to registries: Organizations should 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 should occur between trusted endpoints and should be encrypted in transit.
b) Stale images in registries: The use of stale image should be prevented
c) Insufficient authentication and authorization restrictions: All access to registries that contain proprietary or sensitive images should require authentication. Any write access to a registry should require authentication to ensure that only images from trusted entities can be added to it.

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

2.2B.8 Orchestrator Related

Recommendation:

The following should be met

a) Unbounded administrative access: orchestrators should 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 should be tightly controlled as these accounts provide ability to affect all resources in the

environment. Organizations should use strong authentication methods, such as requiring multifactor authentication.

c) Poorly separated inter-container network traffic: Orchestrators should be configured to separate network traffic into discrete virtual networks by sensitivity level.
d) Mixing of workload sensitivity levels: Orchestrators should 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 should 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)]

2.2B.9 Host OS related

Recommendation:

a) Host OS component vulnerabilities: Organizations should implement management practices and tools to validate the versioning of components provided for base OS management and functionality. Organizations should 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 should be kept up to date not only with security updates, but also the latest component updates recommended by the vendor. Host OSs should 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 should be packaged and deployed in containers.

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

2.2B.10 Build Pipeline

Recommendation:

a) Continuous Integration (CI) servers should be isolated and restricted to projects of a similar security classification or sensitivity. Infrastructure builds which require elevated privileges should run on separate dedicated CI servers. Build policies should be enforced in the CI pipeline and by the orchestrator's admission controllers.
b) 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.
c) It should be ensured that the CI and Continuous Delivery (CD) infrastructure is as secure as possible.

[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

2.2B.11 Container Application Manifest Scanning

Recommendation:

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.
[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

2.2B.12 Dynamic Analysis

Recommendation:

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 Security Operations Centre (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.
[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

2.2B.13 Audit Log Analysis

Recommendation:
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.
a) Logs should be forwarded immediately to a location inaccessible via cluster-level credentials. The systems processing alerts should be periodically tuned for false positives to avoid alert flooding, fatigue, and false negatives after security incidents that were not detected by the system.
[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

2.2B.14 DDoS Attack Prevention

Recommendation:
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.
[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

2.2B.15 Threat Intelligence

Recommendation:

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.
[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

Part 2 (C) VNF_CNF Related

(Wherever VNF or CNF is explicitly mentioned, those clauses are applicable for those VNF or CNF. Otherwise, the clauses are applicable for both VNF and CNF)

2.2C.1 Image Snapshot and VNF/CNF Mobility

Recommendation:

a) Migration of a VNF/CNF from a trustworthy environment to an untrustworthy environment should not be possible, e.g., the access to virtualization management operations, like starting, stopping, pausing, restarting, live migration of a VNF/CNF, should be subject to authentication and authorization.
b) VNF/CNF data should be confidentiality protected when stored as part of a VNF/CNF snapshot or during migration of the VNF to another execution environment.
c) Where VNF/CNF sub-components are in different trust domains, the snapshot should maintain security and isolation requirements for each trust domain within the snapshot of the VNF/CNF.
d) The ability of a VNF/CNF to verify the trustworthiness of another VNF/CNF should not be impeded by pausing, stopping, restarting, or migrating a VNF/CNF.
e) All VNF/CNF Snapshot and VNF/CNF mobility operations should preserve the persistent state of the VNF in order to prevent forking or roll-back attacks.
f) It should be possible to protect and prevent sensitive VNF/CNF or VNF/CNF-components from being subject to snapshot or migration without explicit authorization.
g) All system snapshots events should be subject to secure logging.
h) Snapshots should 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]

2.2C.2 Volume Sanitization

Recommendation:
Secure deletion of the volumes should 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]

2.2C.3 Sensitive authentication data in workloads

Recommendation:
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 should be protected during all phases of the NFV security and trust lifecycle and should 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]

2.2C.4 Encrypting VNF/CNF volume/swap areas

Recommendation:
The hypervisor or CIS should be configured to securely wipe out the virtual volume disks in the event a VNF/CNF is crashed or intentionally destroyed to prevent it from unauthorized access.
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T14]

2.2C.5 Trust domain and Slice Isolation

Recommendation:

a) The Mobile Core should be configured so that NFs can only communicate with NFs which they have a valid reason to communicate with. The default should be that functions are not able to communicate.
b) Delegated administrator roles should be used and should only give the user or administrator the minimum necessary privileges.

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

2.2C.6 Encrypted Data Processing

Recommendation:
It should be possible to control whether untrusted or lower trusted VNFs/CNFs are allowed to run on the same host as VNFs /CNFs in a higher trust domain.
[Reference: 3GPP TR 33.848-0.11.0 Section 5.16]

2.2C.7 Mixed Virtual and Legacy PNF Deployments

Recommendation:

a) The Mobile Core should be configured so that NFs can only communicate with NFs which they are specifically authorized to communicate with. These rules should be applied irrespective of whether the NF is a PNF or a VNF/CNF. The default should be for two NFs not to trust one another and to block communication.

b) The security policies enforced by the system should complement each other in order to protect mixed PNF-VNF deployments.

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

2.2C.8 Secure executive environment provision

Recommendation:
The VNF should support comparing the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF/CNF can query the parsed resource state by the VNFM from the OAM. The VNF should 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]

2.2C.9 Confidentiality protection of Cloned VM image

Recommendation:
If an image contains sensitive information, it should 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]

2.2C.10 Guest OS Security

Recommendation:
The following should be complied

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.
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:

(i) 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.
(ii) 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]

2.2C.11 Container Image Hygiene

Recommendation:
The following best practices should be implemented

a) Build images from scratch or create minimal de-fanged images:
b) Reducing the attack surface of a container image should 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 the container software has a mechanism to create images from scratch, it should 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.
c) If unable to build an image from scratch, developers should 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 and curl that can be used for nefarious purposes.
d) Third-party software should also undergo security review that includes code inspection, threat modelling, and penetration testing to identify and mitigate risks.

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

2.2C.12 Container image authorization

Recommendation:
The following should 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.

[Reference: CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0]

Part 3-SDN

This part presents the SDN specific security Recommendations.

3)

2.3.1 Prevent attacks via SDN controller's Application Control Interface

Recommendation:
Secure coding practices for all northbound applications requesting SDN resources should be used.

Part 4 MANO

This part presents the MANO specific security Recommendations.

2.4.1 Authorized access to MANO

Recommendation:
Access to the MANO should be restricted to a limited number of administrators.

[Reference: 1) 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.19 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP T8]

2.4.2 Orchestrator node trust

Recommendation:
It should be ensured that orchestration platforms are designed specifically to be resilient to compromise of individual nodes without compromising the overall security of the cluster.
[Reference: NIST Special Publication 800-190 [September 2017]

2.4.3 Internal Health Checks in MANO Functions

Recommendation:
MANO functions should 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]

2.4.4 Security Management and Orchestration

Recommendation:
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 should be met

a) The number of privileged accounts for the NFVI is constrained to a minimal

manageable number to meet the TSP's needs.

b) NFV-MANO and NFVI administrators do not have any privileged rights to other services within the TSP.
c) NFV-MANO and NFVI administration access is limited to best practice configuration methods (e.g. authorized API calls).
d) NFV-MANO and NFVI administration is automated wherever possible.
e) Manual administration of the NFVI is by exception and raises a security alert.
f) Functions that support the administration and security of the NFVI are treated as security critical functions.

[Reference: 1) ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.2 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T8]

2.4.5 VIM connectivity to virtualization layer

Recommendation:

It is recommended 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]

2.4.6 NFVO Security Management

Recommendation:

a) The NFVO should 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.
b) 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]

2.4.7 Tracking VNF version changes

Recommendation:

The orchestration and VNF management systems–should 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]

Annexure-I

Definitions

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. 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
7. Confidentiality: The state of keeping or being kept secret or private.
8. Confidential system internal data: that contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).
9. Firewall: A firewall is a network security device that monitors traffic to or from the network.
10. Generic virtualized network product model (GVNP) Type 1: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0
11. Generic virtualized network product model (GVNP)Type 2: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0
12. Generic virtualized network product model (GVNP)Type 3: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0
13. Host path: In Kubernetes, a host Path volume means mounting a file or a directory from the node's host inside the pod. A Kubernetes hostpath is one of the volumes supported by Kubernetes.
14. Host system: collection of hardware, software and firmware making up the system which executes workloads
15. 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.

16. Least Trusted Domain (LTD): The Less Trusted Domain (LTD) contains resources that can be managed without the risk of compromising sensitive information, since these functionalities are offloaded to the MTD.
17. More Trusted Domain (MTD) contains resources (network, storage, processing) where sensitive functions can be offloaded.
18. Namespace: In Kubernetes, namespaces provide a mechanism for isolating groups of resources within a single cluster.
19. Network Functions Virtualization (NFV): principle of separating network functions from the hardware they run on by using virtual hardware abstraction
20. Network Functions Virtualization Infrastructure (NFVI): totality of all hardware and software components that build up the environment in which VNFs are deployed.
21. Network Functions Virtualization Infrastructure (NFVI) components: NFVI hardware resources that are not field replaceable, but are distinguishable as COTS components at manufacturing time.
22. 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.
23. 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)
24. Network Functions Virtualization Management and Orchestration (NFV-MANO): functions collectively provided by NFVO, VNFM, and VIM
25. 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.
26. 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
27. Network Interface Controller (NIC): device in a compute node that provides a physical interface with the infrastructure network.
28. Network operator: operator of an electronics communications network or part thereof. An association or organization of such network operators also falls within this category.
29. 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)

30. Network Service: composition of Network Function(s) and/or Network Service(s), defined by its functional and behavioral specification.
31. Network Service Orchestration: subset of NFV Orchestrator functions that are responsible for Network Service lifecycle management
32. Network Service Provider: type of Service Provider implementing the Network Service
33. 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
34. Personal data: any information relating to an identified or identifiable natural person ('data subject') and also “personal data” means any data about an individual who is

4) identifiable by or in relation to such data;

35. Physical Network Function (PNF). Refers to the legacy network appliances on proprietary hardware.; implementation of a NF via a tightly coupled software and hardware system
36. Physical Network Function Descriptor (PNFD): template that describes the connectivity requirements of Connection Point(s) attached to a Physical Network Function.
37. Platform: A computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run.
38. 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.
39. Pod Spec: PodSpec includes a set of fields that specify the user and/or group to run the application.
40. 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.
41. 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. An entity that relies upon the subscriber’s credentials, typically to process a transaction or grant access to information or a system
42. Sensitive Data: data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.
43. Syscall: The system call is the fundamental interface between an application and the Linux kernel.
44. 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.

45. Virtual Machine (VM): virtualized computation environment that behaves very much like a physical computer/server; A virtual machine (VM) is an isolated computing environment created by abstracting resources from a physical machine
46. VM Image: A Virtual Machine Image is a fully configured Virtual Machine used to create a VM for deployment.
47. Virtual Network: virtual network routes information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity
48. Virtualized Network Function (VNF): implementation of an NF that can be deployed on a Network Function Virtualization Infrastructure (NFVI)
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. VNF Image: It is a fully configured Network Function which is used to deploy the network function in a virtualized environment.
51. 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.
52. VNF Package: VNF Package is a ZIP file including VNFD, software images for VM, and other artifact resources such as scripts and config files
53. 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.

a) 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
ACL	-	Access Control List
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 Tunnelling Protocol Control Plane
GTP-U	-	GPRS Tunnelling 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

References

a) 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).
b) 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).
c) ETSI GS NFV-SEC 001 V1.1.1 (2014-10) "Network Functions Virtualization (NFV); NFV Security; Problem Statement"
d) ETSI GS NFV-SEC 002 V1.1.1 (2015-08) "Network Functions Virtualization (NFV); NFV Security; Cataloguing security features in management software"
e) ETSI GS NFV 003 V1.3.1 (2018-01) Network Functions Virtualization (NFV); Terminology for Main Concepts in NFV.
f) ETSI GS NFV-SEC 006 V1.1.1 (2016-04) Network Functions Virtualization (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns.
g) 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.
h) ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Network Functions Virtualization (NFV); NFV Security; Report on Retained Data problem statement and requirements.
i) 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.
j) ETSI GS NFV-SEC 013 V3.1.1 (2017-02) Network Functions Virtualization (NFV) Release 3; Security; Security Management and Monitoring specification
k) 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.
l) ETSI GR NFV-SEC 018 V1.1.1 (2019-11) Network Functions Virtualization (NFV); Security; Report on NFV Remote Attestation Architecture.
m) ETSI GS NFV-SEC 021 V2.6.1 (2019-06) Network Functions Virtualization (NFV) Release 2; Security; VNF Package Security Specification.
n) ETSI GS NFV-SEC 022 V2.8.1 (2020-06) Network Functions Virtualization (NFV) Release 2; Security; Access Token Specification for API Access.
o) ETSI GS NFV-EVE 005 V1.1.1 (2015-12) Report on SDN Usage in NFV Architectural Framework.
p) NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES "Part I: Prevent and Detect Lateral Movement 2021"

q) NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES "Part II: Securely Isolate Network Resources"
r) NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021)
s) NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES (2021) "Part IV: Ensure Integrity of Cloud Infrastructure"
t) NIST Special Publication 800-125B (March 2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection.
u) NIST Special Publication 800-125 Guide to Security for Full Virtualization Technologies.
v) NIST Special Publication 800-190 Application Container Security Guide.
w) ONAP VNF API Security Requirements
x) ENISA Security aspects of virtualization FEBRUARY 2017.
y) ENISA NFV SECURITY IN 5G Challenges and Best Practices FEBRUARY 2022.
z) GSMA NG 133 Cloud Infrastructure Reference Architecture managed by OpenStack v 1.0, Feb 2022.
aa) GSMA NG 126 Cloud Infrastructure Reference Model Version 3.0
bb) CNCF _Cloud-Native-Security-whitepaper-May2022-v2

-End of Document-