INTERNATIONAL STANDARD

ISO/IEC 27033-7

First edition
2023-11

Information technology – Network security —

Part 7: Guidelines for network virtualization security

Technologies de l'information — Sécurité des réseaux —

Partie 7: Lignes directrices pour la sécurité de la virtualisation des réseaux

Reference number
ISO/IEC 27033-7:2023(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 27033 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The purpose of this document is to address the key challenges and risks of network virtualization security. Network virtualization includes virtual network infrastructure, virtual network function, virtual control and resource management. This document aims to:

1) identify security risks of network virtualization;

2) propose a network virtualization security model;

3) propose security guidelines for virtual network infrastructure, virtual network function, virtual control and resource management.

This document intends to help stakeholders in understanding the main characteristics of network virtualization security. For example, this document can help software and hardware suppliers to securely design and develop products that implement network virtualization, and help operators to evaluate the security of these products and deploy them securely for network services. By proposing security guidelines, this document aims to help the industry to improve system security that is built on network virtualization technology.

The target audience can include the network equipment vendors, network operators, internet service providers and software service providers.

With the rapid development of IT technologies such as cloud computing, IT systems and communication systems are increasingly evolving with the adoption of virtualization technology. Virtualization enables systems to have high agility, flexibility and scalability with low cost, but at the same time, introduces many security challenges.

Information technology – Network security —

Part 7:
Guidelines for network virtualization security

1 Scope

This document aims to identify security risks of network virtualization and proposes guidelines for the implementation of network virtualization security.

Overall, this document intends to considerably aid the comprehensive definition and implementation of security for any organization's virtualization environments. It is aimed at users and implementers who are responsible for the implementation and maintenance of the technical controls required to provide secure virtualization environments.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
network virtualization
technology that enables the creation of logically isolated network partitions over shared physical network infrastructures so that multiple heterogeneous virtual networks can simultaneously coexist over the shared infrastructures

Note 1 to entry: Network virtualization allows the aggregation of multiple resources and makes the aggregated resources appear as a single resource.

[SOURCE: ISO/IEC TR 29181-1:2012, 3.3]

3.2
network functions virtualization
NFV
technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks

Note 1 to entry: This includes the aggregation of multiple resources in a provider and appearing as a single resource.

[SOURCE: ISO/IEC TR 22417:2017, 3.8]

3.3
software-defined networking
set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner

[SOURCE: ITU-T Y.3300:2014, 3.2.1]

3.4
virtual machine
virtual data processing system that appears to be at the disposal of a particular user, but whose functions are accomplished by sharing the resources of a real data processing system

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.4564]

3.5
container
isolated execution environment for running software that uses a virtualized operating system kernel

[SOURCE: ISO/IEC 22123-1:2023, 3.12.4]

3.6
orchestrator
tool that enables DevOps personas or automation working on their behalf to pull images from registries, deploy those images into *containers* (3.5), and manage the running containers

[SOURCE: NIST SP 800-190]

3.7
service function chain
ordered set of abstract functions and ordering constraints that are applied to packets and/or frames and/or flows selected as a result of classification

[SOURCE: IETF RFC 7665, modified — removed “a service function chain defines an” at the beginning of the definition and replaced “must” with “are” in the definition.]

4 Abbreviated terms

The following abbreviated terms apply to this document.

5G	the fifth generation mobile network
AMF	access and mobility management function
API	application programming interface
AUSF	authentication server function
CDN	content delivery network
CIS	centre for internet security
DoS	denial of service
DDoS	distributed denial of service
HMAC	hash-based message authentication code
IDS	intrusion detection system

IPS	intrusion prevention system
MANO	management and orchestration
MFA	multi-factor authentication
NF	network function
NFV	network functions virtualization
NFVO	network function virtualization orchestrator
NRF	network repository function
NSSF	network slice selection function
OAM	operation and management
OMC	operation maintenance centre
OS	operating system
SD-WAN	software-defined wide-area network
SDN	software-defined networking
SFC	service function chain
SMF	session management function
UDM	unified data management
UPF	user plane function
vCPU	virtual CPU
VIM	virtualised infrastructure manager
vI/O	virtual I/O
VNF	virtualised network function
VNFM	virtualised network function manager
VM	virtual machine
vMemory	virtual memory
VMM	virtual machine manager
vRouter	virtual router
vSwitch	virtual switch
vWAF	virtual web application firewall
VxLAN	virtual extensible local area network
WAF	web application firewall

5 Overview

5.1 General

Network virtualization provides a novel solution for the development and deployment of IT systems and communication networks. It greatly reduces the cost of system maintenance, improves the utilization of resources (such as computing, storage and networking) and the flexibility of IT systems or networks. Cloud computing, the dominant platform for new IT systems and networks makes extensive use of network virtualization technology. ISO/IEC 22123-1 and ISO/IEC 22123-2 provide an overview of cloud computing and its concepts. ISO/IEC 22123-3 provides reference architecture for cloud computing. The typical use cases of network virtualization include but are not limited to software-defined wide-area network (SD-WAN), network slice, Virtual WAF and cloud CDN with centralized control, which are referred to in Annex A.

With the adoption of network virtualization, new security challenges to IT and communication systems are introduced. Hence, traditional security protection solutions, which are often static, passive and isolated, would not be effective for virtualized systems. New security solutions, which are dynamic, proactive, coordinated and have intelligent management capability, are needed.

5.2 Description of network virtualization

Network virtualization abstracts physical resources, such as computing, networking, memory and storage into standard and general-purpose entities. Each entity can be deployed with service functions under the control of an orchestrator. Through virtualization, the limitation of physical resources are broken, thus, the utilization of these resources are improved. The new virtual entities of these resources are no longer limited by the way their physical counterparts are deployed.

In this document, network virtualization includes virtual network function and virtual network connection. Virtual network function runs on virtual infrastructure (such as virtual computing, virtual storage and virtual networking) using virtualization technologies (such as virtual machines and containers). NFV is a common method to implement virtual network function. Virtual network connection is applied to connect functional units on demand. The resulting network called SDN is composed of virtual data links. An important characteristic of SDN is that all underlying resources can be centrally managed and provide a standard interface that support software programming based on the customer's requirements. The introduction of SDN and NFV solutions changes the network significantly: general-purpose hardware, virtual software function, programmable network connections and services. With SDN and NFV, the cost of network operation and maintenance is cut down, the utilization of resources (such as computing, storage and networking) is improved, the flexibility of the network and service logic is increased, and the time-to-market of new services is considerably decreased.

5.3 Security model

5.3.1 Model of network virtualization security

ISO/IEC 27033-1 provides a conceptual model of network security for network security risk and management review. In general, network security includes three areas: security of the element, security of network connection and security of management. In network virtualization, the element is a virtual network function and the network connection is a virtual connection. This document further enhances this model according to the technical characteristic of network virtualization, as shown in Figure 1.

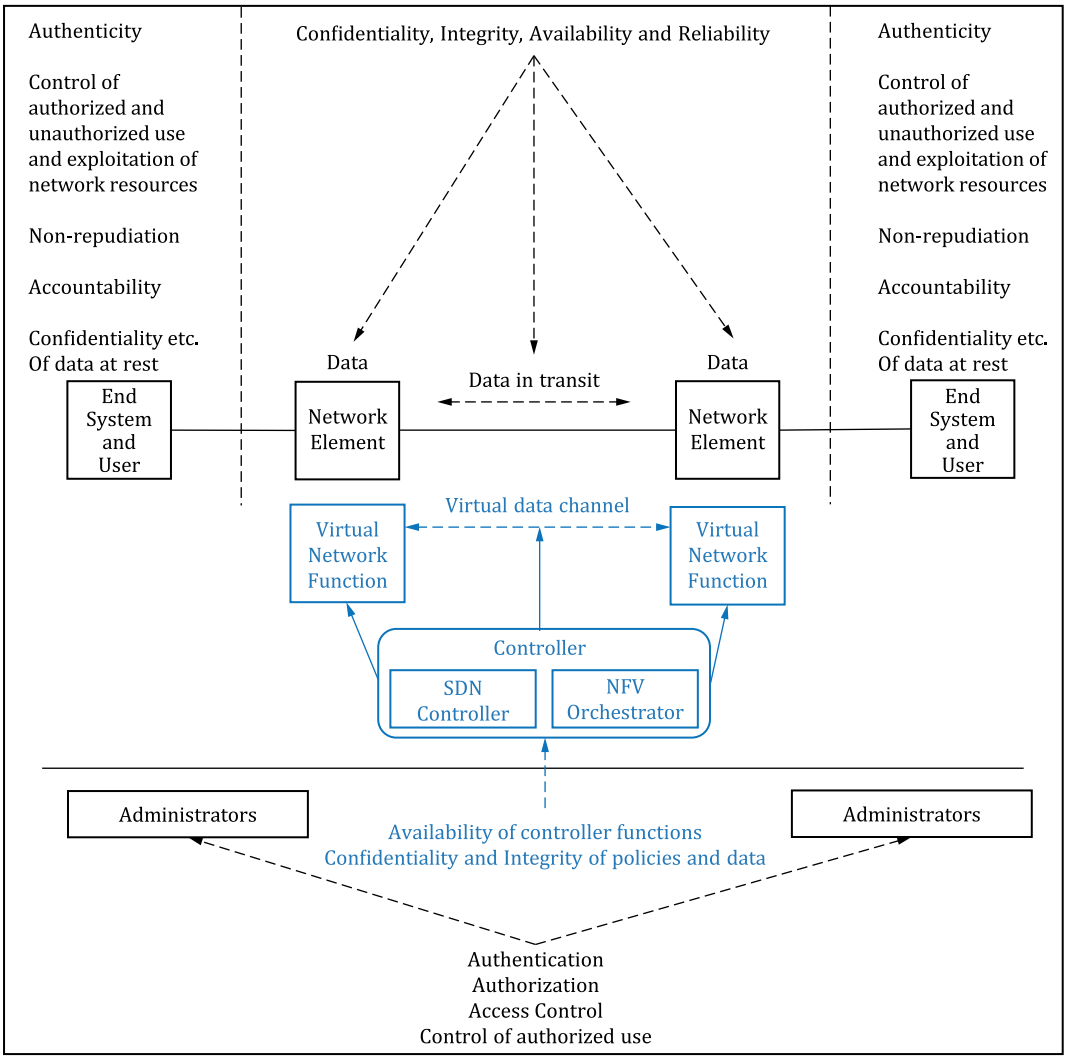

Figure 1 — A conceptual model of network virtualization security risk areas

These changes brought about by network virtualization include:

a) Centralized controllers are included. The NFV orchestrator is responsible for the allocation, scheduling and life cycle management of infrastructure and resources. The SDN controller is in charge of the management of network topology and virtual data links. The NFV orchestrator and SDN controller provide standard northbound API to support the scheduling of computing, network and storage resources in the system in a software programmable manner, and also provide collaborative, dynamic and optimized scheduling of network resources and services.

b) Network elements are now virtual elements (as opposed to physical elements) whose behaviour is directed by the controller (NFV orchestrator). Network elements can be deployed or destroyed on demand as software, with service logic and functionality programmed to run on virtualized infrastructure (such as virtual machines and containers). ISO/IEC 21878 provides guidelines for design and implementation of virtualized servers.

c) Data link has changed. Besides the physical data links, the adoption of new technologies such as SDN and SFC provides efficient virtualized data links according to applications' needs. New technologies can also improve the efficiency of data transmission inside the system and meet the transmission resiliency needs of cloud computing (such as load balancing and high reliability).

5.3.2 Network virtualization components

There are two forms of virtualization, which are bare metal architecture and hosted architecture. For the reason of efficiency, in network virtualization, bare metal architecture is often used. The common components and system architecture of network virtualization are as shown in Figure 2, which consists of three parts: virtual network infrastructure, network functions and management system.

a) Virtual network infrastructure

This layer includes the virtual machine manager and host OS. Hardware resources include hardware for bare metal, hardware for switch and router and hardware for storage. The virtualization machine manager abstracts the hardware resources to form virtual computing, storage and network resources for the upper layer to be invoked. The typical virtualization machine manager includes hypervisor for virtual machines, and container engine for containers.

b) Virtual network functions

To deploy network functions as software based on virtual resources provided by virtualization, VNFs can be applied, and can create on-demand data connections between VNFs under the scheduling of the SDN controller. These VNFs, vRouter and vSwitch provide a standards-based approach to dynamically provision network function from the SDN controller. SDNs enable dramatic improvements in network function agility and automation, while substantially reducing the cost of network operations.

c) Management system

On the basis of the legacy management system such as OMC, the SDN controller and NFV orchestrator are also added. The NFV orchestrator is responsible for the allocation, scheduling and life cycle management of infrastructure and resources. The SDN controller is in charge of the management of network topology and virtual data links.

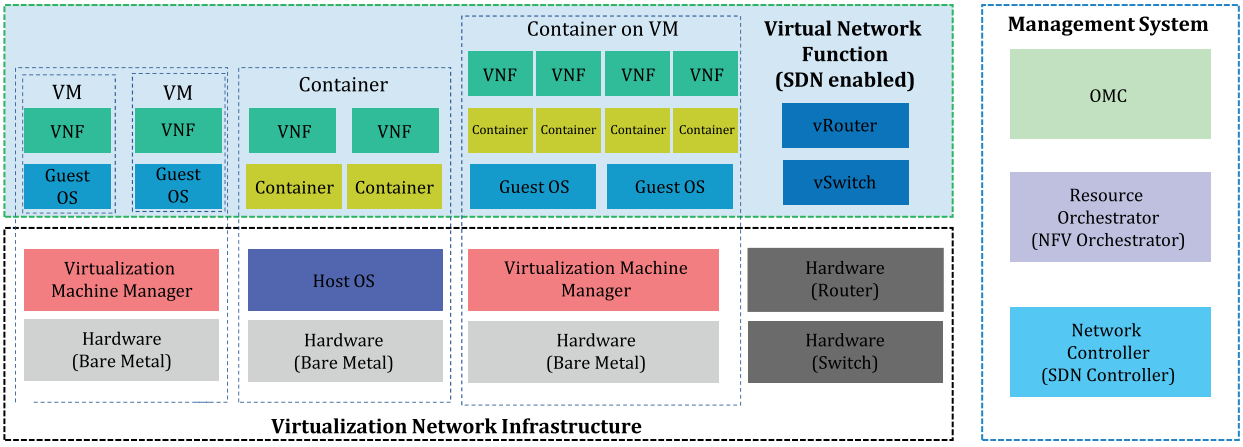

Figure 2 — Components and architecture of network virtualization

There are three types of VNF deployments in bare metal architecture. Figure 2 shows the VM deployment, container deployment that runs on host OS and container deployment that runs on VM.

6 Security threats

Network virtualization uses new technologies such as NFV and SDN, which bring the advantages of resource flexibility and business agility. Meanwhile, the characteristics of these new technologies, as well as the interoperation of these technologies also introduce new security threats.

The following security issues describe the security threats of network virtualization with reference to the dimensions of the security threat description in ISO/IEC 27033-3. Annex B describes the security threats from the dimension of network virtualization architecture that are shown in Figure 2, as well

as the virtualization-specific security threats. The descriptions in Annex B help to better identify the security threats of network virtualization.

Security issues for network virtualization include:

— Virus attacks and introduction of malware: host OS, guest OS of virtual network function, SDN controller software, OS of MANO, etc. in the network virtualization are subject to virus and malware attacks.

— Information leakage: if data under the control of a VM are not processed by special "purification" after deleting a VM, other business systems or malicious operation and maintenance personnel can obtain the key business information, triggering sensitive data disclosure.

— Unauthorized usage and access: an unauthorized attacker uses and accesses data of a VM or API of MANO.

— DoS and DDoS attacks: an attacker utilizes a lot of switches to forward a large number of packages to the SDN controller, resulting in (D)DoS attack of SDN controller.

— Insider attacks: an administrator tampers image or changes security configurations. An administrator also can intentionally jeopardize a security misconfiguration (e.g. opening unnecessary ports of a VNF), an attacker can use this security misconfiguration to launch an attack.

— Insider-outsider collusion: an insider can also collaborate with an outside threat agent to launch attacks.

— Privilege escalation: a user exploits a vulnerability to obtain administrator privilege.

— Forgery of transaction contents: the transaction contents of VM are tampered with by an attacker.

— Reducing network availability: the loss of backup data makes the business unavailable.

— Compromising the network segregation: an attacker can use compromised VM to attack other VMs to which it has access.

— Reducing real-time performance: an attacker uses a virtual machine to maliciously deplete resources on the host, which will affect the real-time performance of other virtual machines on the host.

For detailed security threats of the network virtualization, refer to Annex B.

7 Security recommendations

7.1 General

The primary security objective of network virtualization is to provide a secure runtime environment and data protection in the life cycle. To achieve this objective, the network virtualization should support the security recommendations of confidentiality, integrity, availability, authentication, access control and non-repudiation.

7.2 Confidentiality

The network virtualization should provide the data confidentiality protection. It should include, at the minimum, the following security recommendations:

a) The virtual network infrastructure should provide the storage resource to the virtual network function. It should give support by providing data confidentiality protection for the stored data of the virtual network function. The protected data includes the image and snapshot of the virtual network function, the password, private key, signalling, and customer's data (e.g. subscription data).

b) When data are transmitted, the data confidentiality protection should be provided for the transmitted data. In the network virtualization, the transmitted data include at least the following data:

   — data transmitted in the virtualized data link between two virtualized network elements (see Figure 1).

   — data transmitted in the intra-interfaces between two elements in virtual network management, e.g. between NFVO and VNFM, VNFM and VIM, VIM and SDN controller, etc.

   — Data transmitted in the interface between the external system and the virtual network management, e.g. between the virtual network function and VNFM.

   — Data transmitted in the interface of the remote operation and management such as the interface between OAM and the virtual network function.

7.3 Integrity

The hardware, firmware, OS and applications in the network virtualization should support secure booting to detect whether they have been tampered with. This detection ensures that the critical components are in a trusted state. The image and software such as SDN controller software should support integrity protection. The integrity protection of the transmitted data on the interfaces and the stored data (such as image) should be provided.

7.4 Availability

— The network virtualization should support availability. It includes the following recommendations at least: the virtual network function, SDN controller and MANO should support disaster resilience.

— The virtual network function, SDN controller and MANO should support anti-(D)DoS attacks.

— The network virtualization should support segmentation into security domains as well as boundary protection to prevent (D)DoS from internet.

— The network virtualization should support security policy synchronization in a migration scenario.

— The SDN controller should support the policy conflict detection.

NOTE Policy conflict means that the new policy generated by the SDN controller conflicts with the existing effective policy or another newly generated policy. For example, the attacker issued the shortest path request from server A to server D by calling the northbound API of the SDN controller. The SDN controller had previously generated a policy that the communication from server A to D is required to pass through a firewall. If a new policy of higher priority is generated that provides a path bypassing the firewall, that clearly conflicts and overrides the previous policy.

7.5 Authentication

Access to the physical interface of the hardware (e.g. console interface, WAN interface), the logical interface of the virtualization engine, the virtual network function and the virtual network management should be authenticated.

7.6 Access control

The physical interface of the hardware (e.g. console interface or WAN interface), the logical interface of the virtualization engine, the virtual network function and the virtual network management should support access control, e.g. role based access control or attribute based access control should be provided. Only authorized entities are allowed access.

7.7 Non-repudiation

The network virtualization should support non-repudiation. At least the following recommendations apply:

— Access to physical device, the virtualization engine, the virtual network function and the virtual network management should be logged through appropriate log forms and those log records should be transmitted to the remote server for appropriate analysis.

— The image and the package of the virtual network function should support digital signature.

Table 1 illustrates the relationship between the threats in Clause 6 and the security recommendations in this Clause.

Table 1 — Relationship between threats and recommendations

Threats	Recommendations					
	Support the data confidentiality protection	Support the integrity protection for hardware, firmware, software and image, etc.	Support the availability protection through disaster resilience, anti-(D)DoS, security domain division, etc.	Support authentication for the physical or logical interfaces in the network virtualization	Support access control for accessing the physical or logical interfaces in the network virtualization	Support non-repudiation
Virus attacks and introduction of malware	√	√	√	√	√	√
Information leakage	√			√	√	
Unauthorized usage and access					√	√
DoS and DDoS attacks			√			
Insider attacks				√	√	√
Forgery of transaction contents	√	√				√
Reducing network availability			√			
Compromising the network segregation	√	√		√	√	
Reducing real-time performance			√			

8 Security controls

8.1 General

Based on the design principles such as defence in depth, network segmentation and design resilience in ISO/IEC 27033-2 and the security design techniques and controls in ISO/IEC 27033-3, the security controls for the network virtualization infrastructure are described in 8.2 to 8.4.

8.2 Virtual network infrastructure security

a) Hardware

The hardware in network virtualization (e.g. host server, router, switch) should be deployed in a secure environment. For example, the room where the hardware is deployed should be equipped with waterproof, anti-earthquake mechanisms, and access control should be deployed to monitor personnel access.

The physical interface on the hardware (e.g. console interface, WAN interface) should configure an access control mechanism to authenticate and authorize the access. The administrator should be authenticated and authorized when he/she logs into the device. If a password is used, the complexity of the password should be guaranteed, i.e. the password is no shorter than 8 characters and contains at least three types of uppercase letters, lowercase letters, special characters and numbers. The communication between the management system and the device should be protected for confidentiality and integrity

The host server should support secure boot to ensure the integrity of the host server.

b) Virtualization engine

The virtualization engine should support detection and prevention of the virtual machine escape and the container engine escape. Host OS, virtual machine manager, Guest OS and container engine should support hardening mechanisms such as proper configuration of ports and services, closing of unnecessary ports and services, scanning for vulnerabilities, and virus detection. The virtualization engine should also support resource isolation. For example, vCPU, vMemory and vI/O used by one VM should be isolated from the resources used by another. All access should be authenticated and authorized, e.g. one VM accessing another VM, the virtualization engine accessing the VM/container, or the administrator accessing the VM.

c) Network connection

Virtual network infrastructure should support secure network connection, such as protecting the boundary with internet, e.g. anti-DDoS and anti-botnet devices can be deployed for preventing DDoS attacks and for botnet detection and prevention. The host server should support physical or logical traffic separation. For example, management traffic, signalling traffic, and data traffic should be transmitted through different interfaces.

8.3 Virtual network function security

a) VM

The guest OS should support hardening mechanisms such as closing unnecessary ports and services, scanning for vulnerabilities and virus detection. The resources accessed by VMs, and VMM should be isolated. The VM images should have integrity and confidentiality protection and should be stored securely to prevent unauthorized access. When a VM is migrated, the security policy associated with that VM should be transferred and deployed to the new location so that the security profile of that VM is not affected by the migration. All access to the virtual machine should be authenticated and authorized.

b) Container

As with VM security, the host OS should also support hardening. The resources accessed by various containers, as well as the host OS should be isolated. The image repository and image of container should have integrity and confidentiality protection, and should be stored securely to prevent unauthorized access. All access to the container should be authenticated and authorized.

c) Network function

Virtualized network function should use secure protocols to protect the communication with other VNFs or management elements. There should be disaster resilience mechanisms to ensure the availability of VNF.

d) Data security

There should be life cycle protection for VNF's data, that includes at the minimum secure storage and ensuring authenticated and authorized access. The residual data should be completely erased.

Access to VNFs should be authenticated and authorized, and the data transmitted by them should be encrypted and integrity protected.

e) Network security

VNF's traffic should be monitored, and the monitoring data should be analysed by using techniques such as artificial intelligence, machine learning and other technologies. If DDoS and other attacks are detected, relevant security measures should be taken, such as blocking all traffic to the malicious VNF and re-routing the traffic to a new secure VNF.

The security misconfiguration controls should be supported. Ingress whitelisting at each subnet level can be used to limit the blast radius. For example, using network ACL or subnet level ingress firewalls to provide network segmentation.

f) Management security of VNF

Access to VNF from internal operation and maintenance personnel should be authenticated and authorized.

g) SDN security

The SDN controller should support confidentiality and integrity protection for transmitted data on southbound and northbound interfaces. The SDN controller should check whether the policy is in effect on the switch, and policy synchronization between the SDN controller and the switch should be implemented. If the policy is not synchronized, it should be detected by the SDN controller. The software-defined networking process should not be susceptible to security attacks during the time of reconfiguration.

8.4 Virtual network management security

8.4.1 SDN controller security

The SDN controller should support the detection of the (D)DoS attacks from southbound interface and northbound interface. The related security mechanism (e.g. traffic limit) should be supported by the SDN controller to prevent (D)DoS attacks.

The SDN controller software should have integrity and confidentiality protections. The platform which installs the SDN controller software should support hardening mechanisms such as proper configuration of ports and services, closing of unnecessary ports and services, scanning for vulnerabilities and detection of viruses.

The SDN controller should support the detection and resolution of the policy conflicts to prevent the sensitive information disclosure or security policy bypass, etc. The SDN controller should also authenticate and authorize the access from the southbound interface and northbound interface.

8.4.2 NFV orchestrator security

MANO is responsible for the management and orchestration of virtual resources. It should support the detection of presence of hardening features such as closure of unnecessary ports and services. MANO should also support vulnerability scan, virus detection and the authentication and authorization of all access from other elements in MANO and other systems.

9 Design techniques and considerations

9.1 Overview

This clause provides high-level guidance when designing and deploying network virtualization. According to the architecture of network virtualization in Figure 2, the security of network virtualization includes the following aspects:

— virtual network infrastructure security;

— virtual network function security;

— virtual network management security.

The related design techniques which are used to ensure the security of the above three aspects should be based on the security recommendations and the security controls in Clause 7 and Clause 8 respectively. Ensuring that the design techniques meet the security recommendations and the security controls should also be considered. The design techniques are listed in a) to c).

a) Design techniques for the virtual network infrastructure security

The physical interface on the hardware can be a configured username and password to achieve access control. MFA mechanisms can also be used, such as using passwords and fingerprints for access control of the physical interface on the hardware. The communication between the management system and the device can be protected using security protocols, such as SSH v2.

The secure boot which ensures the integrity of the host server can be implemented using, for example, trusted computing technology which are described in detail in 9.2.

The virtualization engine should be monitored to detect virtual machine escape and container engine escape, and the monitoring mechanism can refer to relevant standards, e.g. ETSI GS NFV SEC 013. Hardening virtualization engines can be done by referring to industry standards or best practices, such as CIS benchmarks. The detailed hardening mechanism of the virtualization engine is described in 9.3. ETSI GS NFV 001, ETSI GS NFV 002 and ETSI GS NFV 003 provide use cases, architectural framework and terminology, respectively.

In order to protect the security of the internal system, security devices (e.g. anti-DDoS, firewall, IDS/IPS) can be deployed at the network boundary of the virtual network infrastructure to protect the communication between the external system and the internal system.

b) Design techniques for the virtual network function security

The hardening of host OS, guest OS and database etc. refers to standards and best practices such as CIS benchmarks. The image of the VM and container can use HMAC for integrity protection. When a virtual machine is migrated, an overlay network that is built by VxLAN can be used to achieve security policy synchronization.

The namespace, cgroup, etc. are used to isolate the resources between containers. Username and password or MFA are used to protect access to VM or container.

The communication protection between the VNFs can be achieved by using HTTPS. For the VNF's availability, the VNF should be backed up periodically and the backed up VNF should be stored in

another data centre. A VNF can authenticate another entity (e.g. another VNF or VNFM) based on PKI technology and use TLS to protect the transmitted data.

The SDN controller orchestrates the traffic path of the virtual network function through sending the flow tables to the switches. The SDN controller should support TLS on the southbound interface and northbound interface.

c) Design techniques for the virtual network management security

The SDN controller software should be protected by the digital signature. The policies should be prioritized. For the policy with higher priority, the corresponding flow table should also have higher priority. When two policies conflict, the higher priority flow table replaces the lower priority flow table.

The detailed hardening and API security of network virtualization is described in 9.3 and 9.4, respectively.

9.2 Integrity protection of platform

Platform in this context is defined as hardware, firmware and virtual infrastructure which includes host OS, guest OS and virtualization machine manager. This platform provides an execution environment for the VM and container. If this platform is attacked, all VMs and containers that run on the platform may be attacked by the attacker. The security of the platform is therefore very important. In addition to using integrity protection algorithms (e.g. HMAC) to protect the integrity of the platform, it is also important to detect whether the platform has been tampered with. Rule automation is a well-known concept that is used to determine the trustworthiness of systems by detecting if the systems have been tampered with. NFV remote attestation architecture is described in ETSI GR NFV-SEC 018. Based on this rule automation architecture, it is possible to use technologies to achieve remote attestation for the platform. For example, using a trusted platform module to build roots of trust and combining root of trust for reporting, root of trust for measurement, and root of trust for storage.

9.3 Hardening for network virtualization

The hardening for network virtualization aims to reduce the surface of vulnerability. Appropriately setting the default configurations of network elements (including operating system software, firmware and applications) is one of the important hardening techniques. Secure configurations of network element can refer to relevant standards and best practices. CIS has developed CIS benchmarks which include benchmarks of operating systems, server software, web server, database server, virtualization, docker and kubernetes.

9.4 API authentication and authorization

OAuth 2.0 protocol as defined by IETF RFC 6749 is one solution designed to handle authorizations for API request and notification. API in network virtualization can use OAuth 2.0.

The authorization of API requests and notifications has also been defined in ETSI GS NFV-SOL 013. The access tokens and related metadata for RESTful protocols and data model for ETSI NFV MANO interfaces, and the process for the token verification by the API producer have been defined in ETSI GS NFV-SEC 022. The APIs of the virtual network management can refer to these standards.

In addition, for scenarios that provide multiple services, API gateway (e.g. security and application gateways and ingress controllers) should be used as a unified entry for applications to access services. The API gateway should have features such as a mutual transport layer security or two-way secure sockets layer, traffic redirection, guardrails and out of band validations.

9.5 Software defined security for virtual network

The traditional network security protection usually relies on physical security boundaries built by the security devices which are deployed at network borders. In the network virtualization, VNF, virtual machine and container can be created, migrated, and deleted on demand. If security boundary builds

by using the security devices, this would lead to deploying a large number of the security devices at a high cost. It takes much longer to procure and deploy security devices than it takes to bring virtual machines/containers online. So, software defined security for network virtualization is necessary. It consists of three critical components, i.e. security service of network virtualization, security control and management, virtualized security function. The security control and management component can send security policy to the virtualized security functions according to the security recommendations of the security service for network virtualization. This enables the realization of the centralized management of the virtualized security functions and provides security services to users on demand. The virtualized security functions can be orchestrated by the virtual network management to realize the scaling on-demand and reduce cost.

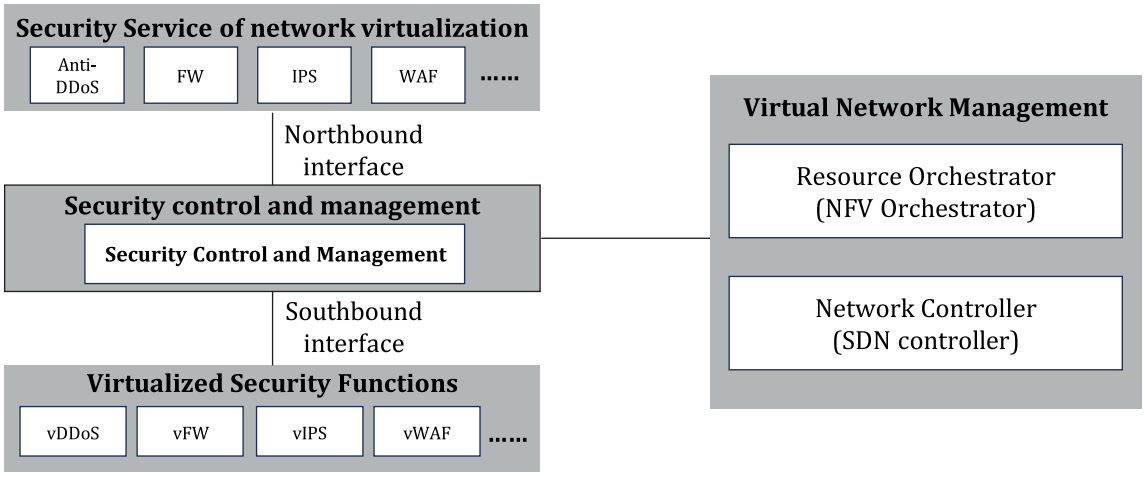

Figure 3 — Critical components of software defined security for network virtualization

The basic functions of the software defined security for network virtualization are described below and illustrated in Figure 3.

a) Security service of network virtualization

This consists of lots of security services such as anti-DDoS, firewall and IPS. A user can subscribe to a security service through the security service of network virtualization.

b) Security control and management

This consists of a security controller and manager. It can receive the security recommendations from the security service of network virtualization through the northbound interface and resolve these security recommendations into the security policies which are sent to the related virtualized security function(s). It also manages the states of all virtualized security functions which include the usage state of the resource and the execution state of the policy. When the virtualized security function does not have enough resources to provide security services to users, the security controller and manager requests the virtual network management to create new virtualized security functions and configure corresponding network connections. The security controller and manager also optimize the security policy according to the execution state of the security policy on the virtualized security function, such as deleting any redundant or expired security policies.

c) Virtualized security function

This can be thought of as VNF, i.e. security function software is deployed to a VM or container on a common server. The virtualized security function processes the data flow according to the security policies it receives from the security controller and manager. It also can send the usage state of the resource and the execution state of the policy to the security controller and manager through the southbound interface.

Annex A
(informative)

Use cases of network virtualization

A.1 Software-defined wide-area network

SD-WAN is a typical application of SDN technology. SD-WAN establishes WAN connections dynamically over all available networks including the internet and other proprietary networks. Thus, it enables connectivity between various branch offices, headquarters and data centres for a large geographically distributed enterprise.

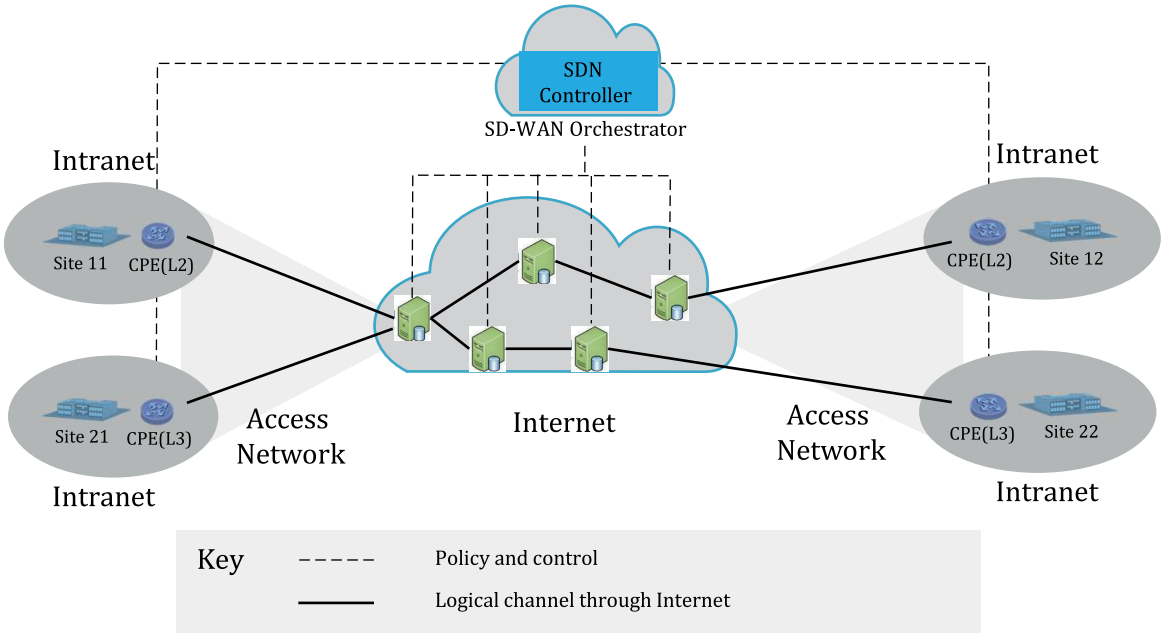

Figure A.1 — SD-WAN based on network virtualization

As shown the Figure A.1, under the control of SDN controller, virtual data channels can be generated for enterprise network to connect different sites (e.g. site 11, site 12). The policy is centrally controlled by the SDN controller (i.e. SD-WAN orchestrator) and applied onto network devices, such as customer premise equipment, switch, router, firewall and IPS.

A.2 Network slicing

5G network slice is a logical network that provides specific network capabilities and network functionalities. Differentiated services for vertical industries will be provided by network slice instances. The following Figure A.2 describes three slices (i.e. slice 1, slice 2, slice 3) for the different services.

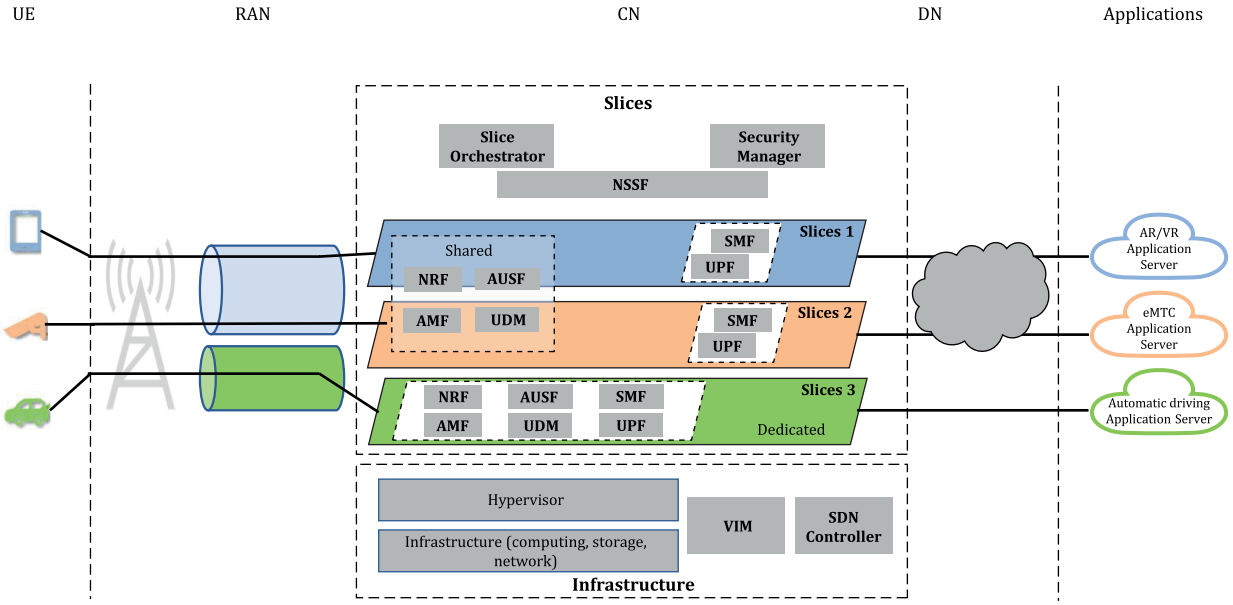

Figure A.2 — Network slicing based on SDN and NFV

By using network virtualization technology, 5G network can flexibly customize and rapidly deploy network slices according to customers' needs, including network element function and data connection. In addition, the management system of network virtualization can also provide flexible network isolation capability according to customers' needs, to ensure the security and availability of 5G slice network.

A.3 Virtual WAF

For a website, WAF provides functions such as monitoring, filtering and/or blocking data packets as they travel to and from a web application to protect the web applications against attack.

A large amount of websites are deployed in the cloud data centre. For disaster resilient reasons, these web servers should be located in multiple data centres, e.g. vWAF pool in cloud DC1, vWAF pool in cloud DC2, as shown in Figure A.3. In each data centre, WAF and web servers are deployed in the form of software and scaled in/out dynamically according to traffic.

The controller is responsible for virtualized function deployment, policy configuration and network traffic route.

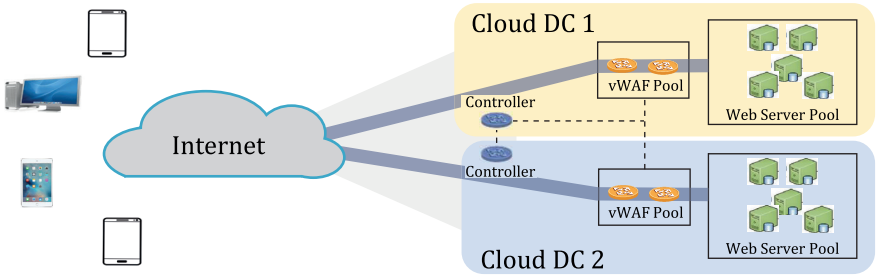

Figure A.3 — Virtualized WAF based on network virtualization

A.4 Cloud CDN with centralized control

CDN is widely used for broadband data delivery.

CDN nodes should be deployed on demand and the scheduling of user traffic under the centralized management of the controller should be optimized according to the network traffic from different geographical locations.

Each CDN site (e.g. CDN site 1, CDN site N in the Figure A.4) is deployed on demand, and load content is based on security policy.

The client traffic is routed to the most suitable site to ensure the best performance.

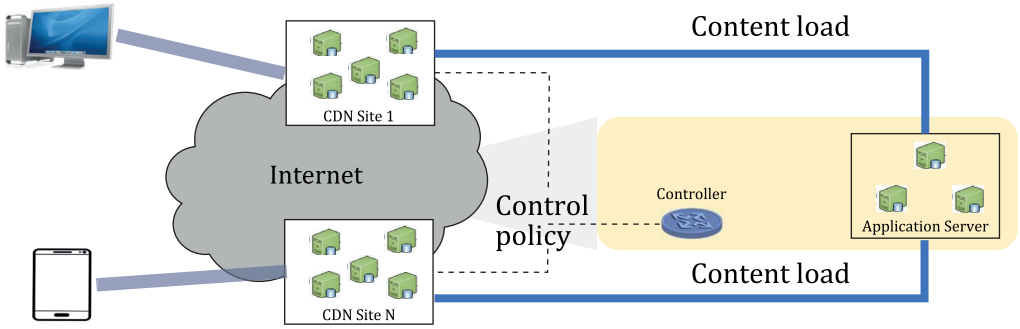

Figure A.4 — Cloud CDN based on network virtualization

Annex B
(informative)

Detailed security threat description of network virtualization

B.1 Security threats to virtual network infrastructure

The following threats should be considered.

a) Hardware: general-purpose hardware can have flaws, such as side channel attacks. X86 server and white-box switch are subject to hardware tampering and vulnerability exploitation.

b) Host OS, guest OS and virtual machine manager: operating system and software vulnerabilities, viruses, worms and Trojans are the main threats.

c) Network connection: Botnet and DDoS attacks are threats that impact network connections.

B.2 Security threats to virtual network functions

B.2.1 Security threats to virtual network function

From the prospect of virtual network function, the following threats should be taken into consideration.

a) Virtual function security

This includes the security of virtual function software and the security issues related to virtual machines or containers. For example:

1) Guest OS and software can have a large number of vulnerabilities or configuration errors and attackers can compromise the virtual function and guest OS by exploiting such security flaws.

2) Flaws such as incomplete isolation of virtual machine resources and the difficulty of monitoring traffic between virtual machines can lead to unauthorized access to virtual machines and mutual attacks between virtual machines.

3) Virtual machine and container image can be tampered with and can affect other virtual machines by spreading virus and Trojan horses.

4) Insufficient security measures for virtual machine instances themselves can lead to sensitive information disclosure.

5) The security policy does not migrate synchronously during the virtual machine migration, which can result in the security policy failing to take effect on the new virtual machine and the security risk of missing or inconsistent security configuration.

6) The communication between virtual machines is not protected, which can lead to the leakage of sensitive data in the communication content.

7) The adoption of container technology can bring new safety problems such as container safety isolation.

b) Network function security

1) When VNF's execution environment is provided by virtual machine, the security level of one VNF will affect others. VNF vulnerabilities can also be exploited by attackers, resulting in business and user information leakage, unauthorized access and other risks.

2) In addition, the security risks of traditional communication services and protocols still affect VNF. Moreover, due to the resource sharing of cloud infrastructure, the consequences of security risk will be more serious than that of traditional network elements. In addition, the traditional network metadata backup and disaster resilience mechanism is no longer applicable in the NFV environment, so it is necessary to enhance the network metadata backup and disaster resilience mechanism.

c) Data security

1) In cloud computing systems, data are stored on cloud servers with dynamic resource allocation and dynamic data access. Other business systems or administrators in cloud platforms can access data illegally, resulting in data leakage.

2) When a virtual machine is deleted or migrated, the data of a business system is deleted and transformed into residual data. The space for storing the residual data can be released to other business systems for use. If these data are not processed by special "purification", other business systems or malicious operation and maintenance personnel can obtain the key business information, triggering sensitive data disclosure.

d) Network security

1) Cloud computing system can provide abundant computing, storage and network resources for users. Virtual network has invisible traffic between virtual machines on the same physical server, which is not protected by the traditional network security monitoring means. With the increase of encrypted traffic, the traditional content-based security detection scheme fails.

2) Attackers can use the characteristics of cloud computing to launch distributed attacks by malicious use or abuse of cloud resources. Such convenience of gathering a large number of resources in a short period of time makes attempts of destructive activities easier. At the same time, it is more difficult to protect against and collect evidence.

e) Management security: compared with a traditional network, the internal operation and maintenance personnel of a cloud computing system can have a wider range of access to users' data. Without effective supervision and management, malicious internal operators can abuse data and services. The security threats of malicious internal operation and maintenance personnel becomes more and more serious in cloud computing system. ISO/IEC 27017 provides information security controls for cloud services. ISO/IEC 27018 provides guidance for the protection of personally identifiable information in public cloud services.

B.2.2 Security threats to software-defined networks

a) Attackers can communicate with vSwitch, virtual function applications to obtain sensitive information. An attacker can also acquire sensitive data or tamper with data transmitted on southbound and northbound interfaces, such as flow table forwarding rules.

b) In addition, a complete flow table usually involves the co-configuration and effectiveness of policies on multiple switches. If there is no uniform policy activation mechanism in policy planning, configuration and download, and the policy activation time on different switches is different, the forwarding behaviour of switches can be inconsistent, which can give attackers a chance to take advantage of.

B.3 Security threats to virtual network management

B.3.1 General

SDN and NFV technology have changed the traditional "SOLO" model of business deployment. In the future, network virtualization suppliers will include virtual layer equipment providers, hardware providers, business software providers, MANO equipment providers, SDN controller providers and other vendors. Improper isolation measures can lead to VNF security problems or business errors by

exploiting vulnerability in one component system to attack other systems, or by obtaining sensitive data from other vendors' VNF or deliberately tampering with different vendors' VNF.

Facing a new ecology, SDN/NFV uses new technology and will have a greater impact on the technical selection, system construction and business operation and maintenance of operators' networks. It should be constantly strengthened in technical capacity and practical experience. SDN network has the characteristics of separation of control functions and traffic forwarding functions, centralization of control functions and together with open interfaces, has the following security risks as described in B.3.2 to B.3.4.

B.3.2 Software-defined networks controller security

a) The attacker takes advantage of the centralized control functions of the SDN controller to launch (D)DoS attacks using the SDN controller, such as sending malformed messages to multiple switches continuously, and sending messages that do not match the OpenFlow flow table through the south-facing interface, which can result in the processing overload of the controller.

b) In addition, the vulnerabilities of SDN controller software itself can be exploited by attackers, who can also implant viruses and Trojans. Attackers can also attack SDN controllers by attacking platforms that install controller software to get network topologies or tamper flow table rules. Once the controller is controlled by the attacker, the attacker can control the traffic of the whole network, and the security risk is very serious.

c) In addition, in the face of many SDN applications, different users and different applications of the same user, the flow tables generated by their control strategies can conflict, and if the conflict is not handled properly, security vulnerabilities can arise.

B.3.3 Management and orchestration security

With its unique virtual resource management and scheduling capabilities, NFV systems can be attacked to exploit MANO vulnerabilities. Once an attacker controls the MANO system, the attacker will control the management and arrangement of virtual resources in the whole resource pool. An attacker can also fake a network element or other system in the MANO system to communicate with the MANO network element, thus carrying out security attacks such as obtaining virtual resource information of business network elements or maliciously requesting virtual resources.

B.3.4 Interface security

If the API of MANO is not well protected, it can be illegally accessed and abused by attackers. For example, if an identity request service from the VIM is not strictly protected, attackers can maliciously impersonate identity to achieve unauthorized access to resources in the NFV system.

B.4 Virtualization-specific threats

B.4.1 Threats to network segmentation

In larger-scale environments with hundreds of hosts and thousands of virtual machines or containers, network segmentation should be utilized to protect virtual network function and limit security infects.

For example, separate hosting zones or networks can be designed to not only isolate virtual machines and containers but also to isolate network traffic more discretely, so that traffic for virtual network functions of one sensitivity level is separate from that of other sensitivity levels.

B.4.2 Threats to resource exhaustion

There are two ways to consume virtualization resources:

— using the scale-in/scale-out mechanism in the virtualization system by generating a large number of concurrent service requests at the same time;

— faking the resource allocation signalling from the centralized management system.

B.4.3 Threats to centralized management

SDN and NFV, as new technologies, are based on the idea of centralized control and management. Centralized control and management system (i.e. NFV orchestrator, SDN controller) is the focus of attackers. Once the attacker obtains the authorization of these centralized control systems, the attacker will control the whole system. The attacker can also exploit the centralized control system for security attacks such as obtaining service configuration or maliciously obtaining virtual resources.

Bibliography

[1] ISO/IEC 22123-1:2023, *Information technology — Cloud computing — Part 1: Vocabulary*

[2] ISO/IEC 22123-2, *Information technology — Cloud computing — Part 2: Concepts*

[3] ISO/IEC 22123-3, *Information technology — Cloud computing — Part 3: Reference architecture*

[4] ISO/IEC 21878, *Information technology — Security techniques — Security guidelines for design and implementation of virtualized servers*

[5] ISO/IEC/TR 22417:2017, *Information technology — Internet of things (IoT) use cases*

[6] ISO/IEC/IEEE 24765:2017, *Systems and software engineering — Vocabulary*

[7] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[8] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[9] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[10] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[11] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[12] ISO/IEC/TR 29181-1:2012, *Information technology — Future Network — Problem statement and requirements — Part 1: Overall aspects*

[13] ETSI GS NFV 001:2013, *Network Functions Virtualisation (NFV); Use Cases*

[14] ETSI GS NFV 002:2014, *Network Functions Virtualisation (NFV); Architectural Framework*

[15] ETSI GS NFV 003:2014, *Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV*

[16] ETSI GS NFV-SOL 013:2017, *Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification*

[17] ETSI GR NFV-SEC 018:2019, *Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture*

[18] ETSI GS NFV-SEC 022:2019, *Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access*

[19] IETF *The OAuth 2.0 Authorization Framework* (RFC 6749), October 2012

[20] IETF *Service Function Chaining(SFC) Architecture* (RFC 7665), October 2015

[21] Recommendation ITU-T Y 3300:2014, *Framework of software-defined networking*

[22] NIST Special Publication 800-190 — *Application Container Security Guide*, September 2017

[23] SDN, NFV and All That https://www.ietfjournal.org/sdn-nfv-and-all-that/

[24] Network Functions Virtualisation https://www.etsi.org/technologies/nfv

[25] NETWORK VIRTUALIZATION RESEARCH CHALLENGES. (RFC 8568) https://datatracker.ietf.org/doc/rfc8568/?include_text=1

[26] Network Function Virtualization https://datatracker.ietf.org/rg/nfvrg/about/

[27] Deterministic Networking https://datatracker.ietf.org/wg/detnet/about/

[28] Autonomic Networking Integrated Model and Approach https://datatracker.ietf.org/wg/anima/about/

[29] Path Computation Element https://datatracker.ietf.org/wg/pce/about/

[30] Interface to Network Security Functions https://datatracker.ietf.org/wg/i2nsf/about/

[31] Network Virtualization Overlays https://datatracker.ietf.org/wg/nvo3/about/

ICS 35.030

Price based on 23 pages