# NETWORK VIRTUALIZATION SECURITY: THREATS, MEASURES, AND USE CASES

*Qin, Qiu[1]; Sijia, Xu[1]; Shenglan, Liu[2]; Tianni Xu[1]; Bei Zhao[2]*

[1]China Mobile Communications Group Co., Ltd, China.

[2]China Mobile Group Design Institute Co., Ltd, China.

**ABSTRACT**

*With the rapid development of technologies such as 5G, cloud computing, and big data, network virtualization technology has been widely applied, effectively improving the utilization of resources such as computing, storage, and network, as well as the flexibility of IT systems or networks, reducing system maintenance costs. However, at the same time, the complexity of network virtualization environment makes security threats more covert and diverse, and traditional security protection methods are difficult to cope with, which also brings many security risks. This article analyzes the current development status and related work of network virtualization, sorts out the security threats of network virtualization, summarizes the characteristics and architecture of network virtualization technology, and further introduces the security measures and typical use cases of network virtualization, which can be used to guide and promote network virtualization security.*

**Keywords** – network virtualization, security threats, security measures

## 1. INTRODUCTION

### 1.1 Trend of development

Traditional communication networks adopt relatively centralized network architectures, streamlined network construction and operation models, which are difficult to support the development of network scale. SDN/NFV technology is driving the transformation of communication networks, moving them towards virtualized networks, achieving agile development and iteration, dynamic resource allocation, and elastic scalability of communication networks.

While network virtualization technology brings a series of conveniences, the new features and changes it introduces also bring security risks. It is necessary to analyze its characteristics and propose relevant response strategies to promote the security and sustainable development of the telecommunication and Internet industries.

### 1.2 Characteristics of Network Virtualization

The application of new technologies such as SDN and NFV has driven the continuous development of network technology, bringing revolutionary changes to network virtualization. ISO/IEC 27033-7 considers the characteristics of network virtualization technology, and summarizes the changes in network virtualization include:

- Introduced a centralized controller. The NFV orchestrator is responsible for infrastructure and resource allocation, scheduling, and lifecycle management, while the SDN controller is responsible for network topology and virtual data link management.

- Virtual network elements' behavior is guided by a controller, which are different from physical components . Software, services, and functions running on virtualization infrastructure can be deployed as needed, demonstrating extremely high flexibility and response speed.

- The data link has been changed. In addition to physical data links, new technologies such as SDN and SFC can also provide efficient virtualized data links according to application requirements, which will improve the efficiency of internal data transmission in the system.

**Table 1- Abbreviations Table**

| Abbreviations | Full name |
|---|---|
| 5G | 5th generation mobile network |
| ACL | Access control list |
| API | Application programming interface |
| AV | Anti virus |
| DoS | Denial of service |
| DDoS | Distributed denial of service |
| ETSI | European Telecommunications Standards Institute |
| IDS | Intrusion detection system |
| IEC | International Electrotechnical Commission |
| IPS | Intrusion prevention system |

| | |
|---|---|
| ISO | International Organization for Standardization |
| IT | Information technology |
| ITU | International Telecommunication Union |
| MANO | Management and orchestration |
| NFV | Network function virtualization |
| NSaaS | Network Security as a Service |
| NVS | Network virtualization services |
| OMC | Operation maintenance centre |
| PoP | Point of presence |
| PKI | Public key infrastructure |
| SDN | Software-defined networking |
| SD-WAN | Software-defined wide-area network |
| SFC | Service function chain |
| VM | Virtual machine |
| VMM | Virtual machine manager |
| VNF | Virtual network function |
| VNFM | Virtual network function manager |
| vCPU | Virtual CPU |
| vI/O | Virtual I/O |
| vMemory | Virtual memory |
| vRouter | Virtual router |
| vSwitch | Virtual switch |

## 2. RELATED WORK

In recent years, network virtualization technology and its security issues have received much attention. ETSI specifically released a series of standards on network virtualization [1-5]. In addition, ITU has also closely explored related topics such as software defined network frameworks [6]. Scholars have also conducted numerous studies on the security issues of network virtualization. In [7], a comprehensive investigation and sorting of the current situation of network virtualization security was conducted. In [8], a detailed analysis was conducted on network function virtualization in multi-tenant cloud environments. [9] focus on the optimization of NFV chain deployment in software defined cellular cores. [10] summarizes the challenges and opportunities faced by network virtualization and provides effective guidance for the security development of network virtualization.

The above related work analyzes the security risks of NFV, the security requirements of the host system and the security requirements of SDN, which can be used as a reference for virtual network security but does not involve the virtual network security framework and systematic security technical requirements.

This article will systematically analyze and propose measures to solve the security threats of virtual network infrastructure, virtual network function, and control and management in virtual networks, and introduced some network virtualization security use cases, which aims to provide reference for stakeholders to protect network virtualization security.

## 3. NETWORK VIRTUALIZATION SECURITY THREATS

With the rapid development and widespread application of network virtualization technology, its security issues are increasingly receiving attention. Network virtualization brings advantages in resource flexibility and business agility. At the same time, it also brings a series of security threats, including virus attacks, malware implantation, information leakage, etc. [11-12], as shown in Figure 1.

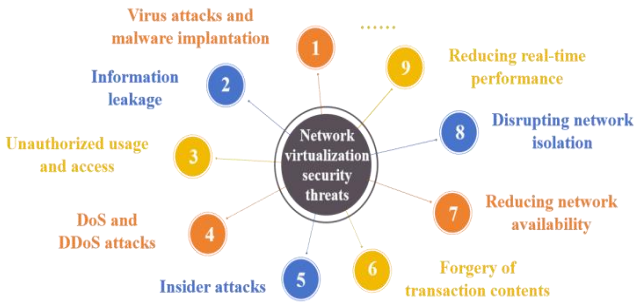


**Figure 1- Network virtualization security threats**

- Virus attacks and malware implantation. In network virtualization, the host operating system and client operating system of virtual network functions, SDN controller software, MANO operating system, etc. might be attacked by viruses and malware.

- Information leakage. After deleting the VM, if special "purification" processing is not performed on the data, other business systems or malicious operation and maintenance personnel may obtain the original business key information, thereby triggering sensitive data leakage.

- Unauthorized usage and access. Unauthorized attackers may use and access data from MANO's VM or API, as well as leveraging defects such as incomplete isolation of VM resources and difficulties in monitoring traffic between VMs, which may lead to unauthorized access to VMs.

- DoS and DDoS attacks. Attackers might use many switches to forward a large number of packets to the SDN controller, causing the SDN controller to be subjected to (D) DoS attacks.

- Insider attacks. Malicious administrators might tamper with images or change security configurations intentionally, or make security misconfigurations (such as opening unnecessary ports on VNF) and launch attacks.

- Forgery of transaction contents. The transaction content of VM can be tampered with by attackers, who can also forge network elements or other systems in

the MANO system, communicate with MANO network elements, and launch attacks.

- Reducing network availability. Backup data loss, inability to recover critical data and business status, will make business unavailable, which may lead to serious consequences such as service interruption, customer loss, and reputation damage for the enterprise.

- Disrupting network isolation. Attackers can use the compromised VM as a springboard, bypass traditional network isolation mechanisms, and utilize shared physical resources, network connections, or management interfaces to further access and attack other VMs;

- Reducing real-time performance. Attackers use VMs to maliciously deplete host resources, thereby affecting the real-time performance of other VMs on the host, such as causing service response delays, reduced data transmission rates, or application crashes, which is particularly fatal for businesses with high real-time requirements.

## 4. NETWORK VIRTUALIZATION ARCHITECTURE

### 4.1 Network virtualization architecture

By analyzing the components and architecture of network virtualization, it mainly consists of three parts: virtualization network Infrastructure, virtual network function, and management system, as shown in Figure 2.

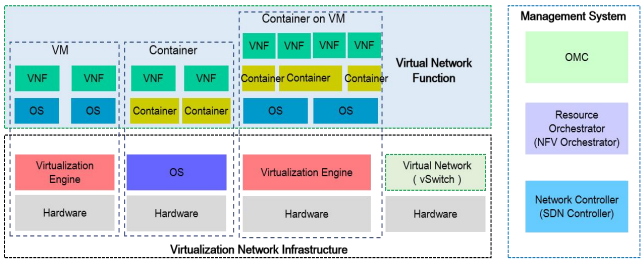


**Figure 2- Network virtualization components and architecture**

### 4.2 Virtualization Network Infrastructure

The virtualization network infrastructure consists of virtual machine managers (VMMs), host operating systems, and hardware resources including bare metal, switches, routers, storage devices, etc. VMMs extract hardware resources to form upper level virtual computing, storage, and network resources. Typical VMMs include VM management programs and container engines.

### 4.3 Virtual Network Function

In order to deploy network functions in virtualization network infrastructure based on virtualization, VNFs should be introduced and data connections should be created as needed between VNFs under the scheduling of SDN controllers. A standard method is formed by VNF, vRouter, and vSwitch to dynamically provide network function from SDN controllers. SDN can significantly improve the flexibility and automation of network functions, while significantly reducing network operating costs.

### 4.4 Management System

In addition to operation maintenance centre (OMC), the network virtualization architecture also adds SDN controllers and NFV orchestrators. The NFV orchestrator is responsible for the allocation, scheduling, and lifecycle management of infrastructure and resources, while the SDN controller is responsible for network topology and virtual data link management.

## 5. NETWORK VIRTUALIZATION SECURITY MEASURES

### 5.1 Virtualization Network Infrastructure Security

#### *5.1.1 Hardware*

The hardware in network virtualization should be deployed in a secure environment. For example, the houses where the hardware deployed should be equipped with waterproof, seismic, and access control mechanisms. The physical interface on the hardware should be configured with access control mechanisms to implement authentication and authorization access. Administrators should through authentication and authorization when logging into the device. If using a password, the complexity of the password should be ensured. The communication between management systems and devices should be protected to ensure confidentiality and integrity. The host server should also support secure boot to ensure the integrity.

#### *5.1.2 Virtualization Engine*

The virtualization engine should support detection and prevention of VM escape and container engine escape. At the same time, security reinforcement measures should be taken for the host operating system, VMMs, and container engines, such as correctly configuring ports and services, closing unnecessary ports and services, scanning for vulnerabilities, and detecting viruses. The virtualization engine should also support resource isolation, such as isolating the vCPU, vMemory, and vI/O resources used by different VMs. All access should be authenticated and authorized, such as mutual access between VMs, virtualization engine access to VMs/containers, or administrator access to VMs.

#### *5.1.3 Network Connection*

For network boundary protection, security devices such as anti DDoS, firewall, IDS/IPS can be deployed at the network boundary of virtualization network infrastructure to perform network detection and defense, thereby protecting communication between internal and external systems. The physical server should also support traffic separation and transmit management services, signaling services, and data services through different interfaces, effectively reducing interference and risks between different services. In addition, regular security audits and vulnerability scans are required to promptly identify and fix potential security vulnerabilities.

## 5.2 Virtual Network Function Security

### *5.2.1 VM Security*

The customer's operating system should be reinforced with security measures, such as closing unnecessary ports and services, scanning for vulnerabilities, virus detection, and resource isolation. The integrity and confidentiality of the VM's image should be protected, and secure storage should be carried out to prevent unauthorized access. When migrating VMs, security policies should be synchronized to ensure their continuity and availability. In addition, all access to the VM should be authenticated and authorized.

### *5.2.2 Container Security*

As for container security, it is crucial to ensure resource isolation between containers and between containers and host operating systems. The secure storage of image warehouses and container images is an important aspect of ensuring container security. Measures should be taken to protect the integrity and confidentiality of image warehouses and container images, and secure storage should be carried out to prevent unauthorized access. At the same time, all access to containers should be authenticated and authorized to achieve fine-grained permission management for container operations.

### *5.2.3 Data Security*

We should provide full lifecycle security protection for VNF data, including at least secure storage, allowing only authenticated and authorized access, and thoroughly removing residual data. VNF should support authentication and authorization of access to others, as well as encryption and integrity protection of transmitted data. In addition, VNF should be backed up and stored in another data center. VNF can authenticate other entities based on PKI and use TLS protocol to protect data during transmission.

### *5.2.4 Network Security*

VNF traffic can be monitored and analyzed using technologies such as artificial intelligence and big data. When an attack is detected, corresponding security measures should be taken, such as blocking all traffic from malicious VNFs and migrating traffic from malicious VNFs to new secure VNFs. Meanwhile, security error configuration control should be supported, and the entry whitelist at each subnet level can be used to limit the explosion radius. In addition, virtualization network function should also use security protocols to protect communication with other VNFs or management components, and establish disaster recovery mechanisms.

### *5.2.5 Manage Security*

VNF should support authentication and authorization of access for internal operations and maintenance personnel. The SDN controller should support the protection of confidentiality and integrity of data transmitted in both south and north directions. The SDN controller should check whether the policy is effective for the switch, and achieve policy synchronization between the SDN controller and the switch. If the policy is not synchronized, the SDN controller will find the policy. The availability of software defined networks should not be affected by security attacks related to configuration options or time, such as the duration of reconfiguration.

## 5.3 Virtual Network Management Security

### *5.3.1 SDN Controller Security*

The SDN controller should be able to detect (D) DoS attacks from both southbound and northbound interfaces, and will take appropriate security measures to deal with (D) DoS attacks. At the same time, the integrity and confidentiality of the SDN controller software should be protected. The platform where SDN controller software installed should undergo security reinforcement, such as correctly configuring ports and services, closing unnecessary ports and services, scanning for vulnerabilities, and detecting viruses. In addition, the SDN controller should also support detection and resolution of policy conflicts, authentication and authorization of access to southbound and northbound interfaces, etc.

### *5.3.2 NFV Orchestrator Security*

MANO is responsible for the management and orchestration of virtual resources and should support reinforcement detection to ensure that unnecessary ports and services in the system are closed. In addition, regular vulnerability scanning and virus detection are also essential. At the same time, MANO should also implement strict access control policies, authenticate and authorize all requests to access MANO and other elements in the system, ensuring that only authorized users can access and operate related resources, and significantly improving the security of the entire system.

# 6. NETWORK VIRTUALIZATION SECURITY USE CASES

## 6.1 SD-WAN

SD-WAN is a typical application of SDN technology, which combines network virtualization technology to achieve centralized management and optimization of wide area network connections. SD-WAN establishes WAN connection through the Internet and connects enterprise networks with different geographical distances, including branch sites, breaking the limitations of traditional network architecture. SD-WAN based on network virtualization is gradually becoming the preferred solution for enterprise network architecture due to its efficient, flexible, and secure characteristics [13-14].

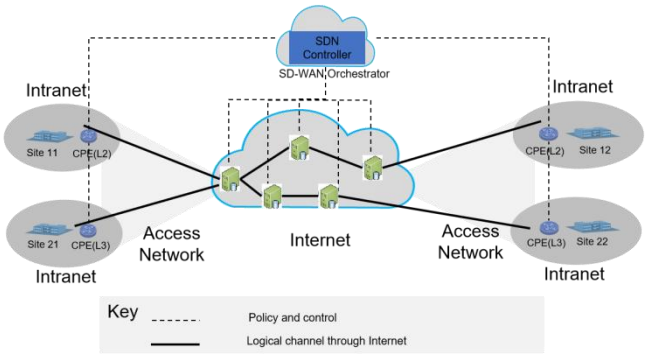


**Figure 3- SD-WAN based on network virtualization**

As shown in Figure 3, under the control of the SDN controller, virtual data channels can be generated for the enterprise network to connect different sites (such as site 11 and site 12). This strategy is centrally controlled by the SDN controller (i.e. SD-WAN orchestrator) and applied to network devices such as customer home devices, switches, routers, firewalls, and IPS.

By utilizing SD-WAN, enterprises can flexibly configure and manage their networks without setting up specialized hardware or network devices at each branch site. This centralized control not only simplifies network management, but also improves network security. The benefits and advantages are as follows:

- High flexibility: Virtual data channels in SD-WAN can be quickly established and adjusted according to business requirements, without tedious physical circuit laying and configuration work.
- Stability and reliability: The SDN controller can monitor network status and adjust routing in real-time to ensure the stability and reliability of data channels.
- Enhance security protection capabilities: By integrating security devices such as firewalls and IPS, SDN technology can provide powerful security protection capabilities to protect enterprise data from attacks and leaks.
- Reduce operation and maintenance costs: The SDN controller provides a unified network management platform, simplifying the configuration and management process of network devices, and reducing operation and maintenance costs.

## 6.2 Network Slicing

Network slicing is a on-demand customized network service approach that is based on network virtualization technology, dividing a physical network into multiple logically independent, customized virtual networks. Each slice can be independently designed, deployed, and managed to meet the network needs of different industries and scenarios.

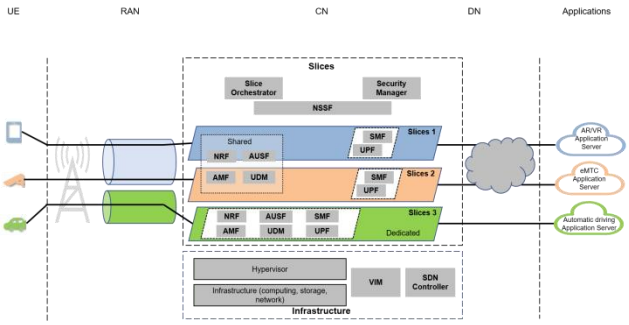


**Figure 4- Network Slicing Based on SDN and NFV**

As shown in Figure 4, three slices of different services are deployed (i.e. slice 1, slice 2, and slice 3). By using network virtualization technology, 5G networks can flexibly customize and quickly deploy network slices according to customer needs [15]. These slices not only cover network element functions, but also involve data connections, ensuring that each slice can meet specific business needs from customer.

In addition, the network virtualization management system can flexibly provide refined network isolation capabilities according to customer needs. The data flow and information exchange between different slices are strictly controlled, thereby avoiding potential security risks. It not only ensures the independence between slices, effectively enhances the security and availability of 5G slice networks, but also provides differentiated services for vertical industries and ensures their safe and stable operation of business. The advantages can be mainly summarized in the following aspects:

- Improve resource utilization: Network slicing can effectively utilize physical network resources, create slices according to demand, dynamically allocate resources as needed, and avoid resource waste.
- Improve key performance: Network slicing can optimize performance according to business needs, ensuring that key indicators such as data transmission speed, latency, and bandwidth within the slicing reach optimal levels.

- Enhance network security: The isolation between network slices ensures independence between different slices, not only preventing potential interference between slices, but also enhancing the security of the sliced network.

- Rapid response to market changes: The flexibility of network slicing enables telecommunications operators to respond quickly to market changes and meet new business needs by quickly creating slices.

### 6.3 NSaaS

Shifting an enterprise's applications and data to the cloud introduces numerous benefits, such as reducing operational costs and increasing competitive advantages. However, it also expands an organization's cyber-attack surface and makes them vulnerable to many cyber threats. NSaaS is a new cloud-native network security deployment service solving this challenge. NSaaS inspects and protects against malicious ingress, egress, and east-west traffic within an organization's network.

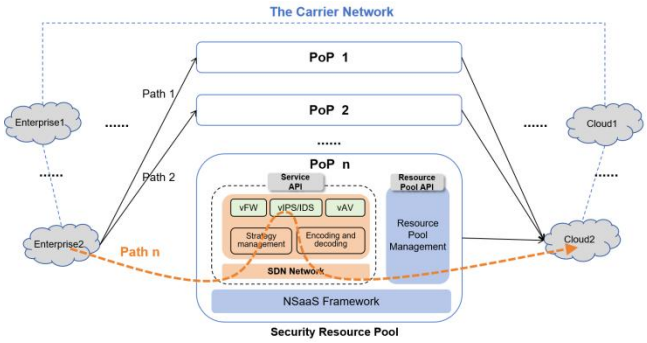


**Figure 5- NSaaS Based on SDN and NFV**

At present, there are use cases applying the NSaaS in carrier networks, leveraging the technology of network virtualization security. In this case, PoP nodes are deployed on the private cloud network, and cloud-based security functions are deployed on the PoPs to form a security resource pool. SDN and network virtualization technologies drain user traffic in the private cloud network and use security resource pools to implement IDS, IPS, AV, etc. NSaaS provides centralized, flexible orchestration and scheduling network security services for individuals, households, and enterprise connected to carrier networks. The advantages and benefits of deploying NSaaS include:

- Enhance safety protection capabilities; Operators can monitor network traffic in real-time, accurately identify and block malicious entrances, exits, and east-west traffic, effectively reducing the success rate of network attacks and protecting the integrity and confidentiality of user data.

- Flexibility and Scalability: NSaaS is a cloud native security deployment service that can be flexibly configured and expanded according to business needs. Whether it is adding security features or adjusting security resources, it can be quickly implemented.

- Reduce costs and improve efficiency: Through the cloud based security function, NSaaS achieves the sharing and reuse of security resources, reduces the security cost of individual users, and improves the efficiency of security investment.

- Improve the efficiency of security management operations: NSaaS achieves centralized management and flexible scheduling of security services, simplifies network security management processes, reduces operating costs, and improves the operational efficiency of operators.

## 7. CONCLUSION

Based on the above analyzation, this article provides guidance on the security development of network virtualization, solves the security threats faced by network virtualization, and proposes use cases for SD-WAN, network slicing, and NSaaS, which can be used to guide relevant parties in the industry for reference. Mainly including the following aspects:

- Introduced the current development status of network virtualization, as well as the relevant work in the industry on network virtualization security.

- Sorted and analyzed the security threats faced by network virtualization, including virus attacks, malware implantation, information leakage, unauthorized use and access, etc.

- Introduced the characteristics of network virtualization and analyzed the components and architecture of network virtualization, including virtualization network infrastructure, virtual network function, and management system.

- Provided network virtualization security control measures, mainly proposing detailed security control measures for virtualization network infrastructure security, virtual network function security, and virtual network management security.

- Analyzed typical use cases and achievements of network virtualization security, including SD-WAN, network slicing, and NSaaS.

In the future, with the deepening application of artificial intelligence and big data technology, network virtualization will become more intelligent and automated, achieving more accurate risk identification and more efficient threat response. Network virtualization security is a complex and arduous task that requires joint efforts from the industry to continuously achieve technological innovation.

## REFERENCES


[1] ETSI GS NFV 001:2013, Network Functions Virtualisation (NFV); Use Cases [S], ETSI.

[2] ETSI GS NFV 002:2014, Network Functions Virtualisation (NFV); Architectural Framework [S], ETSI.

[3] ETSI GS NFVSOL 013:2017, Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification [S], ETSI.

[4] ETSI GR NFVSEC 018:2019, Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture [S], ETSI.

[5] ETSI GS NFVSEC 022:2019, Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access [S], ETSI.

[6] [ITU-T Y.3300], Recommendation ITU-T Y.3300:2014, Framework of softwaredefined networking.

[7] Yang W , Fung C .A survey on security in network functions virtualization[C]//Netsoft Conference & Workshops.IEEE, 2016:15-19.

[8] Yu R , Xue G , Kilari V T ,et al.Network function virtualization in the multi-tenant cloud[J].Network IEEE, 2015, 29(3):42-47.

[9] Zheng J , Tian C , Dai H ,et al.Optimizing NFV Chain Deployment in Software-Defined Cellular Core[J].IEEE Journal on Selected Areas in Communications, 2020, 38(2):248-262.

[10] Han B , Gopalakrishnan V , Ji L ,et al.Network function virtualization: Challenges and opportunities for innovations[J].IEEE Communications Magazine, 2015, 53(2):90-97.

[11] Lal S , Taleb T , Dutta A .NFV: Security Threats and Best Practices[J].IEEE Communications Magazine, 2017, PP(8):2-8.

[12] Aljuhani A , Alharbi T .Virtualized Network Functions security attacks and vulnerabilities[J].IEEE, 2017:1-4.

[13] Liyanage M , Ahmed I , Okwuibe J ,et al.Enhancing Security of Software Defined Mobile Networks[J].IEEE Access, 2017, 5(99):9422-9438.

[14] Yigit B , Gur G , Tellenbach B ,et al.Secured Communication Channels in Software-Defined Networks[J].IEEE Communications Magazine, 2019, 57(10):63-69.

[15] Abdelwahab S , Hamdaoui B , Guizani M ,et al.Network function virtualization in 5G[J].IEEE Communications Magazine, 2016, 54(4):84-91.