Novel VNFI Security Management Function Block For Improved Security Framework For SDN/NFV Networks

Rahaf Hamoud Alruwaili[i], Haifa Khaled Alanazi[+], Saloua Hendaoui*
Rahafhamoud1418@gmail.com, Haifa11khaled@gmail.com, selhechi@ju.edu.sa
Department of computer Science, College of Computer and Information Sciences, Jouf University, Jouf, Skaka, Saudi Arabia

Abstract
Software Defined Networking (SDN) is a novel approach that have accelerated the development of numerous technologies such as policy-based access control, network virtualization, and others. It allows to boost network architectural flexibility and expedite the return on investment. However, this increases the system's complexity, necessitating the expenditure of dollars to assure the system's security. Network Function Virtualization (NFV) opens up new possibilities for network engineers, but it also raises security concerns. A number of Internet service providers and network equipment manufacturers are grappling with the difficulty of developing and characterizing NFVs and related technologies. Through Moodle's efforts to maintain security, this paper presents a detailed review of security-related challenges in software-defined networks and network virtualization services.

Keywords:
SDN, NFV, Security, issues.

1. Introduction

All modern networks are traditionally built on the basis of several special equipment that implement the distributed protocol suite and work specifically for a company-owned software package. These distributed protocols implement a different set of services such as access control, proper routing, quality of service, topology discovery, and others. The task faced by all network operators, in this case, is the process of installing these various devices and configuring all the special protocols that are specifically planned to be used on the network. This diversity and difficult combination of network management and data transmission control functions within vendor equipment slows down the delivery of new modern services and limits innovation in modern networks. The use of a standards-based, programming-based, open networking approach is key to the deployment of Software Defined Networking (SDN). Therefore, rapid, and effective advances in diverse computing and networking technologies have enabled and defined a diverse and efficient set of applications with diverse and different requirements on all network services. The diverse and dynamic network services required by today's emerging applications may bring a variety of new challenges for the provision of network services in the future. Software Defined Networking (SDN) and Network Function Virtualization (NFV) are a group of very important recent and new innovations that are expected to effectively address these challenges [1].

SDN separates a set of functions, including all the functions that control the network and the functions specialized in redirecting data traffic in order to not be able to control the main central and programmable process in the network. SDN includes a set of major components of the engineering process at the data level and consists of multiple network sources for forwarding traffic, and a control plane that includes and includes controllers. The interface that provides control between groups of levels for control and data is called the south interface while the interface for the control application is called the north interface. The benefits promised by SDN include simplified and enhanced network control and control, flexible and efficient network management, and improved network service performance.

Network virtualization has introduced a specific abstraction of the underlying infrastructure in which multiple virtual networks with an alternate architecture can be built in order to meet all the requirements of various services [2]. More recently, ETSI developed Network Function Virtualization (NFV), a specific network architecture concept that uses several virtualization techniques to transfer all private functions in a network from hardware in use to software applications. Essentially, NFV adopts a proprietary concept for network virtualization and provides a set of specific mechanisms to separate service functions from infrastructures. The advantages offered by NFV include simplified service development, more secure and flexible service delivery, and reduced network capital and operating costs.

The remaining of this paper is organized as follow: In section II, we detail the main principles of network virtualization then in section III we highlight the main security challenges of SDN/NFV networks. Section IV

Manuscript received October 5, 2022
Manuscript revised October 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.10.39

summarizes the main security schemes and in section V we explain our proposed block in the SDN/NFV architecture. Section VI summarizes this paper.

II. Network virtualization

NFV and SDN use network abstraction, but they do it in different ways. Despite the popularity of bringing virtualization to the network, confusion reigns over two different but related approaches: Software Defined Networking and Network Function Virtualization. In the following subsections, we explore the differences between the techniques.

II.1. Network Functions Virtualization (NFV)

Network Function Virtualization (NFV): The concept that virtualizes the main elements of a network, rather than having dedicated hardware to provide a particular functionality where software running on a computer or server is used. In this way, the whole classes of network node functions can be set up as building blocks that can be connected to create public communication networks.

In NFV, network functions run as software modules on x86 servers. An NFV infrastructure, or NFVI, provides the underlying computing, storage, and network resources required for NFV which uses traditional server virtualization but greatly advances the concept. Therefore, one or more virtual machines may run different software that provides different operations. In addition to industry-standard high-volume servers, it can also provide switches, storage, or even cloud computing infrastructure functions as an alternative to dedicated hardware, each with a network function [3].

II.2. Software Defined Networking (SDN)

In an SDN architecture, control and data levels are separated, network and state intelligence are centralized, and the underlying network infrastructure is extracted from applications. Software Defined Networking “SDN”: It is a network technology that is controlled through software functions to enable it to be adaptable, dynamic, manageable, and cost-effective. SDN architecture separates the network control functions and redirects so that control of the network is directly programmable, and then the underlying infrastructure for applications and network services is extracted[4].

II.3. SDN vs. NFV: Similarities and Differences

The primary similarity between SDN and NFV is that they use a network abstraction process. SDN always seeks to separate all network control functions from those of network forwarding, while NFV always seeks to strip network forwarding and other network functions from the devices in use and on which it is running. Thus, both rely heavily and significantly on virtualization to provide and enable network and infrastructure design to be abstracted into software and then implemented by software platforms across hardware platforms [5].

When used in conjunction with the NFV architecture, SDN is responsible for passing data packets from one network device to another. At the same time, the virtual machine somewhere on the network hosts the set of SDN control services for routing, policy formulation, and applications. As a result, while NFV provides basic networking capabilities, SDN manages and regulates it for individual applications [6]. Configuration and behavior can also be defined and modified programmatically using SDN.

The way SDN and NFV separate abstract functions and resources are different. SDN abstracts physical network resources - switches, routers, etc. - and moves decision-making to the level of virtual network management. The level of control determines where the traffic is routed in this way, while the device continues to route and handle the traffic. NFV intends to turn all physical network resources into a hypervisor by default, allowing the network to scale without requiring more hardware.

In addition to making network architectures more flexible and dynamic, SDN and NFV play different roles in defining those architectures and the infrastructure that supports them [6].

Networking software with SDN and NFV has attracted a lot of attention lately in many industries and academia. In fact, due to the use of software networks and the work of many different vulnerabilities, they are discovered and used by many attackers. To deal with security threats effectively, security experts share their knowledge, through the use of different programming languages. In this paper, we present some of the security issues that SDN/NFV faces, what are the possible security solutions and what are the causes of security threats.

III. Security Challenges for NFV and SDN.

This section summarizes current security-related issues and challenges for SDN and NFV.

It is generally recognized that confidentiality, integrity, availability, reliability, and accountability are the five core security functions needed to protect the system (CIAAA). Confidentiality ensures that private and sensitive information is not disclosed or disclosed regarding data or persons to unauthorized users. Unauthorized users cannot interfere with the information or the intended function of the system unless done in error or on purpose. Availability ensures that unauthorized users are not denied access to systems and services. Credibility ensures that people can be validated and trusted for who they say they are and that the system's input stems from a trustworthy source.

Real and virtual entities, interconnected infrastructure, and interactions between entities through infrastructure constitute a system, organization, or cyberspace. Real and virtual entities include physical things such as humans, computers, sensors, mobile phones, and electrical gadgets, as well as virtual abstractions such as data/information, software, and services. Networks, databases, information, and storage systems are examples of infrastructure that connects and supports things in a system/space. With an interconnected infrastructure and information about communications, politics, business, and management, the interaction includes actions and interdependence between system/cyberspace entities. Systems, tools, processes, practices, concepts, and strategies to prevent and protect cyberspace from unauthorized interaction by agents with elements of space to maintain and maintain the confidentiality, integrity, availability, and other characteristics of space and protected and preserved resources are referred to as information or cybersecurity [7]. Cybersecurity is primarily concerned with discovering vulnerabilities in cyberspace, analyzing risks associated with attacks that exploit vulnerabilities, and implementing security solutions. A vulnerability is a flaw in a system (a component, product, system, or cyberspace) that allows an attacker to undermine the confidentiality, integrity, availability, reliability, or accountability of a system. Threats and dangers are similar, but they are not the same. Any person, activity, or circumstance that causes injury, loss, damage, or deterioration of existing conditions is considered a threat. Threat risk is an attribute that includes three components: the impact or significance of a threatening event, the possibility or probability of a threat occurring in the future, and the potential loss as a result of a threatening event. The drive to move forward with security solutions and the need for these solutions comes from assessing the risks associated with the threat [7].

-NFV Security Challenges:

NFV networks provide a level of abstraction that conventional networks lack since network components are virtualized. According to CSA, securing this complex and dynamic environment, which includes virtual/physical resources, controls/protocols, and the borders between virtual and physical networks, is difficult for a variety of reasons.

- Dependencies on the hypervisor Many different suppliers offer hypervisors. They need to fix the security flaws in their software. Understanding the underlying architecture, installing proper forms of encryption, and rigorously updating patches are all essential for hypervisor security.

- Network boundaries that are elastic The network fabric in NFV support numerous functionalities. In NFV architecture, physical and virtual barriers are blurred or nonexistent, making security system design problematic.

- Inserting a service Because the fabric automatically routes packets that fulfill programmable criteria, NFV offers elastic, transparent networks. Traditional security measures are conceptually and physically installed in a logical and physical order. When it comes to NFV, there is frequently no easy way to add security services that aren't already built into the hypervisor.

- The stateful inspection vs. inspection that is stateless Stateful inspection has been considered more sophisticated and better than stateless access restrictions in security operations during the previous decade. Where security safeguards are unable to manage the asymmetrical flows caused by several, redundant network channels and devices, NFV may increase complexity.

The ETSI Security Expert Group focuses on software architecture security. It discovered possible NFV security vulnerabilities and determined if they are new or old flaws disguised as something else. Table 1 lists the additional security issues found as a result of NFV [8].

Table 1. Security isssues

Checking and validating the structure and implementation process
Availability of infrastructure to support management
secure boot
Safe crash
performance isolation
User/Tenant Authentication, Authorization and Accounting
Authentication time services
Special keys inside cloned images
Tailgates via virtual testing and monitoring functions
Multi-responsible dismissal

Regarding SDN, it offers a new networking paradigm, with new frameworks, components, structural levels, and interfaces as a result. SDN introduces additional security issues that aren't present in conventional networks. As SDN decouples the control plane from the data plane, it introduces new components and interfaces, as well as a slew of new security concerns. The data plane, the control plane, and the application plane are the three levels that provide security problems in SDN. Hostile OpenFlow switches, flow rule discovery, flooding attacks (e.g., switch flow table flooding), forged or simulated traffic flows, credential management, and insider malicious hosts are all potential risks to the data plane. Unauthorized or unauthenticated apps, fraudulent role insertion, a lack of authentication techniques, and insecure provisioning are among the security issues that the application plane inherits. The centralized SDN controller, communication interfaces, policy enforcement, flow rule modification for modifying packets, controller-switch communication flood, system-level SDN security challenges (due to a lack of auditing accountability mechanisms), and lack of trust between the SDN controller and third-party applications are all security issues that the control plane faces. Because the control plane is the core of the virtual network infrastructure in the SDN design, security flaws in this layer might cause the entire virtual network infrastructure to fail .

Scott-Hayward et al. offered a thorough examination of SDN's security issues. The following are the security problems connected with the SDN framework, organized by impacted layer/interface:

- Layer of the Application The unauthenticated application is used to get unauthorized access. Fraudulent rule insertion can be introduced by malicious apps. A lack of policy enforcement causes configuration difficulties.

- Layer of Control Unauthorized access can be introduced by unauthenticated applications and unauthorized controller access. To alter packets, data modification is introduced in the form of flow rule modification. Fraudulent rule insertion and controller hijacking can be introduced by malicious apps. A controller-switch communication flood can cause a denial of service (DoS). Due to a lack of TLS (or other authentication mechanisms) adoption or policy enforcement, configuration difficulties may develop.

- Layer of Data Unauthorized controller access can lead to unauthorized access. Flow rule discovery (side-channel attack on input buffer) or forwarding policy discovery can lead to data leakage (packet processing timing analysis). Flow rule updates result in data modification. Controller hijacking can be caused by malicious apps. A controller switch communication flood or a switch flow table flood might cause a denial of service. Lack of adoption of TLS (or other authentication mechanisms) may cause configuration difficulties.

- Northbound Interface (NBI) (Application Control Interface) unauthenticated apps can lead to unauthorized access. Fraudulent rule insertion might be introduced by the malicious program. Due to a lack of policy enforcement, configuration difficulties may arise.

- SBI (Southbound Interface) (Control-Data Interface) unauthorized controller access can be used to introduce unauthorized access. Flow rule changes are used to introduce data alteration. Controller hijacking can be caused by malicious apps. A controller switch communication flood may cause a denial of service. Lack of adoption of TLS (or other authentication mechanisms) may cause configuration difficulties [8].

IV. SECURITY SCHEMES

Before going into some of the various security strategies and countermeasures, it's vital to note that cryptographic protocol suites provide fundamental services like authentication and encryption. For instance, consider Internet Protocol Security.

Table 1. Countermeasures to the danger factors

Threat Reason:	Possible countermeasure:
Orchestrator/SDN controller hijacking.	Restrict malicious/compromised applications with application containerization.
Configuration issues.	Real-time policy checker.
DdoS.	Physically distributed SDN controllers; detect attack and redirect legitimate traffic to a new server address.
Repudiation of shared data.	Digital signatures over ITU-T X.509.

In the IP layer, (IPSec) offers end-to-end security. Data flows between a pair of hosts, a pair of security gateways, or a security gateway and a host can all be protected by IPSec. Another example is Transport Layer Security (TLS), which allows client/server applications to interact in a secure manner that protects against eavesdropping, manipulation, and message forging. TLS was created with communications over a secure transport protocol like TCP in mind. When comparing IPSec with TLS, it's worth noting that TLS protects application streams, but IPSec links hosts to complete private networks, including over a public network. Table 2 shows possible countermeasures to the danger factors (thus, threats). Using (or providing support for) application containerization, the impact of harmful application activity can be limited or prevented. Network applications can be statically built with the controller code or dynamically created with the controller software. Authenticating the application during startup and managing the program's access permissions on the infrastructure are both possible with containerization. Furthermore, containerization allows each application's resource utilization to be limited and isolated.

Policy checker mechanisms, insofar as they work, can be used to identify information leakage caused by configuration errors. Because it is responsible for flow rule determinations and generation in an SDN network, the controller is aware of the network status. As a result, SDN permits the verification of proper forwarding behavior. "Traffic emanating from hosts A and B shall never exit the domain during working hours," for example, is a policy verification example. Because the SDN controller may create forwarding rules based on network identifiers and has a limited view of the kind of traffic, such as application identifiers, one of the primary issues in policy verification is the separation of various categories of traffic using fine-grained policy checking. External traffic classifiers and deep packet inspection technologies in the network can help with this. It is also necessary to synchronize the network-wide state among all dispersed controllers to execute policy checking in the case of numerous controllers in the network. The immediate remedy is to physically spread the control layer, as centralized control renders an SDN network more vulnerable to DDoS attacks. Another viable countermeasure is to use traffic volume as a trigger for an SDN application that also filters malicious traffic to detect DDoS. The work, for example, proposes the following method: A blocking application sits atop the SDN controller and establishes a secure link with the server, which can be an orchestrator or a MdO, and is protected from DDoS. In the event of a DDoS assault, the server uses the secure channel to warn the stopping application, which then safely supplies the server with a new IP address at which the service should continue. As a result, valid traffic is diverted to a new address from the attacked server IP. Another way to avoid DDoS assaults is to employ data plane rate limiters to identify aberrant traffic that exceeds a certain threshold [8].

V. MODEL TO THE SECURITY OF NETWORK VIRTUALIZATION SDN/NFV

In Figure 1, ETSI presents a paradigm for integrating SDN and NFV infrastructures [9]. The Infrastructure SDN Controller (IC) and the Tenant SDN Controller (TSDC) are the two centralized SDN controllers in this system (TC). The IC is in charge of the underlying network infrastructure's control and management. It regulates the infrastructure's behavior and adjusts it in response to VIM requests. The TC is a VNF that is created in the tenant domain to govern and administer the VNFs that make up the tenant's network service. In terms of management and orchestration, the Management and Network Orchestration Working Group (ETSI SG) has proposed the NFV MANO, which is a standard for managing and orchestrating cloud and data center resources.

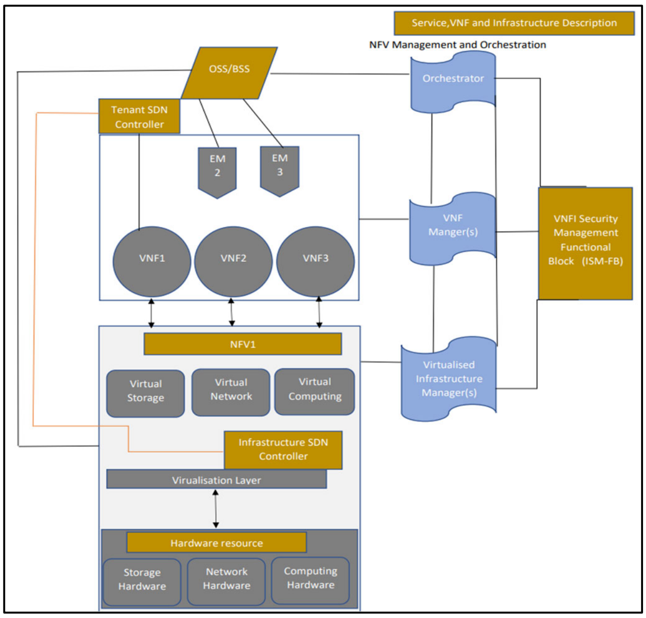

Figure 1. SDN, NFV infrastructure with VNFI block

The NFV-MANO system manages the lifespan of virtual network functions and orchestrates the resources of the underlying infrastructure to enable VNF deployment [10]. The NFV-MANO is made up of three main components: the NFV Orchestrator (NFVO), the VNF

Manager (VNFM), and the Virtualized Infrastructure Manager (VIM) (VIM). It also interfaces with the operator's Operations Support System (OSS) and Business Support System (BSS). The following sections go through the NFVO, VNFM, and VIM in detail:

1 .VNF Manager (VNFM): The VNFM's job is to oversee and manage the VNF lifecycle. i) starts a VNF, ii) updates its software and configuration, and iii) ends it by releasing the allotted resources. Multiple VNFs can be served by a single VNFM. VNFMs can be deployed in the same way as existing VNFs.

2 .VIM (Virtualized Infrastructure Manager): VIM (Virtualized Infrastructure Manager) is a program that The operator infrastructure domain's Network Function Virtualized Infrastructure (NFVI) resources (i.e. compute, storage, and network) are controlled and managed by VIM. It is capable of dealing with various forms of materials. It controls virtual resource capabilities and generates information on capacity and utilization for each NFVI resource. It can specialize in managing a specific resource (e.g. computer-only, storage-only, or network-only). The allocation of NFVI resources and the association of virtual resources to physical resources are two functions of resource management. As a result, VIM maintains an NFVI Resources repository, which contains information on the allocated and available hardware (i.e. computing, storage, and networking) as well as software (e.g. hypervisors and virtual machines).

3 .NFV Orchestrator (NFVO): is in charge of orchestrating network resources, network services, and virtual network functions (VNFs). It exposes the network service catalog, which is a repository that houses all of the network services that have been registered. NFVO's primary responsibilities include cataloging network services and managing their lifecycles. The NFVO is also responsible for registering VNFs in a VNF catalog and, if necessary, instantiating the accompanying VNFM. Furthermore, it verifies the network service and VNF's consistency and feasibility. Finally, it gives VNFM permission to use NFVI resources.

Finally, the NFVI Security Management Functional Block (ISM-FB) has been added for the MANO Virtual Infrastructure Manager responsible for the horizontal management of the virtualization layer. In the NFVI layer, ISM is the logical function assigned to security management. Builds and manages security in NFVI to support all requests for security management of network services at a higher layer. Closely related to the three stages described above, this step focuses on the gap issues that may arise in each of the functions of the previous three stages. To ensure that the security of each stage is fully managed. Figure 1.1 also shows a different functional design of the screen, which we will mention at the end of this section. A set of protocols and services are created within this architecture to develop trust for the entire infrastructure, assuming a chain of trust that extends to virtual network activities.

Separation of interests, tasks, and privileges in MANO, as well as the management of individual security functions, must be ensured through security controls (eg, various security controls and access management). Security function administrators may be responsible for setting security rules and policies, as well as limitations on the validity of the security policy (eg dependencies between VSFs such as relative order or VSF security hierarchy). MANO subsystem components may be responsible for integrating new VSF packages, controlling their lifespan (including defining the execution environment for VSF packages but not security policy rules for VSFs), and managing the resources associated with these requests and NFVI resource requests. Separate privileges and being the least privileged is one of the security concepts. In addition, to reduce the attack vector of the management layers and mitigate the risk of illegal privilege escalation, a less common approach is used.

Network services and network functions can be deployed dynamically in an NFV network. The current document is selected. Security policy management and automated and dynamic security functions have functional and security requirements. For NFV systems, life cycle management and security monitoring are essential. Effective implementation of NFV depends largely on security management and oversight. The criteria and results of this document will catalyze the rapid release of NFV.

VI. CONCLUSION

SDN and NFV have seen widespread use in core data centers and more resiliency in networks, where they have been used to improve process flow and policies by separating the levels of controllers and datasets, and extensive and effective use of level virtualization for different datasets. Furthermore, SDN and NFV allow for accurate and improved security monitoring currency, which allows and enhances faster and more accurate network knowledge through the use of a centralized control level. However, both SDN/NFV brings great combinations and attack surface. So in this article, we introduced the basic concepts needed for both SDN and NFV to enhance resilience and service delivery programming in virtual networks. In fact, we have discussed the differences and similarities of emerging use case requirements and the importance of SDN, NFV, and Network Segmentation techniques in providing a suite of services. We also discussed the security challenges of NFV and SDN, as well as security schemes. Finally, we present an SDN / NFV Virtual Network Security Model.

Acknowledgment
The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

REFERENCE

[1] Ageyev, Dmytro, et al. "Provision security in SDN/NFV." *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*. IEEE, 2018.

[2] Duan, Qiang, Nirwan Ansari, and Mehmet Toy. "Software-defined network virtualization: An architectural framework for integrating SDN and NFV for service provisioning in future networks." *IEEE Network* 30.5 (2016): 10-16.

[3] Pattaranantakul, Montida, et al. "SecMANO: Towards network functions virtualization (NFV) based security management and orchestration." *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 2016.

[4] Mazher, Alaa Noori, Jumana Waleed, and Abeer Tariq MaoLood. "The Security Threats and Solutions of Network Functions Virtualization: A Review." *Journal of Al-Qadisiyah for computer science and mathematics* 12.4 (2020): Page-38.

[5] Jain, Aman, et al. "A comparison of SDN and NFV for re-designing the LTE packet core." *2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. IEEE, 2016.

[6] Ray, Partha Pratim, and Neeraj Kumar. "SDN/NFV architectures for edge-cloud oriented IoT: A systematic review." *Computer Communications* 169 (2021): 129-153.

[7] Murillo, Andrés F., et al. "SDN and NFV security: Challenges for integrated solutions." *Guide to Security in SDN and NFV*. Springer, Cham, 2017. 75-101.

[8] Zhu, Shao Ying, et al., eds. *Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications*. Springer, 2017.

[9] *Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework.* v. 1.1.1. ETSI GS NFV-EVE 005.

[10] “What Is NFV MANO?” *ADVA*, www.adva.com/en/products/technology/what-is-nfv-mano.