安全意见书

网络功能虚拟化

cloud security alliance®

鸣谢

中文版翻译说明：

由中国云安全联盟(C-CSA)秘书处组织翻译安全意见书--Security Position Paper Network Function Virtualization，华为专家翻译，中国云安全联盟专家委员会专家及华为专家审校。

翻译工作专家：

沈桂斌、金懿鑫、游顺刚、梁珩、高勇、石新美

审校工作专家：

石文昌（C-CSA专家委员会副主任）
刘　浩（C-CSA专家委员会专家）
张志亮（华为专家）
余晓光（华为专家）
罗　斌（华为专家）
刘茂俊（华为专家）

C-CSA工作人员：

史晓婧（C-CSA研究助理）

鸣谢

联席工作组组长
Kapil Raina
Saif Chaudhry

贡献者
Aleksandar Milenkoski
Bernd Jaeger
Kapil Raina
Mason Harris
Saif Chaudhry
Sivadon Chasiri
Veronica David
Wenmao Liu

CSA 全球员工
Victor Chin, Research Analyst

序言

网络功能虚拟化NFV（Network Functions Virtualization)与云计算、大数据、软件定义网络SDN、物联网、区块链、人工智能、5G等都是近年或未来将给世界带来变革的新兴技术，这些技术犹如双刃“达摩克利斯之剑”，既给业务带来价值，也给业务带来风险。NFV由ETSI（European Telecommunication Standards Institute）的NFV-ISG组织于2012年10月并提出概念和计划，这项技术在电信行业已经开始普及并将在未来几年改变整个电信行业。这期间，电信运营商渴望NFV革命所带来的高效和敏捷，实现运营成本降低和业务创新突破。但是NFV技术迁移带来了一些威胁和安全问题，造成的危害与影响越来越大，这些网络安全事件无疑都是对NFV发出的警告。一旦通信网络安全事故爆发，通信服务中断、用户隐私泄露、电信欺诈、运营商信誉受损等，结果都是灾难性的。在ETSI工作组的早期研究基础上，云安全联盟发布了NFV安全意见书，专家们给出了应对风险的安全专业意见。中国云安全与新兴技术安全创新联盟（简称：中国云安全联盟）组织华为专家进行翻译为中文版本，相信一定会有助NFV技术在中国的安全落地。

中国云安全联盟和云安全联盟大中华区非常感谢翻译和支持工作者们，特别是华为专家们和中国云安全联盟专家委员会专家们的无私贡献。

中国云安全与新兴技术安全创新联盟常务副理事长
CSA云安全联盟大中华区主席
李雨航 Yale Li

目录

第一章

1 概述

近五年来，随着云基础设施的能力和复杂性飞速演进，安全风险也相应上升。

虽然虚拟化已不是一个很新的概念，但几乎任何人都可以对计算、存储、网络和应用程序等资源进行虚拟化的想法会增加安全威胁的影响和速度。同时，全球地缘政治格局已从由机遇驱动的网络攻击转变为资金充足的国家行动。

云安全联盟（Cloud Security Alliance，CSA）已识别这一趋势，并认为当下是发起一个专项论坛以帮助网络和数据中心技术专家了解如何保护虚拟基础设施安全的适当时机。

考虑到虚拟化涵盖多项技术，CSA 虚拟化工作小组将着力于计算、网络、容器及存储等关键领域。在这些关键领域中，容器及存储虚拟化安全研究正在计划中；计算虚拟化技术已成熟，工作组已对其研究制定了指导建议；对于网络虚拟化的探索尚不深入，因此需要一个先行者先输出风险模型或逐步的实践指导。

这份白皮书就是这个“先行者”。本文讨论了一些潜在的安全问题和关注点，并为保护基于虚拟网络功能（NFV）的架构提供了指导，其中安全服务以虚拟网络功能（VNF）的形式提供。我们将这种基于NFV的架构称为NFV安全框架。本白皮书还引用软件定义网络（software-defined networking，SDN）概念，因为SDN是驱动虚拟化的关键技术。本文正是这个“先行者”。

本文包含五个章节：

第一章	**概述**
第二章	**NFV概念与SDN简述**
第三章	**NFV引入云环境后带来的安全问题及思考**
第四章	**NFV安全框架带来的好处与机遇**
第五章	**NFV安全框架的挑战及重要元素**

[1] https://virtualizationreview.com/articles/2015/03/20/security-top-reason-for-cloud-hesitancy.aspx
[2] http://www.oracle.com/us/products/middleware/data-integration/ioug-di-for-cloud-survey-2596248.pdf
[3] “With cloud, these practices have become more complex. And they’ve shifted from leading practices to critical core disciplines. Integration stability and reliability was the number two challenge in a recent survey on cloud adoption, trailing only security concerns.” - source: http://dupress.com/articles/2014-tech-trends-cloud-orchestration/
[4] https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf

受众及范围

本文面向对部署NFV基础设施感兴趣的虚拟化、安全、及网络架构师。NFV减弱了网络服务对硬件的依赖，通过将网络功能虚拟化，云服务提供商（cloud service provider，CSP）能以更快的速度部署网络服务，增加收益；降低企业资本支出（CAPEX）与运营支出（OPEX）。

今天，CSP和企业都需要解决其特有而又复杂的安全问题。两者都必须考虑NFV基础设施将如何影响其总体风险情况，以及NFV的动态灵活性如何影响其总体安全架构。本文旨在帮助CSP与企业更好地理解这两类影响，同时提供技术及非技术手段下的安全控制方式。虽然本文主要为技术人员撰写，但也能帮助业务相关方理解所涉及的概念。

部署场景、实施蓝图、及风险削减技术均不在本文详述。CSA虚拟化工作组后续会发布详细的风险模型及安全风险规避指南。

第二章

2 NFV与SDN

SDN支持通过动态调整网络配置来改变网络功能特性及行为。例如，在SDN拓扑上可实时调整网络路径。NFV与SDN可不依赖对方独立部署，但通过SDN网络提供的平台，用户可部署一个动态的虚拟网络业务链，从而形成一个端到端的网络业务（见图1）。

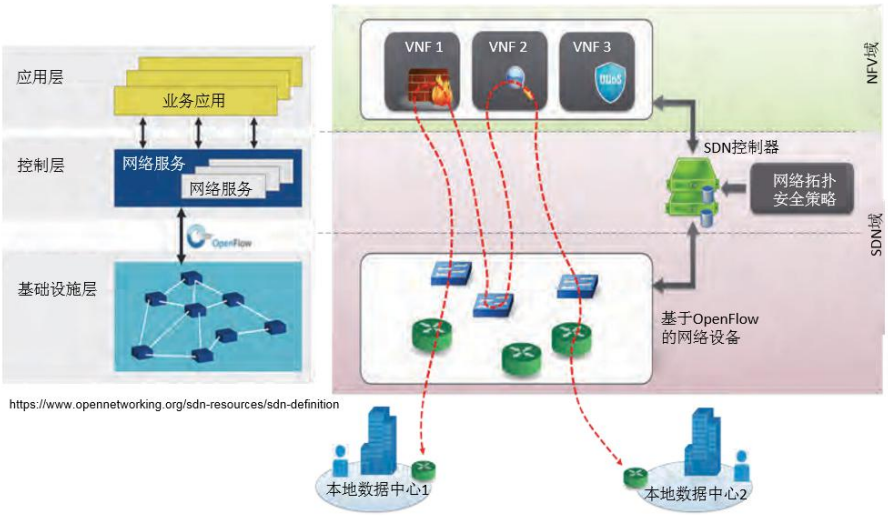


图1.使用SDN动态编排VNF构建端到端网络业务

如图1所示，左侧为开放网络基金会（Open Networking Foundation，ONP）定义的SDN架构，右侧对应实际企业用例。图中企业已为本地数据中心1和2建立安全连接。SDN网络路径以红色虚线标识。在非SDN区域，该路径经过由某网络设备提供商提供的固定高带宽虚拟网络防火墙VNF（图中VNF1）。这极大得限制了安全事件的响应速度，尤其是那些对响应速度要求很高的事件，如安全入侵、软件产品的零日缺陷等。SDN场景会按需在网络路径上额外地添加一个虚拟安全功能（图中VNF2），如IPS或恶意软件过滤器。

鉴于在SDN方面已有大量输出，本文将聚焦NFV。更多关于SDN的介绍，请参见附录1-SDN：风险、对比和现有文献。

[5] https://www.opennetworking.org/sdn-resources/sdn-definition

2.1 NFV

NFV通过使用虚拟化技术将基于软件实现的网络功能与底层硬件解耦，并提供丰富的网络功能与部件，包括路由、内容分发网络、网络地址转换、虚拟专用网络（Virtual Private Network，VPN）、负载均衡、入侵检测防御系统（intrusion detection and prevention system，IDPS）及防火墙等。多种网络功能可以合并到同一硬件或服务器上。NFV能够使网络操作人员或用户在通用硬件或CSP平台上按需发放或执行网络功能。

NFV与SDN不相互依赖，可分别独立部署。但两者是相得益彰的，SDN提供的动态虚拟网络功能编排能力能够简化并加速NFV网络部署，提升网络性能。

2.2 NFV网络与传统网络

在传统网络上，网络功能与部署为网络设备的专有硬件紧密绑定。随着网络设备的激增，部署新的网络业务及应用的难度与费用越来越高。业务发放也因持续波动的话务量及不断变化的业务需求变得低效。相比之下，NFV将网络功能与底层的硬件及平台解耦，从而使网络功能可以按需发放，新业务及应用部署变得简单高效。

3 安全问题与思考

3.1 NFV安全挑战

NFV将网络划分为可在通用硬件（如x86服务器）上运行的组件，这些组件被虚拟化，这种资源的抽象化是不存在于传统网络中的。NFV网络中的虚拟机监视器（hypervisor）及其相关的控制与协议非常复杂，虚拟网络与物理网络边界难以区分。因此，嵌入式安全对于提升虚拟化部件整体安全性必不可少。

确保NFV环境安全的挑战源自于以下方面：

1. **Hypervisor依赖：**当前市场被少数hypervisor厂商主宰，其他更多的厂商希望成为市场参与者。正如其操作系统提供商一样，hypervisor厂商必须解决其代码中的安全漏洞。及时更新补丁对于解决安全漏洞固然重要，但hypervisor厂商也需要理解深层架构，如报文如何在网络架构中流动，各类加密机制如何工作等。

2. **弹性网络边界：**在NFV网络上，网络架构适配各类网络功能，物理控制点的位置受限于物理位置与线缆长度，网络边界变得模糊甚至消失。模糊的边界让安全问题变得更加复杂。VLAN已不再同以往一样被认为是安全的，从某些原因来看，物理隔离仍然是必要的。

3. **动态负载：**NFV的吸引力在于其敏捷性和动态能力。传统的安全模型是静态的，无法随着网络拓扑的变化而演进。将安全服务嵌入NFV架构通常需要依赖一个叠加模型，而这个叠加模型很难与厂商边界共存。

4. **服务插入：**NFV宣称能够打造弹性、透明的网络，因其网络结构能够根据预置标准智能地路由数据包。传统的安全举措需要以逻辑和物理方式部署。引入NFV后，安全服务尚未与hypervisor建立分层关系，这些服务通常没有简单的插入点。

5. **状态与无状态检查：**今天的网络需要系统级的网络冗余。路径冗余会导致网络流量不对称，而传统访问控制的设备需要查看每个数据包状态来进行访问控制，这对他们带来了挑战。在过去的十年里，人们认为有状态比无状态检查更先进，并以此为前提进行访问控制操作。多个冗余网络路径或设备导致的流量不对称，势必增加有状态检查访问控制的难度，而NFV的引入使其变得更加复杂了。

6. **可用资源的伸缩性：**如前所述，NFV的吸引力在于它能够使更少的数据中心机架空间、电源和散热发挥更大的功效。

将核心用于工作负载和网络资源可以实现资源整合。更深入的检测技术，如下一代防火墙和传输层安全（Transport Layer Security，TLS）解密等，是资源密集型的，并在没有卸载能力的情况下无法持续扩展。而安全控制必须普遍有效，并且通常需要大量的计算资源。

NFV与SDN一起为安全控制带来了更高的复杂度及挑战。将SDN模型与某些集中控制方法相结合在虚拟层部署网络服务并不罕见。这种NFV与SDN相结合的方式是当前数据中心整合趋势的一部分。

3.2 NFV与SDN：云化风险

将NFV和SDN引入云环境并非易事，原因如下：

1. **NFV与hypervisor的兼容性：**将物理设备迁移到虚拟设备上是个挑战，除存在安全风险外，还有以下原因：一方面，诸如防火墙、入侵防御系统等设备使用的是自定义驱动程序和内核，如果把这些设备部署在计算节点上的基础架构即服务（infrastructure as a service，IaaS）hypervisor上，它们可能无法正常工作。另一方面，某些IaaS系统中的hypervisor提供的是定制化的应用程序接口（application program interface，API）来用于业务流定向。NFV提供商需要为此须投入大量工作来确保其虚拟化设备兼容性。

2. **系统可用性：**虚拟安全设备固然给云化带来了巨大便利，但物理和虚拟NFV的功能之间可能有所出入。即便我们已经根据对应的hypervisor为NFV设备作了优化，其性能可能仍不能媲美物理设备。

3. **SDN架构：**SDN架构是集中式的，而云计算是弹性的、分布式的。SDN要实现集中式运行，同时要对云计算的弹性分布式特性提供必要支持，再叠加云环境的多租户特性，三个因素综合起来可能催生各种复杂难题和不一致现象。

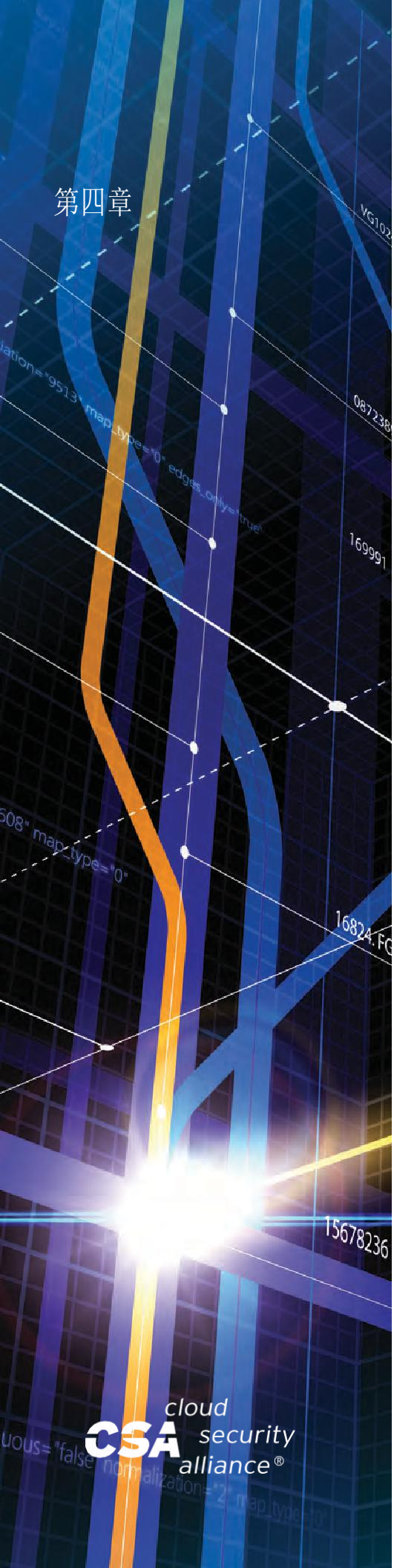
4. **SDN实现方式：**首先，SDN架构囊括各种应用程序、控制器、交换机和管理系统，它们都存在漏洞。恶意竞争者可以利用这些漏洞来对流量进行非法访问或拦截、操纵。例如，当前许多商用白盒交换机都在Linux系统上运行，其中一些通过预置凭证默认允许基于shell的明文访问；其它的则仍使用过时的、易受攻击的SSL协议实现方式。这些状况使整个SDN系统暴露在风险之中。

   其次，引入VNF可能扩大攻击面。攻击者可能利用这些应用程序中的安全漏洞来绕过各种隔离机制，从而危害整个网络，或在其他网络进行非法操作。

   再次，在一些云架构中，数据网络可以和管理或控制网络共享。这种共享式架构可能会降低SDN或IaaS控制节点的安全性。攻击者成功入侵后，可操纵底层路由来绕过NFV安全设备的防控。

5. **策略一致性：**访问控制互相关联的NFV设备群原本禁止了恶意流量，但如果SDN控制器缺乏策略一致性检查机制，恶意用户就可以构建多个策略（例如基于OpenFlow构建网络地址转换规则）来将恶意流量转变为“正常”流量。Porras等人在2015年描述过这类问题。

6. **与IaaS兼容性：**IaaS网络虚拟化模块负责隔离租户资源（如网络流量）。若引入不具备IaaS感知功能的独立SDN控制器来管理虚拟交换机上的流量，则该控制器无法映射租户流量，从而阻碍资源隔离。所以我们必须考虑SDN与IaaS的兼容性问题。例如，CSP若想把运行在不同平台上的网络进行互连，需要SDN控制器有能力感知所涉及的网络组件。



4 NFV安全架构优势

在NFV安全架构中，网络安全功能被作为VNF而非硬件设备来部署。VNF相较于硬件设备而言更具优势，主要包括：

- **节约部署与管理资源：**许多传统的网络安全功能都是通过昂贵而难以管理的硬件网络设备来实现的。而借助NFV，我们把这些功能以虚拟化软件的形式部署在通用硬件上，简化了它们的部署和管理，大大降低了所需耗费的成本和人力。此外，利用SDN技术来管理VNF的收发流量可进一步降低成本和工作量（参见图2a）。

- **提升灵活性：**和传统的网络安全基础设施相比，NFV安全架构更加灵活，主要体现在以下方面：

  1. **按需部署与扩展：**实现安全功能的各种能力是NFV安全架构的一部分。借助NFV，我们可以按需部署和扩展这些能力。例如，倘若虚拟机上部署了具有入侵检测和防御功能的VNF，我们就可以按需迁移这些VNF来实现此安全功能，譬如以此来优化出口处的流量分析。再例如，我们可以直接克隆功能完整的虚拟机，从而极大地扩展流量分析能力。

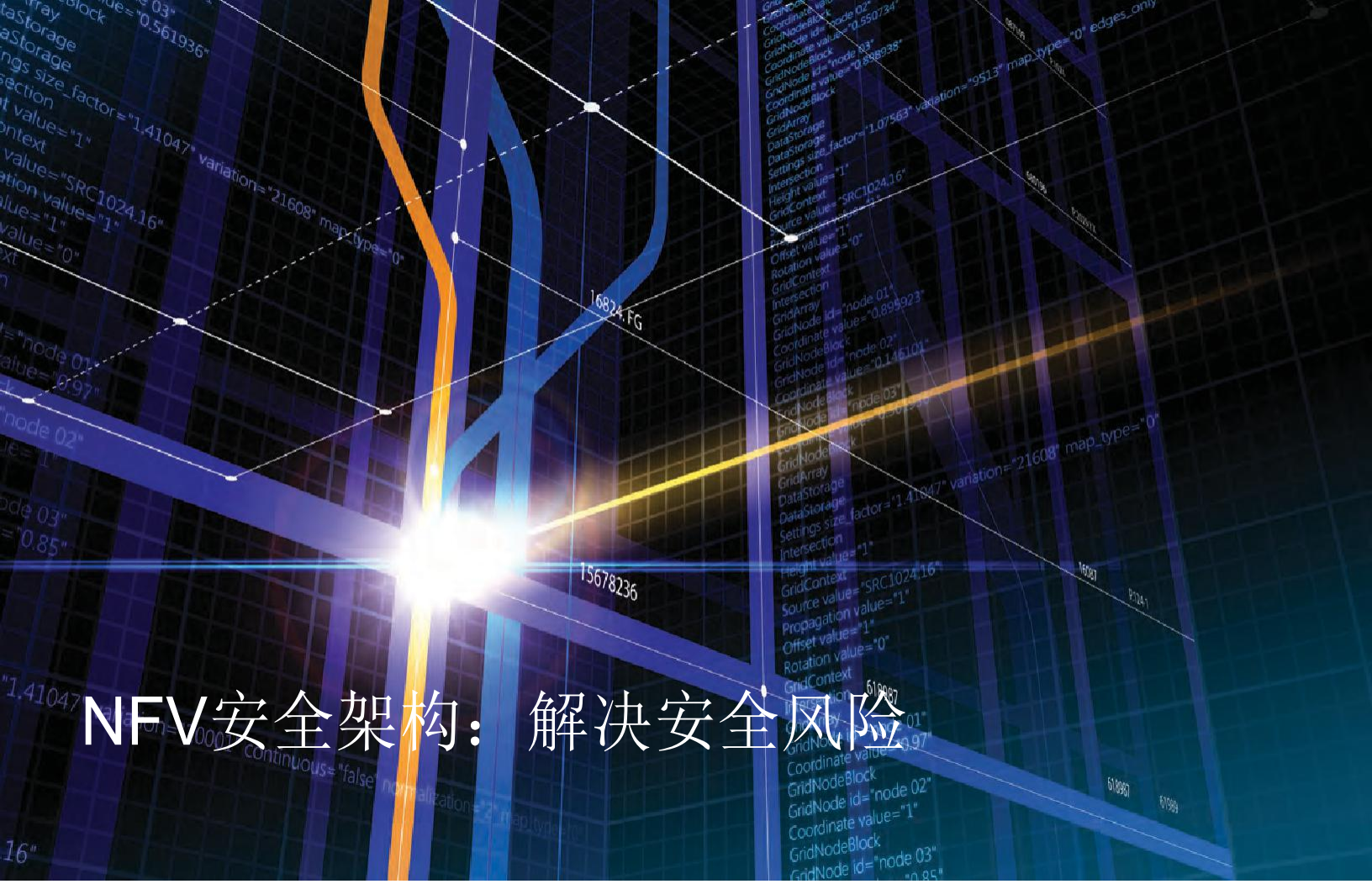
  2. **动态威胁响应：**NFV安全架构提供动态的、实时的威胁响应。该架构与SDN结合后，此功能尤为有效。例如，我们可以用SDN来重新编排服务链，提升VNF功能与性能。

  3. **全局实时视图：**凭借集中式架构，SDN控制器可提供实时的全局网络视图，包括拓扑结构、路由和流量统计信息，帮助用户应对DDoS攻击和及时检测网络异常。

  4. **灵活响应：**在线业务浪涌时，例如黑五期间（美国大型电商线上购物日），安全服务提供商能够快速配置大量防火墙。除此之外当年其余时间，提供商则可通过维护最少量的安全设备来提升资源效率。

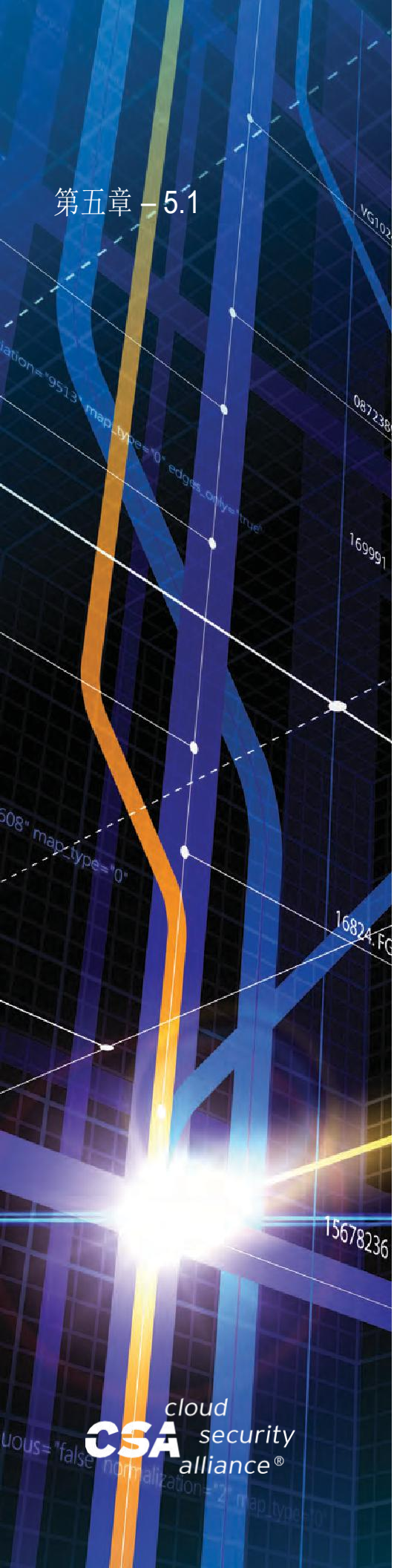
  5. **基于NFV与SDN的软件定义安全：**SDN和NFV可共同提供快速、可拓展的方式来按需构建安全解决方案。一方面，NFV控制平面能够快速配置不同类型的虚拟安全设备；另一方面，SDN控制器能够牵引、拦截或镜像需要进行安全检查的流量，双方由此协同建立起一条安全服务链。安全资源和流量控制均由一个北向安全应用来确定，使得安全解决方案灵活高效。

即便有上述优势，NFV安全架构仍会产生安全问题。在网络功能虚拟化的普及过程中，这些问题影响重大。



NFV安全架构：解决安全风险

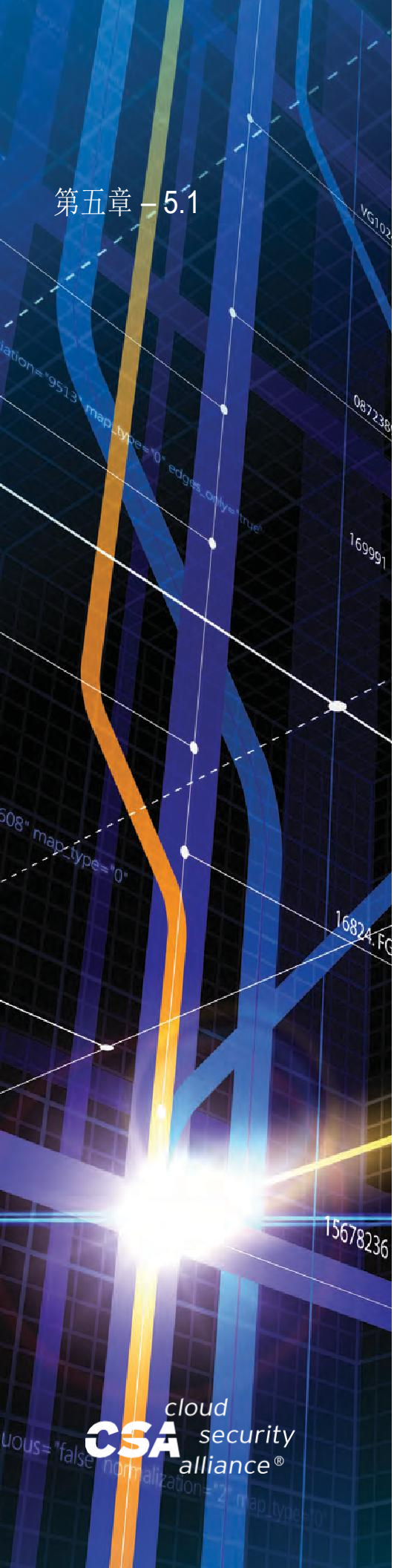
为了使读者更好地了解NFV安全问题的应对之策，5.1章节描述了初步的NFV安全架构，及其为保护和加固基础设施带来的好处。5.2章节介绍了我们使用NFV架构时面临的安全挑战，无论是否以提升安全性为目的使用NFV架构，这些挑战都需要去应对，此外还讨论了NFV架构安全防护各要素。



5.1 NFV安全架构

如上所述，虚拟化技术推动了虚拟机或Linux容器上运行的网络安全功能的部署，例如入侵检测防御系统（intrusion detection and prevention system，IDPS）、访问控制及身份管理。初步的NFV安全框架以生产基础设施中最常见的功能为着眼点，具体如下：

- **入侵检测与防御功能**。该功能由各种网络IDPS解决方案提供，例如使用深度报文检测技术分析流量的解决方案，以及使用浅度（全状态）报文检测技术的解决方案。
- **访问控制功能**。该功能由凭借访问控制策略评估网络数据流量的系统提供，例如，对报文进行状态检测的传统防火墙以及用来分析更深层、上下文相关的数据流量的下一代防火墙。
- **恶意软件防护功能**。该功能由传统的反病毒或反间谍软件系统提供。这类系统可以在出入口检测传播的恶意软件（病毒、间谍软件），并阻止传输或存储感染文件。
- **DoS防护功能。**该功能由专门部署和/或配置的系统提供，用于检测和抵御DoS攻击，特别是针对网络协议或应用程序设计缺陷的非分布式DoS攻击。该防护主要包括DoS防御系统，许多这类系统可执行数据流量分析、访问控制和流量策略。同时，该防护还包括具有流速限制功能的交换机或路由器等。
- **加密功能。**该功能由提供加密服务的系统实现，用于确保数据在传输或其他时期的机密性及完整性。此类系统包括在开放系统互连（Open Systems Interconnection，OSI）参考模型的第二、三、四层提供加密服务的系统。考虑到性能原因和密钥存储，一般使用专门的硬件设备部署加密服务。将密码服务作为VNF部署需要全新的方法，具有挑战性。各组织可能需要决定将着重点放在速度上（即不加密、不完善加密、较小密钥）还是放在保密性上（即前向加密、较大密钥、较强算法）。应根据待传输或待存储数据的分类（敏感、绝密等）进行决策。
- **身份管理和访问控制。**这个系统能够管理和强制执行认证、授权和审计策略，例如单点登录。对用户和系统（API）的管理均适用。



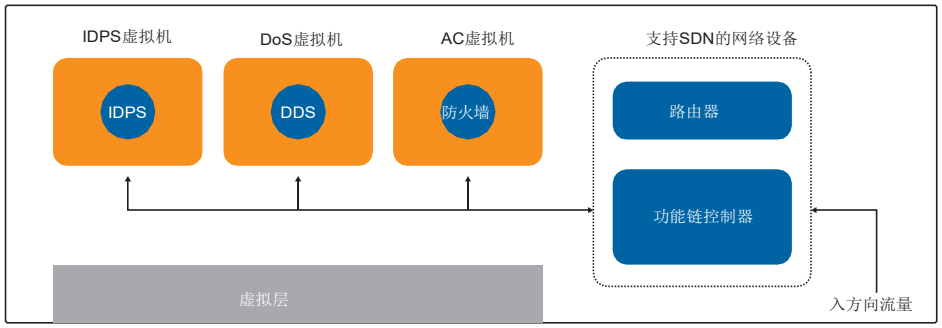


图2a.NFV安全框架部署场景示例

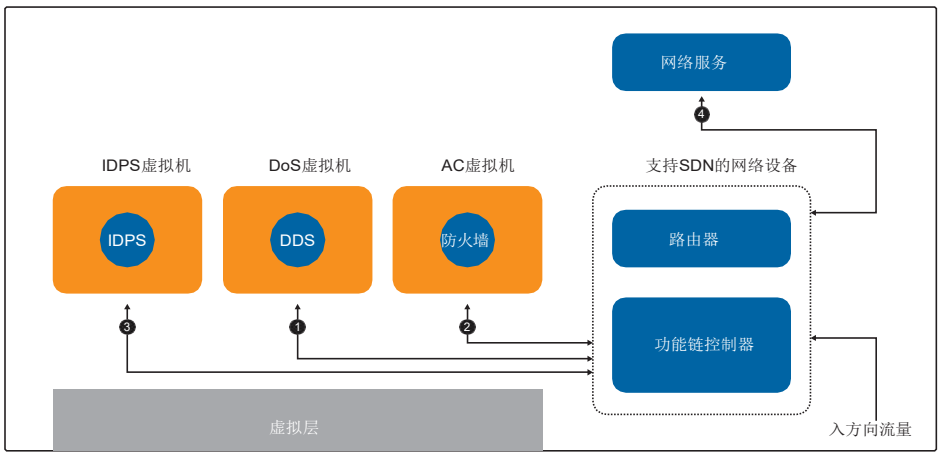
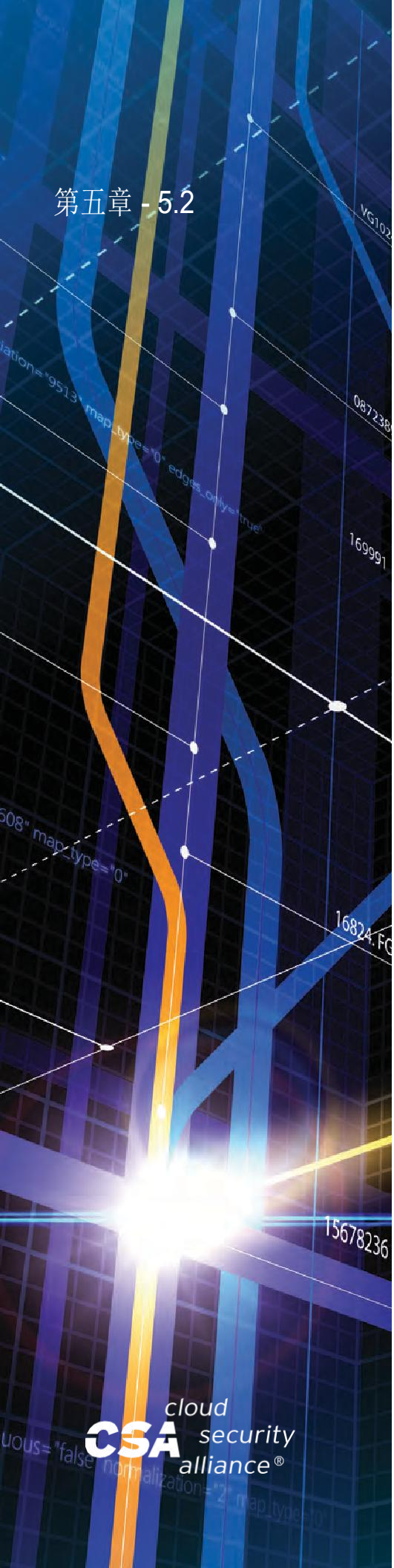


图2b.DDoS泛洪攻击虚拟网络功能链

通过VNF部署安全功能的前提是要有可执行VNF操作的虚拟化软件系统。图2a描述了NFV安全框架的一个示例部署，其中执行入侵检测和防御（IDP）、数据分发服务（data distribution service，DDS）的系统和防火墙部署在虚拟机中。这种情况下，入方向流量由支持SDN的网络设备管理，该设备将流量导向由网络管理员部署好的VNF。我们将此种活动称为网络功能链。图2a中描述的网络设备通过其组件执行网络功能链接，该组件具有路由和功能链功能。

图2b给出了一个示例场景来说明SDN与NFV安全框架结合使用的好处。当网络服务遭受分布式拒绝服务（DDoS）攻击时，可使用编排功能对支持SDN的网络设备进行重新配置，使得发往网络服务的入方向流量在点1就首先被导向DDS。然后，再将流量导向防火墙和点2、点3处的IDPS，并最终到达目的地点4，以期在恶意DDoS流量到达防火墙、IDPS和目标网络服务之前将其过滤，从而在部署的VNF上实现最佳防护效果。



5.2 保护基于NFV的环境安全

图3中的简易化NFV架构列出了主要组件、组件接口以及它们如何交互、相互依赖。

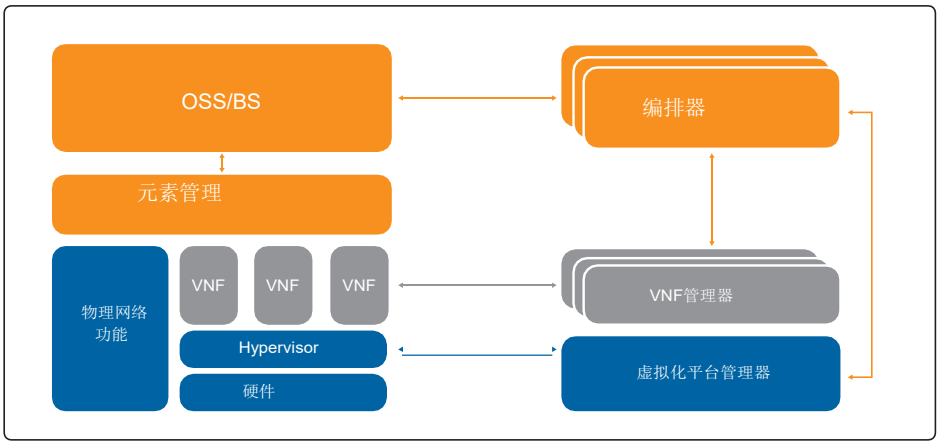


图3.简易化NFV架构

图3展示了NFV基础设施技术方面的静态视图以及一些必须要保护的要素。要成功部署和运行这种使用SDN将多个VNF动态链接到网络路径中的复杂的端到端网络服务模型，必须解决NFV的动态方面以及组织流程中遇到的挑战。第5.2.2章节就保护NFV安全框架时必须考虑的要素进行了讨论。

5.2.1 NFV安全框架保护

NFV安全框架包含VNF环境的技术层，包括像VNF这样的核心元素、核心元素管理系统以及VNF依赖的元素。这些元素包括虚拟化平台或可被虚拟化的常见网络服务功能。

该框架还考虑到了非技术层面，如NFV组件的生命周期管理以及动态变化的网络对安全管理和事件响应的影响。

图4为框架元素的高级视图，将在下一节进行讨论。

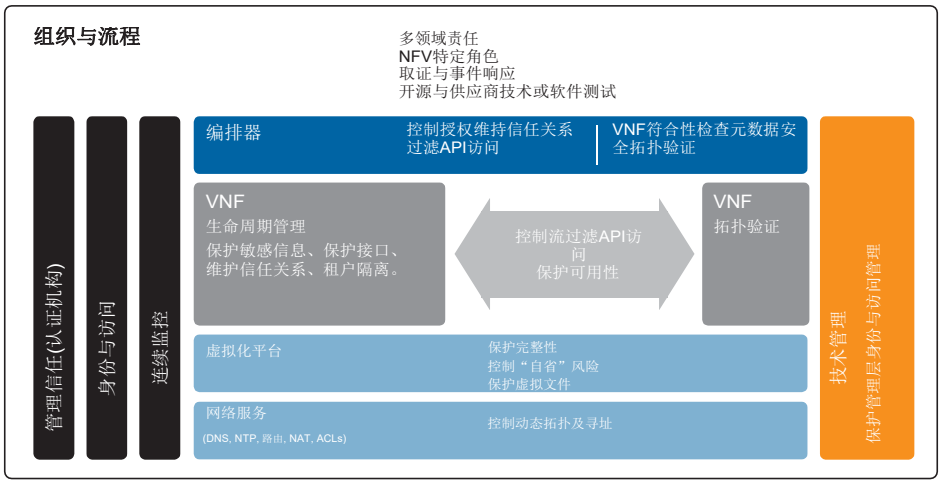
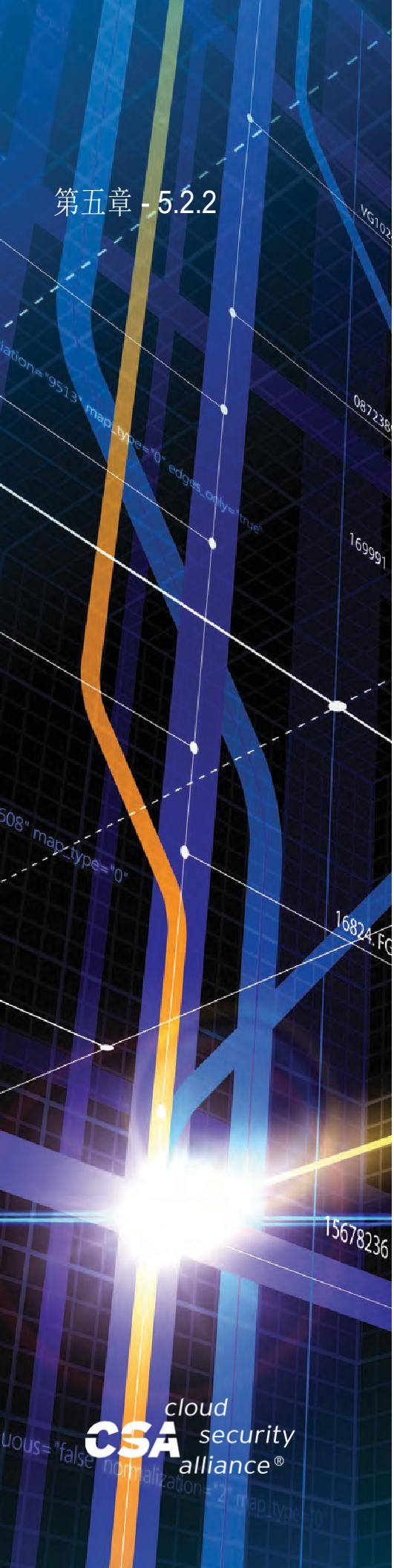


图4.NFV安全框架元素高级视图

该框架的技术层面和控制要素嵌入在组织结构和流程中，这些组织结构和流程包含传统网络运营中没有的元素。例如，VNF交叉网络的设计、创建和运营，管理程序、计算、存储、SDN以及多个管理和编排领域。而过去的网络团队只处理其自身系统，可能不会考虑将他们的路由器集成到反病毒防御流程中。在硬件设备变成核心网中的虚拟机或他们的用户端设备之前，他们可能都没有想过克隆网络设备证书。



5.2.2 重要元素

根据NFV的具体要求，安全架构的重要元素包含如下几点：

组织和流程

- **多领域责任与全新流程：**虚拟网络的建设和运营涉及诸多管理域，还可能需要NFV特定角色，并通过精细化控制进行角色分离、功能分离及范围分离。生命周期管理、安全监控、事件响应和取证、合法监听及其他流程必须适应更加动态的环境，包括快速变化的网络拓扑、数据流路径及网络地址。
- **模式转变：**传统网络的一部分将变成非物理形式，因此将失去其抵御恶意软件等威胁的自然防御能力。为解决此问题，需要在NFV安全架构中补充额外的流程。

VNF安全生命周期

- **创建和部署：**在部署VNF之前，编排或管理系统应检查其是否符合构建配置标准。检查项包括但不限于：

  - 配置安全
  - 软件包是否仅包含可信和预期的组件
  - 可信组件是否被更改（即完整性）

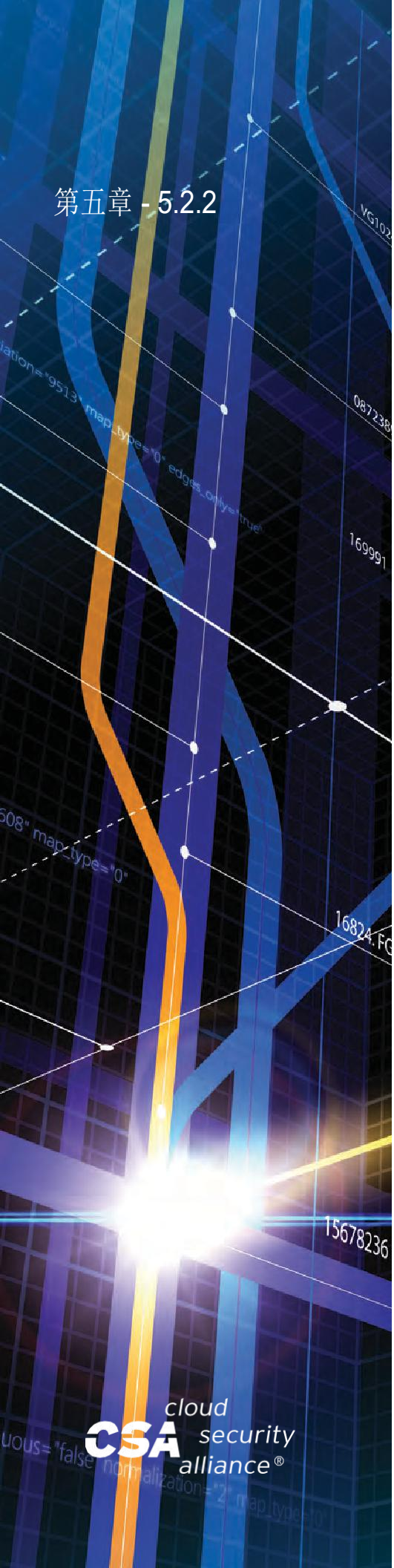
  相比物理网路设备而言，虚拟路由器的部署十分简单，因此需要在编排层中设置控制举措，以避免VNF散乱、非预期的拓扑结构以及网络流路径更改。

- **虚拟设备克隆和移动/迁移：**虚拟网络设备可被轻松克隆和实例化。因此，安全框架必须涉及以下要素：

  - 依靠迁移技术，证书、帐户、媒体访问控制地址或硬件ID在克隆后看起来完全相同。但这可能不满足实际需求，例如，有时会需要设备'B'，其配置与'A'类似但证书不同，或有时需要移动'A'但要求保持其身份。如果证书基于这些属性，那么编排层可能在需要时注入并更正这些属性。

  - 需要可信平台模块，例如Intel可信执行技术（Trusted Execution Technology，TXT），来确保虚拟设备可以提供底层硬件的安全证据或真实状态及其物理位置。

- **动态状态管理：**安全框架要求与云计算层要求非常相似。虚拟网络组件可以动态更改其休眠、睡眠、重续、中止、恢复、开机和关机状态。当一台旧式、数据配置不佳或被篡改的设备在网络中突然“重新出现”时，很容易危害安全。因此，编排层应执行与首次部署类似的合规性检查。应验证源和目标的完整性。.



- **快照，备份和删除（虚拟安全退服）**：虚拟网络设备包含与其对应的物理设备相同的敏感信息，例如设备证书、VPN和加密密钥、管理员帐户和API密钥。尽管物理网络设备的安全擦除和配置备份的安全措施是标准的，但虚拟化为NFV安全框架增加了新的要求：
    - 快照会将设备RAM内容复制到文件中，并可能备份到不同的位置。这些内容可能包括解密数据，因此必须在传输等时期加以保护。
    - 同时还需要考虑虚拟机克隆，因为在部署（基于主映像）时它们是合法的，但当恶意内部人士或黑客试图窃取信息或插入到损坏系统时，它们又可能是伪造的。
    - 在编排层删除的设备实例可能会在主机文件系统上保留一段时间，因此可以恢复。
    - 虚拟路由器比物理路由器更容易删除，这可能会增加无意或有意的DoS攻击风险。

本节提到的安全框架要素包括技术性和组织性要素。任何存储的文件，例如克隆、数据或快照，都可以通过加密方式在虚拟层进行保护。如果无法加密，则必须使用进程来安全地管理备份文件或VNF文件。

管理静态和动态拓扑

- **虚拟组件及其管理系统的可见性**：必须采取如下技术和非技术措施来控制访问：
    - 基于角色的访问控制（职责分离，最小权限，工作流升级）
    - 定义了接口、流程和保护（过滤）功能的安全架构
    - 隔离功能
    - 受控的（即封套，代理）、多租户可感知的虚拟化层访问的详细信息，确保不存在侧信道和相关安全风险。

- **拓扑验证**：使用SDN的优势之一是能够动态地重新配置网络路径，从而在服务链中纳入额外的VNF安全功能。但这种能力引入了拓扑变化威胁，将会导致通信丢失，或导致绕过过滤器或访问控制的意外直接流量。因此，需要在编排层和VNF层实施拓扑验证。同时还需注意一点：VNF应检查其新的对端实体并决定是否信任验证结果。

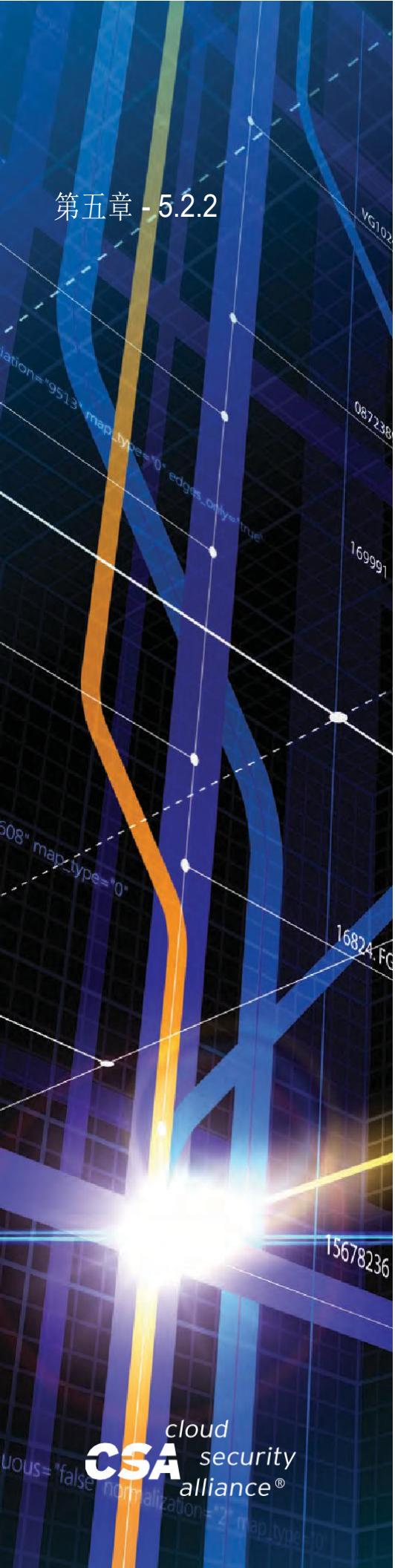
日志、监控、安全信息和事件管理、配置管理

鉴于虚拟化网络的动态特性，需要考虑以下几点：

- 为了识别复杂NFV环境中的异常情况，必须收集所有层的安全信息并进行关联，从而创建强大的审计跟踪来进行取证和合规性评估。

- 现代安全信息、事件管理和入侵分析师的思维方式可能仍受静态网络的影响。在NFV网络中，IP地址可能变化很快，因此像在静态网络上那样去创建硬拷贝列表也许不再可行。可能需要新的指标和分析。如上文“克隆和移动/迁移虚拟设备”部分所述，可动态地或程序化地创建或克隆新的虚拟资源。因此必须通过审计机制发现这些新资源及其相关安全策略，以便生成适当的审计跟踪。这就需要编排和生命周期管理组件与审计框架之间进行交互。

- 用于特定业务流或网络路由的端到端网络路径使得数据包捕获或检测更加困难。应使用上文“管理静态和动态拓扑”章节中提到的拓扑验证和实施来应对这一挑战。



- 取证流程可能需要适配。尽管获取取证图像比在物理设备上更容易，但可能需要技术上作相应改变来分析时间点和网络日志。分析师需要访问更多系统和日志以获取完整的取证图片。此外，获取完整且原始的管理员审核日志也至关重要，由此可确定威胁是由管理员创建（例如内部人士产生的安全威胁），还是由于不遵循程序（例如，未能退出会话），或是由于管理员帐户受到攻击（例如，通过僵尸网络，恶意软件等）而引起的。

- 应考虑通过连续监测来确保物理和虚拟系统的实时合规性。

- 实施双人原则（亦称为“四眼原则”），对重要任务或敏感操作（例如删除虚拟对象）实施双重权限。.

信任管理

如上文所述，信任管理在任何动态网络中都是一个关键的安全控制措施。以下双向信任关系在NFV安全框架中尤为重要：

- VNF与VNF
- VNF与外部实体（例如DNS、NTP、路由设备）
- VNF与VNF管理器
- VNF与网管系统（Element Management System，EMS）
- VNF管理器与VNF编排器以及VNF基础设施管理器

在编排域和管理域实施端到端信任管理非常重要。可以基于软硬件元素来建立信任，例如通过可信计算库状态，如信任平台模块（Trust Platform Module，TPM）状态、安全启动、包源和/或完整性。可使用数字证书进行安全验证。

技术平台

最后一点，但并非最不重要的一点是，平台安全取决于运行的技术平台。关键方面包括：

- **虚拟化平台安全**。该平台保护hypervisor、管理域和API。
- **NFV身份和访问管理系统**。无论VNF是否为新实例化，休眠还是退服状态，该系统都应能够管理VNF帐户和凭证。该系统还应能够管理特权访问，包括允许“自省”的角色和实体，并提供这些组件中所有活动的大量日志。

结论

NFV和SDN技术在现代网络改造中拥有广阔前景。在此背景下，本文为安全意识建立了一个基本框架。未来CSA虚拟化工作组的交付成果将为NFV和SDN技术人员提供进一步实用的步骤，从而简化基础设施安全防护流程。

[7] 网管系统为一个或多个VNF提供典型的管理功能（ETSI，2013）

参考文献

1. Keith Ward. (2015). Survey: Security is Top Reason for Cloud Hesitancy. Virtualization Review. Retrieved: https://virtualizationreview.com/articles/2015/03/20/security-top-reason-for-cloud-hesitancy.aspx

2. Joseph McKendrick. (2015). Data Integration for Cloud Survey. Independent Oracle Users Group. Retrieved: http://www.oracle.com/us/products/middleware/data-integration/ioug-di-for-cloud-survey-2596248.pdf

3. Andy Main and John Peto. (2014). Tech Trends 2014, Cloud Orchestration. Deloitte University Press. Retrieved: http://dupress.com/articles/2014-tech-trends-cloud-orchestration/

4. Mario Maawad Marcos et al. (2015). How Cloud is Being Used in the Financial Sector: Survey Report. Cloud Security Alliance. Retrieved: https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FI- NAL.pdf

5. Open Networking Foundation. Software-Defined Networking (SDN) Definition. Retrieved: https://www.opennetworking.org/sdn-resources/sdn-definition

6. P. Porras, S. Cheung, M. Fong, K. Skinner, and V. Yegneswaran. (2015). Securing the Software-Defined Network Control Layer. Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS).

7. European Telecommunications Standards Institute (ETSI). (2013). ETSI GS NFV 002 V1.1.1 - Network Functions Virtualization (NFV); Architectural Framework

8. McBride, M. C. (2013). SDN Security Considerations in the Data Center. Open Networking Foundation. ONF SOLUTION BRIEF.

9. Kreutz, D., Ramos, F. M., & Verissimo, P. (2013). Towards Secure and Dependable Software-Defined Networks. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 55-60). ACM.

10. Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013). SDN security: A survey. Future Networks and Services (SDN4FNS), 2013 IEEE SDN for (pp. 1-7). IEEE.

11. European Telecommunications Standards Institute (ETSI). (2014). ETSI GS NFV-SEC 003 V1.1.1 - Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance.

缩略语

CM	Continuous Monitoring，连续监控
CPE	Customer Premises Equipment，客户终端设备
CSP	Cloud Service Provider，云服务提供商
EMS	Element Management System，网元管理系统
IAM	Identity and Access Management，身份管理与访问控制
IR	Incident Response，事件响应
SIEM	Security Information and Event Management，安全信息和事件管理
OSS	Operations Support Systems，运营支撑系统
BSS	Business Support Systems，业务支撑
MSS	Managed Security Service安全托管服务

附录

附录1-SDN：风险、对比和现有文献

1. SDN控制器依赖性：在几乎所有形式的SDN中，都有一个基于API的南北向通信对象模型。 这些对象将按照服务合同需要进行部署。该模型强调对控制器的信任，因为双向通信对于管理至关重要。安全举措必须在控制面和数据面提供职责分离并提供精细化访问控制（以在控制平面上维持最小访问权限的原则）。考虑到控制器所要求的访问性质，SDN模型与传统物理网络相比拥有不同的边界。这种向量意味着对环境的威胁。

2. API安全性和最佳实践：API在本质上是开放和有效的，以支持实体之间的通信。当今API编程语言数量惊人。安全举措依赖于底层的API库正确安全地执行责。很多底层的API库都面临自己的安全挑战，因此有人认为底层的API结构影响了安全防护能力。对安全操作来而言这是一个挑战。API端点及其服务代表整个后端环境中的攻击媒介。因此，应该使用适当的控制措施来保护API端点，并应防止黑客通过API入侵到内网（最简单的形式是通过DMZ隔离）。

3. 不断演进的标准：NFV/SDN快速演进来极大的安全挑战。因为用户和开发者还未充分理解安全问题，如何对其提供有效控制。此外，各SDN实现方式之间缺乏统一标准，可能会进一步造成安全漏洞。

SDN与传统网络对比

传统网络的安装和配置需要熟练的技术人员。网络节点的控制平面和数据平面的紧密集成使运营商难以动态扩缩容其网络。

通过控制平面和数据平面分离、可编程性和集中控制，SDN网络运营商可以在保障网络可见性的同时管理数据包流量，从而能够调整网络配置以满足不断变化的流量需求，并最终提高整体网络性能。

SDN报告

指导SDN标准化的开放网络基金会发布了数据中心中SDN安全注意事项（McBride，2013）。该报告指出，由于策略与物理资源紧密耦合，现有的安全解决方案（如防火墙和IDPS）难以在云上部署、管理、编程和保护。另外，特定供应商的网络组件可能会限制安全解决方案的能力。 该报告介绍了基于OpenFlow的SDN的优势及其解决这些环境所面临的安全挑战的能力。

Kreutz，Ramos和Verissimo在2013年发现了网络可编程性和控制逻辑集中造成的威胁。网络编程可以允许缺陷和恶意代码攻击网络流量和组件，软件或用户可以中断集中控制。主要的SDN安全攻击针对控制平面通信和SDN控制器。由于缺乏在SDN控制器和管理应用程序之间建立信任的机制，可以轻松部署有害应用程序。

Scott-Hayward、O'Callaghan和Sezer于2013年展示了对SDN安全问题的调查结果。 他们将这些问题分为六类：未经授权的访问、数据泄漏、数据修改、恶意应用程序、拒绝服务以及与配置相关的问题。

相比之下，NFV是一项新兴技术，安全问题和挑战尚未得到深入的研究。主导NFV标准化的欧洲电信标准协会近期发布了一份报告，列出了NFV的威胁并提供了安全和信任指导[欧洲电信标准协会（ETSI），2014]。