Network Functions Virtualization (NFV) helps service providers become more agile and reduce their costs. However, NFV's new architecture, operations, and openness create new security challenges. Those challenges must be overcome for service providers to scale NFV and earn its business benefits. This paper discusses a risk identification methodology, followed by a careful review of the top five security risks when migrating services to NFV. The intent is to provide security practitioners with a basis for developing a documented risk dashboard in order to bring down the overall security risk to an acceptable level when migrating to NFV.

About the NFV Insight Series

NFV represents a major shift in the telecommunications and networking industry through the application of virtualization and cloud principles. Until recently, this approach appeared to be impossible due to stringent performance, availability, reliability, and security requirements in communication networks. Many service providers now implement NFV to gain an advantage through automation and responsiveness and to deliver an enhanced customer experience while reducing operational costs. This series of white papers addresses some of the key technical and business challenges on the road to NFV.
Contents

Introduction 3
Context and target audience 4
Migration to NFV 5
Assessing the risk: The approach and methodology 8
Risk 1: Isolation failure 14
Risk 2: Topology instantiation validation and enforcement failure 17
Risk 3: Legal and regulatory compliance failure 20
Risk 4: Infrastructure DoS protection failure 22
Risk 5: Security incidents identification and troubleshooting failure 25
Next steps and going forward 27
Concluding remarks 29
Acronyms 30
References 31
Appendix 34
Introduction

NFV (Network Functions Virtualization) represents a radical change in the telecom industry. This new model and architecture is based on migrating telecom functions from dedicated appliances to virtualized IT platforms based on commodity hardware. While much is promised, including elasticity (auto-scaling), flexibility (auto-onboarding), as well as cost reduction, the migration to this new model introduces several risks. These risks are linked with changing technologies and operational processes—in addition to changes of an organizational nature.

One key success factor for NFV is security. It is an area in continuous evolution, which requires the utmost attention. NFV security objectives are the same as for legacy deployments; however, migration to the NFV model brings specific security risks. Those risks are either known risks from legacy environments that need new approaches or actual, new risks inherent in the new architecture.

As NFV matures, numerous threats and vulnerabilities are being documented by the industry. To support early NFV adopters, Nokia has created and maintains a list of top-level security risks. Using a top-down approach, which takes input from some key industry players, combined with a bottom-up approach, which takes key security attributes as input, Nokia has initially identified a list of security risks, which have been further refined to address migration-specific issues. This iterative methodology complies with ISO 27005, the key standard for Information Risk Management, where the notion of domains enables a high-level risk assessment to address specific or limited threats and vulnerabilities.

Based on widely accepted industry resources, this paper presents the risk identification methodology followed by a review of the top 5 security risks. These risks are analyzed according to the following categories:

- Asset-threat-vulnerability
- Scenario-based/event-driven
- Quantitative and/or qualitative approaches.
The goal is to maintain a documented NFV migration risk dashboard with the ultimate objective to reduce the level of the overall security risk to an acceptable level when adopting NFV. By guiding the NFV community for security resource planning and effectively minimizing the migration risk, this dashboard will effectively contribute to NFV acceptance and adoption.

**Context and target audience**

When considering migration to NFV, the first questions were initially focused on technology and the nature of NFV. Subsequently, key success factors, such as security, and reliability were identified. Later, long lists of issues originating from a number of technology forums and industry groups began to be published and discussed. Ever since the early inception of NFV at the end of 2012, potential users have been up and down the emerging technology hype cycle, passing the peak of inflated expectations and moving through the trough of disillusionment. As the climb proceeds up the slope of enlightenment, one of the key questions is: “What does migrating to NFV mean for security?”

After dozens of presentations to elite customers, conferences, and workshops over the past three years, it has become clear that identifying and documenting the top security risks is among the most important priorities. The objectives are clear: Provide guidance to vendors on R&D management, as well as to service providers on the risks linked with NFV environments, NFV technologies, and the new mode of NFV operations. Beyond raising awareness and providing a solid support for discussion, this paper prioritizes risk due to the enormous volume of new information, as well as the magnitude of change that NFV represents for telcos in the coming years.

New environments, such as NFV, bring new business opportunities but also new risks. Security CIA (Confidentiality Integrity Availability) attributes and security operations will most likely be challenged to meet the shared and highly dynamic properties of the NFV environments.

Based on a standardized methodology and using first-hand knowledge, Nokia has identified and prioritized security risks. These risks impact many dimensions: architecture and design, as well as security operations. Ensuring isolation, validating topology, meeting new regulatory compliance, protecting against Denial of Service (DoS) in addition to tracking security incidents across the NFV stack, have been identified as the major security objectives derived from top risks.

---

8 “NFV security: 9 top security impacting choices.” https://resources.nokia.com/asset/201089
10 “Gartner Hype Cycle.” Available at http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp
This paper provides security practitioners with background on risk identification, as well as many illustrations of threats and realistic attack scenarios. Nokia has used the up-to-date consolidated ENISA Threat Taxonomy (ETT). The methodology complies with ISO 27005—the key Information Risk Management Standards. As a result, this makes the paper easier to understand for security experts familiar with similar approaches. As noted, each risk is analyzed in terms of asset-threat-vulnerability, a scenario-based/event-driven approach, and a quantitative and/or qualitative approach.

Finally, it is important to remember that, although security is only a fraction of the overall NFV migration, it is a key and critical success factor for NFV. Ultimately, this paper should also guide decision makers on the allocation of effort and on the resources required for security on the NFV migration path.

Migration to NFV

NFV represents a radical change from the telco perspective. It brings numerous promises that target most of the pain points associated with current legacy environments. These include:

- Agility
- Faster time to market
- Elasticity
- Resource pooling
- Automation
- Location optimization

NFV can be realized by adopting the approach used in the IT environment for many years—replacing dedicated appliances by virtualized IT platforms based on commodity hardware. This also means that the impressive promises listed above can be brought about with cost savings and a reduction of vendor lock-in. Beyond new architecture and platforms, NFV also introduces a new way to design, deploy, and manage network services.

The ETSI NFV (Industry Specification Group) ISG and several industry initiatives from the OPNFV, CSA, TMForum, IETF, IRTF, NGMN, and IEEE are targeting consensus and long-term efforts for standardization in this manner.

As illustrated in Figure 1, an initial high-level architecture diagram has been published and introduces key concepts.

---


13 Some existing IT clouds mitigation techniques are presented in the Appendix. This also gives a further indication of the impact on resources.
MANO stands for NFV Management and Orchestration. It is composed of three function blocks:

- **NFV Orchestrator (NFVO):** The NFVO is responsible for on-boarding of new network services (NS) and virtual network function (VNF) packages; NS lifecycle management, (including instantiation, scale-out/in, performance measurements, event correlation, termination); global resource management; validation and authorization of network functions virtualization infrastructure (NFVI) resource requests.

- **VNF Manager (VNFM):** The VNFM oversees the lifecycle management of VNF instances and the coordination and adaptation role for configuration and event reporting between NFVI and E/NMS.

- **Virtualized Infrastructure Manager (VIM):** The VIM controls and manages the NFVI compute, storage, and network resources, as well as the collection and forwarding of performance measurements and events.

Finally, Figure 1 depicts an overlay boundary known as IaaS (Infrastructure as a Service). This outlines the separation between the network functions and the supporting infrastructure. The NFV stack and its security is discussed in more detail in the white paper, “9 Top Security Impacting Choices.”

---

14 NFV security: 9 top security impacting choices. [https://resources.nokia.com/asset/201089](https://resources.nokia.com/asset/201089)
As one might imagine, the transition to NFV will not occur overnight. As depicted in Figure 2, the NFV journey first made its way through the peak of inflated expectations and then through the trough of disillusionment. Furthermore, as illustrated in Figure 3, other dimensions such as hardware, management, automation, organization, applications and network must all evolve in order to reach the full potential of NFV. These dimensions will continue to evolve differently depending on service providers’ roadmaps and commitments, as well as on their capacity to execute.
To illustrate the migration paths, four phases have been identified on the NFV journey from first deployments to advanced NFV.

- **Type 1**: Single VNF focus
- **Type 2**: NFVI focus
- **Type 3**: MANO focus
- **Type 4**: Highly distributed

Figure 4 depicts these different phases.

**Figure 4: Four types of NFV deployment**

As the slope of enlightenment is slowly climbed, the following question needs to be answered: “What does migrating to NFV mean for security?” The next section introduces an approach for assessing security risks introduced by migrating to NFV.

## Assessing the risk: The approach and methodology

### Context establishment

Risk is formally defined as the effect of uncertainty on objectives.\(^{15}\) When considering migration to NFV environments, uncertainty can arise from the following sources:

- Changes to the operating environment with an additional attack surface layer combined with the complexity of a shared infrastructure

---

• Changes in ownership/liability boundaries with potentially mismatched assumptions and expectations among vendors concerning hardware, hypervisors, VNFs, as well as management and orchestration systems.

NFV risks originate from legacy environment security risks taking on a new dimension, or from new risks inherent in NFV technologies, new architectures, and operating environments.

Although the security practitioner’s intuition is a valid input, Nokia decided to rationalize the methodology based on a dual approach:

• Top down: This approach entails surveying and identifying security issues from industry literature, customer engagements, standard bodies, and research institutions.

• Bottom up: This approach revisits the “usual security suspects” (confidentiality, integrity, availability, etc.) with a view to cloud deployment and the operational environment (IaaS as compared to legacy platforms).

To have a manageable output, Nokia set its objective as the creation and maintenance of a Top 5 list of issues that would cover risk in a holistic way—both in breadth and depth. By providing a strongly grounded security risk assessment, Nokia expects to support and optimize NFV players’ risk treatment, including NFV infrastructure vendors, NFV operators, and VNF providers. The ISO 27005 framework, which summarizes the approach to risk management, is depicted in Figure 5. The terms used are formally defined in the ISO glossary.\(^\text{16}\)

Figure 5: Illustration of an information security risk management process

---

\(^{16}\) [Link to ISO 27005](http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip)
**Risk identification**

Risk identification is the process of finding and describing risks. As mentioned, part of the top-down approach is to survey and identify potential sources of risk based on informed experts’ opinions and stakeholders’ needs. Sessions were held beyond the Nokia security community at large and included IT, the business units, the chief technical officer, as well as Bell Labs Research. Although it is not possible to provide an exhaustive list of sources, the following list provides an overview of our approach since early 2013:

- Service providers engagements from CSO to strategy teams, architecture teams and operational teams, as well as research teams
- Regulatory and government agencies engagements
- Industry events participation
- SDO monitoring and active participation to: ETSI NFV security, IEEE SRPSDVE, IETF
- Industry groups: OPNVF, CSA, TMF, NIS, ISO
- Vendors events
- Academic presentations and invited talks
- Professional security training courses
- Nokia Security Partners input
- Analysts perspectives
- Nokia Bell Labs research projects

When adding regular industry publications and press coverage, Nokia was able to establish an initial list, which was consolidated by domain:

- Segregation and isolation-related issues
  - Data segregation
  - Inter VM traffic isolation
  - System vulnerabilities
  - Shared technology
  - Data breaches
  - Data protection
  - Data loss
  - Insider threats
  - Guest OS isolation

---


• Denial of service-related issues
  – Shared technology
  – Data availability
• Topology-related issues
  – Data location
  – Lack of visibility
  – Elastic network boundaries
• Compliance and regulation-related issues
  – Regulatory compliance
  – Data location
  – Elastic network boundaries
  – Software integrity and trust
• Access and authorization-related issues
  – Privileged user access
  – Access management
  – Multi-factor authentication
  – (Open) API security
  – Hijacking of accounts
  – Insider threats
• Investigative support-related issues
  – Recovery
  – Lack of visibility
  – Visualization and debugging
  – Secure logging
  – Data exfiltration
  – Monitoring and correlation
  – Incident management
  – Guest OS monitoring
• Other identified security issues
  – Long-term viability
  – APT
  – Hardening
  – Data privacy
  – Malware injection
  – Orchestration of security

Risk prioritization

Making long lists of security issues, concerns, and pain points is a comparatively easy task for seasoned security practitioners and consultants. However, setting priority is a much harder and necessary endeavor. Setting priorities introduces a level of subjectivity, which can be challenged by security experts and professionals with significantly different backgrounds and experience.

By default, security issues are of great importance and a never-ending process. This is the case whether one operates in a cloud environment, a co-location facility, or in one's own datacenter. Migration to NFV will not change most of one's existing security struggles and successes. Despite this fact, NFV migration introduces a fair degree of disruption, and NFV players are encouraged to retain their best-practices security practices and gold standards. Those practices and standards have been built from years of operating in legacy telco environments and should be enhanced by IT components developed from experience operating large datacenters.
As noted, the objective of this document is to create a prioritized list, which can be used as prime input for an NFV migration security dashboard. Starting from the identified domains, the selection process took place during a series of internal security workshops, where Nokia finalized the high-level risk assessment process. Nokia used two key selection criteria likely to be high-impact security factors for NFV migration:

1. Type and source of the identified risks:
   - Risks that are new and inherent to NFV. These are risks that did not exist in legacy environments.
   - Incremental risks that are legacy risks already but which assume a new and significantly higher level of risk in an NFV context.

2. Issue of relevance and plausibility of identified risks:
   - Can we find mitigation in existing large public “IT” service providers that appear to address similar risks?  
   - Can we easily identify new or existing threats and elaborate credible attack scenarios given our current knowledge?

This iterative and peer review process led to the creation of a list of the top 5 security risks. This list identifies major security risks when considering migration to NFV environment. The current list is summarized in Table 1. Each risk has a high-level definition, as well as a number of related threat scenarios, which illustrate some possible abuse paths to NFV.

---


20 API security takes on a new dimension in NFV. However, it was decided to attach API security to the top 5 security risks and insert an API-related risk where a more critical impact was identified.
<table>
<thead>
<tr>
<th>Risks</th>
<th>High-level definition</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC-1 Isolation failure</td>
<td>In the NFV deployment and IaaS context, isolation failure becomes a challenge given the additional software layers (Hypervisor/VM), orchestrators and shared infrastructure.</td>
<td>• SEC-1.1: Abuse of host resources or DoS on VM/host exploiting a VM isolation vulnerability (e.g., VM escape)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-1.2: abuse of VM#2 resources or DoS on VM#2 or information leakage (or sharing) about VM#2 exploiting an isolation vulnerability of VM#1 (e.g., VM hopping/jumping, hyper-jumping)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-1.3: Abuse of VM resources or DoS on VM or information leakage (or sharing) about VM exploiting prejudicial data access (in memory, in transit, at rest, or in retirement)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-1.4: Abuse of infrastructure resources or DoS or information leakage (or sharing) by misusing the APIs</td>
</tr>
<tr>
<td>SEC-2 Topology instantiation validation and enforcement failure</td>
<td>In the NFV deployment and IaaS context, the virtual networking configuration layer can be prone to additional errors and make control assurance more challenging.</td>
<td>• SEC-2.1: Eavesdropping, interception, hijacking, or information leakage (or sharing) exploiting dynamic workloads and elastic network boundaries</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-2.2: Eavesdropping, interception, hijacking, or information leakage (or sharing) by misusing the APIs</td>
</tr>
<tr>
<td>SEC-3 Legal and regulatory compliancy failure</td>
<td>In the NFV deployment and IaaS context, the geo-localization of data might need to be enforced. The encryption of specific data might be mandatory. This issue is driven mostly by regulations and laws.</td>
<td>• SEC-3.1: Violation or failure of compliance with geo-deployment regulations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-3.2: Violation or failure of compliance in heterogeneous environments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-3.3: Violation or failure of compliance by insecure APIs</td>
</tr>
<tr>
<td>SEC-4 Infrastructure DoS protection failure</td>
<td>In the NFV deployment and IaaS context, DoS needs to be reconsidered with the additional factor of shared resources (Hypervisor, virtual network, compute and storage, etc.)</td>
<td>• SEC-4.1: DoS or DDoS by network flooding of public interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-4.2: DoS by internal network resource exhaustion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-4.3: DoS by CPU/memory/disk resource exhaustion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-4.4: DoS by malicious misconfiguration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-4.5: DoS of APIs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-4.6: DoS through APIs</td>
</tr>
<tr>
<td>SEC-5 Security incidents identification and troubleshooting failure</td>
<td>In the NFV deployment and IaaS context where infrastructure is operated independently of the applications, security event management and attack identification become more challenging.</td>
<td>• SEC-5.1: Repudiation of actions or unauthorized actions exploiting the loss or destruction of logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-5.2: Repudiation of actions or unauthorized actions exploiting the lack of logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SEC-5.3: Information leakage due to the complexity of defining and reconciling logs’ logical boundaries (technical and organizational)</td>
</tr>
</tbody>
</table>
Each risk (SEC-1 to SEC-5) is described in detail in the remainder of the document. The goal is to provide documentation to distinguish between NFV security’s fear, uncertainty and doubt (FUD) and other associated myths from the security realities. The description is designed to help assign the appropriate level of attention and provide a central point in order to monitor the evolution and relevance of attacks as new scenarios arise or technology advances.

**Risk 1: Isolation failure**

SEC-1 isolation failure is about nefarious and abuse activities with the potential to directly harm new technology assets arising from the migration to an NFV infrastructure (the additional software layers (Hypervisor/VM), shared infrastructure and orchestrators). At the same time, SEC-1 isolation failure may also have an adverse impact on other NFV assets, including VNFs. In this section, only deliberate and malicious threats are covered.

Nokia has defined 16 realistic attack scenarios where the threats, in the context of the new technologies, can cause at least one clear adverse impact. The scenarios align with the shared technology vulnerabilities identified as top threats by the 2016 CSA top threats technical report.

**Assets**

NFV architectures introduce new assets. For simplicity, icons are used for each asset category with assets aligned with the relevant risk.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Assets</th>
</tr>
</thead>
</table>
| Networking | - Switching assets local to a hypervisor, e.g., OVS  
| | - Distributed switching and firewalls assets, e.g., multiple OVSs with switching/routing agents  
| | - Internal virtual NIC cards, e.g., Qemu-emulated NIC  
| | - Internal tunneling protocols, e.g., VXLAN  
| | - Dedicated hardware, e.g., SR-IOV NIC  
| Computing | - vCPU, CPU pining  
| | - Emulated hardware, e.g., Qemu-emulated PCI controller  
| | - Virtual memory and physical memory  
| | - Virtual Machines (VMs)  
| | - Containers  
| Storage | - Virtual disks  
| | - VM images, e.g., OpenStack glance images  
| Orchestration | - Orchestrator of multiple composite NFV applications using templates, e.g., OpenStack Heat and HOT  

---

Threats and realistic attack scenarios

In line with the previously listed assets, this section covers four realistic threats: SEC-1.1, SEC-1.2, SEC-1.3 and SEC-1.4 together with associated attack scenarios prefixed with A-1:

• Attacks from A-1.1.1 to A-1.1.6 are VM escape scenarios where the adversary manages, from a compromised or malfunctioning VNF, to perform actions on the hypervisor. These attacks are not traditional; even so more and more vulnerabilities (e.g., CVE) show that these attacks are doable, and once successfully perpetrated, have a huge impact. Attacks from A-1.2.1 to A-1.2.4 are similar to the VM escape type, augmented with a jump to another VM, either co-located or not with the initial VNF. These attacks are more speculative.

• Attacks from A-1.3.1 to A-1.3.5 list techniques and vectors, including techniques transparent to the VNF. These attacks maliciously access VNF data—in memory, in transit, at rest, or in retirement.

• A-1.4.1 gives an example of how APIs that are used by a VNF to orchestrate other VNFs can be subverted to break the VIM <> VNF isolation.

For the interested reader, additional details are given below:

Table 2. Risk 1 threats, descriptions, impacted assets and attack scenarios

<table>
<thead>
<tr>
<th>Threats</th>
<th>Descriptions</th>
<th>Impacted assets</th>
<th>Attack scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC-1.1: Abuse of host resources or DoS on container/VM/host exploiting a container/VM isolation vulnerability</td>
<td>Process of breaking out (possibly a container first) a VM and interacting with the hypervisor, which is also called a “VM escape.”22</td>
<td></td>
<td>A-1.1.1: One application in a VM leverages errors in the display function to execute arbitrary code in the hypervisor – total compromise (CVE-2009-1244). A-1.1.2: One containerized application hosted in a VM escapes its environment and writes on the /proc/sys VM directories. From the VM, the adversary moves to other VMs until it finds a vulnerable VM to escape from and gets access to the host (CVE-2015-3456) – total compromise. A-1.1.3: One application in the VM sends crafted network packets resulting in an exploitable heap overflow with a compromised virtualization process and execution of arbitrary code on the hypervisor – total compromise. A-1.1.4: One application in the VM triggers specific instructions to interfere with the virtualization process and change the allocated resources – partial compromise. A-1.1.5: One application in the VM triggers some emulated optical drive operations resulting in a crash of the virtualization process. A-1.1.6: one Application in the VM triggers power instruction that halts the VM.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threats</th>
<th>Descriptions</th>
<th>Impacted assets</th>
<th>Attack scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC-1.2: Abuse of VM#2 resources or DoS on VM#2 or information leakage (or sharing) about VM#2 exploiting an isolation vulnerability of VM#1 (or VM#1 and container#1)</td>
<td>Exploits weakness in (possibly a container first) a VM, transforming it into a platform that can be used to launch attacks against other machines that are using the same infrastructure (or the same hypervisor), also called VM hopping/jumping (or VM hyper jumping).</td>
<td>A-1.2.1: One application, “VM escapes,” rewrites the network packets in the hypervisor, and gets network access to the other co-located VMs. A-1.2.2: An adversary with elevated VM privileges reads up to 3 KB of random memory that contains confidential information, if assigned to a different VM or the hypervisor (e.g. CVE-2014-7188) A-1.2.3: One application. “VM escapes,” drops every VM call to migrate A-1.2.4: One application, “VM escapes,” reduces all VM resources</td>
<td></td>
</tr>
<tr>
<td>SEC-1.3: Abuse of container/VM resources or DoS on container/VM or information leakage (or sharing) about container/VM exploiting prejudicial data access (in memory, in transit, at rest, in retirement)</td>
<td>Access to cloud consumer confidential data through various techniques (VM introspection, direct access to storage and memory of the VM, modification of VM images, access to storage and memory of a container) from the host and the infrastructure</td>
<td>A-1.3.1: One honest but curious cloud provider transfers files from the hypervisor to the VM A-1.3.2: One honest but curious cloud provider dumps a VM's memory and extracts passwords in clear text (or any other VNF-specific private key) from a Linux memory dump A-1.3.3: One honest but curious cloud provider dumps a VM's hard disk, reconstructs the partition table, mounts the logical volume, and copies files A-1.3.4: One honest but curious VNF operator instantiates a VNF with a direct device assignment card for performance (e.g., SR-IOV) without IOMMU memory protection and gets access to memory of other co-located VNFs using the same card A-1.3.5: One VIM operator optimizes its infrastructure from a memory point of view: it enables the KSM feature and memory ballooning. One honest but curious VIM operator may get access to swap files and sensitive information (e.g., SSH private keys) or even force some VNF to swap in order to get access to sensitive information</td>
<td></td>
</tr>
<tr>
<td>SEC-1.4: Abuse of infrastructure resources or DoS or information leakage (or sharing) by misusing the APIs</td>
<td>NFV and cloud services highly rely on orchestration and APIs to handle the instantiation of VNFs, the firewall rules instantiation, the whole lifecycle of VNFs (scaling, pausing, stopping, migration, etc.). APIs are boundaries crossing points between zones (e.g. the IaaS provider and the NFV provider). Misuses of APIs may therefore lead to isolation failure.</td>
<td>A-1.4.1: One VNF managing other VNFs requires VIM (e.g., OpenStack) API access to start new VNFs instances. This usage establishes a legitimate connection between the VNF and the infrastructure; if APIs are misused—for instance, if a VM has been compromised—the adversary can use the APIs to break the isolation between the VNFs and the infrastructure.</td>
<td></td>
</tr>
</tbody>
</table>

Risk 2: Topology instantiation validation and enforcement failure

SEC-2 Topology instantiation validation and enforcement failure is about (i) eavesdropping, interception or hijacking, (ii) information leakage or sharing, (iii) isolation failure, failures/malfunctions or (iv) DoS threats that have the potential to directly harm new technology assets arising from the migration to an NFV infrastructure. These threats may also have adverse impacts on other NFV assets, such as VNFs and co-located tenants. Nokia defined eight realistic attack scenarios, where threats in the context of the new technologies, could cause at least one adverse impact.24

Assets

NFV architectures introduce new assets. For simplicity, Nokia uses icons for each asset category, and considers assets particularly relevant to the defined risk:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Networking</th>
<th>Assets</th>
</tr>
</thead>
</table>
| ![Icons](image) | Networking | • Internal switching assets local to a hypervisor, e.g., OVS  
• Internal distributed switching asset, e.g., multiple OVSs with switching/routing agents  
• Internal virtual NIC cards, e.g., Qemu-emulated NIC  
• SDN controller, e.g., Nuage VSD, OpenStack Neutron  
• Internal tunneling protocols, e.g., VXLAN  
• Network traffic between VMs, e.g., east-west  
• Management traffic triggering configuration and actions, e.g., VMkernel traffic for VMware hypervisor management  
• VM migrations, e.g., hot, cold, evacuate  
• Hypervisor layer firewall, e.g., Nuage ACLs in VRS, OpenStack Security Groups in OVS |
| ![Icons](image) | Storage | • Virtual disks  
• VM images, e.g., OpenStack glance images |
| ![Icons](image) | Orchestration | • Orchestrator of multiple, composite NFV applications using templates, e.g., OpenStack Heat and HOT |

24 This is in line with "Weak Identity,” “Credential and Access Management,” “Malicious Insiders, and Shared Technology Vulnerabilities,” which have been identified as top threats by the 2016 CSA top threats technical report.
Threats and realistic attack scenarios

In line with the assets previously listed, here are two realistic threats SEC-2.1 and SEC-2.2—and their associated attack scenarios, which are prefixed with A-2:

- The full software infrastructures, combined with orchestration capabilities, enable the dynamism of the NFV topology. The network dynamism can lead to several attacks:
  - Attack A-2.1.1 illustrates how, after exploiting the “VM escape” attacks developed in the previous section—A-1.1.1 to A-1.1.6—the adversary may alter the Virtual Intrusion Protection System (VIPS) or Virtual Firewall (FVW) template images. This would let the adversary control or subvert any virtual appliance, such as the VIPS or VFW dynamically deployed afterwards. This attack has some level of speculation.
  - Attack A-2.1.2 illustrates how the network dynamism—compared to the legacy cables and physical appliances deployment model—when applied to virtual appliances (enforcing security countermeasures such as firewalls and routers), can unexpectedly lead to faulty isolation between subnets.
  - Attack A-2.1.3 illustrates how the dynamic service chaining/insertion decisions can be subverted to avoid a security inspection.
  - Attack A-2.1.4 illustrates how the dynamic instantiation of commercial virtual appliances (enforcing security countermeasures) may itself be exploited by an adversary. Indeed, by exhausting the amount of licensed virtual firewall, the adversary could trigger a fail-safe mechanism where the virtual appliance filtering features are restricted until new licenses are purchased. Consequently, the adversary might perform network attacks without being blocked or detected (e.g., limited number of sessions with VM-firewall).

- The elasticity of the network can also lead to several attacks:
  - Attacks A-2.1.5 and A-1.2.6 illustrate how an adversary, having knowledge of a multi-site deployment, could exploit the elasticity of the NFV environment. In particular, the attacker could trigger either a VNF migration or a deployment over a site to violate the initial security design.
  - Attacks A-2.2.1 and A-2.2.2 illustrate how insecure APIs can subvert the initial security design. Indeed, the NFV infrastructure relies heavily on the VIM infrastructure APIs to provide the dynamism and elasticity. These are well-known attacks outside of NFV.

For the interested reader, additional details are given below:

---

Table 3. Risk 2 threats, descriptions, impacted assets and attack scenarios

<table>
<thead>
<tr>
<th>Threats</th>
<th>Descriptions</th>
<th>Impacted assets</th>
<th>Attack scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC-2.1: Eavesdropping, interception, hijacking, or information leakage (or sharing) exploiting dynamic workloads and elastic network boundaries</td>
<td>In NFV, network and security controls are not limited by location and physical constraints. Anywhere in the datacenter, the network segmentation, firewall rules and other network services move with the workload. Boundaries are dynamic, changing over time along with changing scope (e.g., spawning new VNFs), which complicate security topology validation and enforcement.</td>
<td><img src="image" alt="Diagram" /></td>
<td>A-2.1.1: By leveraging A-1.1.x attack scenarios, an adversary may compromise a network element golden image, such as a VIPs, in order to control all traffic going through each VIP instance. The adversary may divert some traffic flows or enable eavesdropping; this is also called traffic diversion. A-2.1.2: A VNF operator launches a virtual router by mistake (e.g., OpenStack Neutron L3 agent) and interconnects Layer 2 networks without a firewall in between. Dues to such ease of use and the software routing component’s low maturity level, the zoning of a NFV solution can be jeopardized. A-2.1.3: A VNF service is running and a decision for an IPS service insertion has been made by the security orchestrator. To implement this decision, one service chaining instantiation option is to alter the network path based on network attributes. The problem, though, is that the network attributes may be crafted to enable avoidance of an IPS inspection. A-2.1.4: A VNF is compromised and floods the API of the VFW instantiation server. In this case, the adversary might succeed in exhausting commercial VFW licenses. This scenario can allow the adversary to perform well-known exploits while the VFW inspection capabilities are restricted until new licensed are purchased. A-2.1.5: A VNF service is running on a given cloud infrastructure. An adversary might flood the VNF to trigger the migration of VNFs in another cloud with lower security capabilities. These might include no IDS/IPS/DPI inspection capabilities. The adversary can then exploit vulnerabilities without being detected and blocked at the network level. A-2.1.6: A VNF service is running on a given cloud infrastructure. An adversary might flood the VNF to launch the instantiation of new VNFs in the cloud where the adversary as physical cable access to dump all network packets.</td>
</tr>
</tbody>
</table>

| SEC-2.2: Eavesdropping, interception, hijacking, or information leakage (or sharing) by misusing the APIs | Some parts of the topology instantiation are enforced by the infrastructure provider who gets the provisioning rules and designs templates from the NFV provider; the NFV provider may assume that the actual/effective topology matches the topology design rules given but the actual/effective topology instantiation may have failed (e.g. no firewalling, no anti-spoofing rules) due to misuse of the APIs. | ![Diagram](image) | A-2.2.1: An OpenStack heat template has an invalid CIDR and causes a Neutron security groups bypass (CVE-2014-0187) that is exploited by a compromised VM. A-2.2.2: The anti-IP spoofing rules, anti-MAC spoofing rules, and anti-DHCP spoofing rules are bypassed by a tenant administrator who accidentally changes the device-owner field of a compute node’s port to something that starts with ‘network’ thereby starting a VM. On the VIM layer, this VM will have no IP table rules applied to it (CVE-2015-5240) but the VM application will not know explicitly that is the case. | ![Diagram](image) |
Risk 3: Legal and regulatory compliance failure

SEC-3 legal and regulatory compliance failure is about threats, such as (i) violation of laws or regulations and (ii) failure to meet contractual requirements. These threats are associated with prohibition of commercial service and/or financial penalties. These are not generally new, but new regulations in the cloud field are emerging. Forthcoming regulations include the General Data Protection Regulation (GDPR). It is a regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). The GDPR was developed with a focus on social networks and cloud providers.26

In this section, seven realistic attack scenarios have been defined, where the threats in the context of the new technologies, cause at least one clear adverse impact.27

Assets

NFV architectures introduce new assets. For simplicity, we are using icons for each asset category, and considering assets particularly relevant to this risk:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Assets</th>
</tr>
</thead>
</table>
| Networking | • SDN controller, e.g., Nuage VSD, OpenStack Neutron  
| | • VM migrations, e.g., hot, cold, evacuate  
| | • Hypervisor layer firewall, e.g., Nuage ACLs in VRS, OpenStack Security Groups in OVS |
| Computing | • vCPU, CPU pining  
| | • Emulated hardware, e.g., Qemu-emulated PCI controller  
| | • Virtual memory and physical memory  
| | • VMs  
| | • Containers |
| Storage | • Virtual disks  
| | • VM images, e.g., OpenStack glance images  
| | • Databases, e.g., MySQL  
| | • Objects, e.g., OpenStack swift object storage |
| Orchestration | • Orchestrator of multiple composite NFV applications using templates, e.g., OpenStack Heat and HOT  
| | • Placement of images or database or objects (data at rest)  
| | • Placement of VMs, e.g., OpenStack Nova placement |

26 Wikipedia article on General Data Protection Regulation. Available at https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Threats and realistic attack scenarios

In line with the assets previously listed, here are three realistic threats—SEC-3.1, SEC-3.2 and SEC-3.3—and their associated attack scenarios prefixed with A-3.

- Attacks from **A-3.1.1** to **A-3.1.3** are geo-deployment related. These are based on placement, migration, and replication features that were not possible outside of well-defined boundaries with the legacy infrastructure. They are used against VNFs in a way that violates a law and/or regulation. These scenarios are realistic, whether it is an attack, an abuse, or a lack of restrictions enforcement.

- Attack **A-3.2.1** refers to the previous three attacks—A-3.1.1 to A-3.1.3—in a larger deployment scope (i.e., with heterogeneous and distributed infrastructures).

- Attack **A-3.2.2** concerns disaster-like scenarios where the adversary manages to force a migration from one cloud infrastructure to another (e.g., to a backup one) that is not compliant with the latest laws, regulations, or certifications (industry standards).

- Attack **A-3.3.1** illustrates how insecure APIs can lead to legal or regulatory violations. A speculative scenario is proposed about VNF-exposed APIs in a telco.²⁸

For the interested reader, additional details are given below:

Table 4: Risk 3 threats, descriptions, impacted assets, and attack scenarios

<table>
<thead>
<tr>
<th>Threats</th>
<th>Descriptions</th>
<th>Impacted assets</th>
<th>Attack scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC-3.1: Violation of geo-deployment regulations</td>
<td>Data in use, motion, or at rest in foreign locations during normal operations or even during recovery can lead to regulatory redress, accidental or deliberate/malicious VM geo-deployment (e.g., replication of data across datacenters in different regions (America, EMEA, APAC)) can encounter this problem.</td>
<td>![icon]</td>
<td>A-3.1.1: Placement: One VNF application can be placed in a violating location, according to regulations and policies. A-3.1.2: Migration: One VNF application can be migrated to a violating location, according to regulations and policies. A-3.1.3: Replication: VNF application data can be replicated to a violating location, according to regulations and policies.</td>
</tr>
</tbody>
</table>

²⁸ This kind of scenario has happened already in the IT environment. In mid-2015, the US Internal Revenue Service (IRS) exposed more than 300,000 records using a vulnerable API.
## Threats, Descriptions, Impacted assets, and Attack scenarios

<table>
<thead>
<tr>
<th>Threats</th>
<th>Descriptions</th>
<th>Impacted assets</th>
<th>Attack scenarios</th>
</tr>
</thead>
</table>
| SEC-3.2: Violation or failure of compliance in heterogeneous environments | In certain scenarios, the application (cloud consumer) might rely on multiple cloud providers. Enforcing the constraints associated with regulation geo-deployment (SEC-3.1) become (most probably) a more complex issue with hybrid cloud deployment environments (i.e., inter-heterogeneous cloud/cloud provider enforcement of locations policies. | ![Diagram](image1.png) | **A-3.2.1**: Use of replication/migration/replication vulnerabilities across multiple cloud providers (e.g., offload) (Scenarios A-3.1.1, A-3.1.2, A-3.1.3 from SEC-3.1).  
**A-3.2.2**: In a hybrid scenario, where the public cloud is used for disaster recovery, an adversary could force the disaster recovery scenario and the compliance might be violated for data in transit and even at rest during recovery. |

| SEC-3.3: Violation or failure of compliance by insecure APIs | NFV and cloud use APIs. NFV can even expose some APIs to allow dynamicity, interoperability, and service chaining/insertion. These APIs can lead to data breaches, therefore violating laws and regulations (e.g., privacy). | ![Diagram](image2.png) | **A-3.3.1**: An adversary might exploit a vulnerable and exposed telco VNF API to dump a database of personally identifiable information (PII). |

## Risk 4: Infrastructure DoS protection failure

In this section, only deliberate and malicious threats are covered. SEC-4 Infrastructure DoS protection failure concerns nefarious and abuse activities with the potential to directly harm new technology assets arising from the migration to an NFV infrastructure (e.g., the additional software layers (hypervisor/VM), shared infrastructure and orchestrators) in addition to adverse impacts on other NFV assets, such as VNFs.

In this section, 12 realistic attack scenarios have been defined where the threats, in the context of the new technologies, cause at least one clear adverse impact.²⁹

Assets
NFV architectures introduce new assets. For simplicity, we are using icons for each asset category, and considering assets particularly relevant to this risk:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>• Internal switching assets local to a hypervisor, e.g., OVS</td>
</tr>
<tr>
<td></td>
<td>• Internal distributed switching asset, e.g., multiple OVS with switching/routing agents</td>
</tr>
<tr>
<td></td>
<td>• Internal virtual NIC cards, e.g., Qemu-emulated NIC</td>
</tr>
<tr>
<td></td>
<td>• Internal tunneling protocols, e.g., VXLAN</td>
</tr>
<tr>
<td>Computing</td>
<td>• vCPU, CPU pining</td>
</tr>
<tr>
<td></td>
<td>• Virtual memory and physical memory</td>
</tr>
<tr>
<td>Storage</td>
<td>• Virtual disks</td>
</tr>
<tr>
<td></td>
<td>• VM images, e.g., OpenStack glance images</td>
</tr>
<tr>
<td>Orchestration</td>
<td>• Orchestrator of multiple composite NFV applications using templates, e.g., OpenStack Heat and HOT</td>
</tr>
<tr>
<td></td>
<td>• Placement of images or database or objects (data at rest)</td>
</tr>
<tr>
<td></td>
<td>• Placement of VMs, e.g., OpenStack Nova placement</td>
</tr>
</tbody>
</table>

Threats and realistic attack scenarios
In line with the assets previously listed, here are six realistic threats—SEC-4.1, SEC-4.2, SEC-4.3, SEC-4.4, SEC-4.5 and SEC-4.6—which are associated with attack scenarios, prefixed with A:

- Attacks **A-4.1.1** and **A-4.1.2** concern network DoS and DDoS against or from VNF public interfaces.
- Attacks **A-4.2.1** to **A-4.2.3** are about internal network DoS and DDoS from VNF to VNF in different deployment scenarios (co-location, same site, different sites). Attack **A-4.2.4** is about DoS or DDoS arising from numerous migrations in a limited timeframe, possibly exhausting network bandwidth.
- Attacks **A-4.3.1** to **A-4.3.3** are similar to the previous DoS and DDoS attacks, but are leveled against the CPU, memory, or disk.
- Attack **A-4.4.1** is about rogue administrators. It demonstrates possible adverse impacts of an internal threat on the infrastructure.
- Attacks **A-4.5.1** and **A-4.6.1** show how APIs can be the target or the source of DoS.

For the interested reader, additional details are given below:
Table 5. Risk 4 threats, descriptions, impacted assets, and attack scenarios

<table>
<thead>
<tr>
<th>Threats</th>
<th>Descriptions</th>
<th>Impacted assets</th>
<th>Attack scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC-4.1: DoS or DDoS by network flooding of public interface</td>
<td>External network resources exhaustion</td>
<td></td>
<td>A-4.1.1: Network Distributed DoS (DDoS) - multiple machines external to the cloud flood the public facing vNF App interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A-4.1.2: Network Distributed DoS (DDoS) - multiple Virtual Machines hosting Apps flooding from the cloud outside through the public interfaces</td>
</tr>
<tr>
<td>SEC-4.2: DoS by internal network resource exhaustion</td>
<td>External network resources exhaustion</td>
<td></td>
<td>A-4.2.1: High volume of network traffic from VNF Apps to VNF apps co-located on the same HV</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A-4.2.2: High volume of network traffic from vNF apps to VNF apps on different HVs – same site</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A-4.2.3: High volume of network traffic from vNF apps to VNF apps on different HVs – different sites</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A-4.2.4: VNF apps exhausting (network; CPU; storage) resources to trigger a migration and consume all the bandwidth</td>
</tr>
<tr>
<td>SEC-4.3: DoS by CPU/memory/disk resource exhaustion</td>
<td>Compute resources exhaustion</td>
<td></td>
<td>A-4.3.1: One VNF application consumes the VM’s CPU and, by extension, of the hypervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A-4.3.2: One VNF application consumes the VM’s memory resource and, by extension, of the hypervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A-4.3.3: One VNF application writes intensively outside the expected range to the disk, and reduces the overall performance</td>
</tr>
<tr>
<td>SEC-4.4: DoS by malicious misconfiguration</td>
<td>Unauthorized access to the hypervisor using management interfaces. This can allow rogue administrators to create VMs, installing rootkits, installing rogue placement routines...</td>
<td></td>
<td>A-4.4.1: Rogue administrators using theft cloud consumer portal admin credentials (e.g., CloudBand Management System self-provisioning portal)</td>
</tr>
<tr>
<td>SEC-4.5: DoS of APIs</td>
<td>APIs exposed by the VIM (e.g., OpenStack) and VNFM enable orchestration, management, and operations. APIs expose capabilities for service chaining and migration etc. A DoS on the APIs could prohibit any VIM and NFV actions.</td>
<td></td>
<td>A-4.5.1: By sending a single request with the same authentication method multiple times, a remote attacker could generate unwanted load on the authentication server (e.g., OpenStack Keystone host), resulting in a DoS of the authentication service; As a result, all actions that require authentication would be denied. In the case of the Keystone authentication server, it would result in a DoS on the VIM infrastructure (e.g., CVE-2014-2828).</td>
</tr>
<tr>
<td>SEC-4.6: DoS through APIs</td>
<td>APIs exposed by the VIM (e.g., OpenStack) and the VNFM enable orchestration, management, and operations. APIs expose many capabilities, and can be exploited to perpetrate a DoS on the VIM or NFV infrastructure.</td>
<td></td>
<td>A-4.6.1: By active servers listing request using an IP filter, an authenticated user could overload the VIM component (e.g., OpenStack nova-network or neutron-server process), resulting in a DoS (e.g., CVE-2014-3708).</td>
</tr>
</tbody>
</table>
Risk 5: Security incidents identification and troubleshooting failure

SEC-5 security incidents identification and troubleshooting failure is about threats, such as (i) accidental damage, including information leakage, as well as the usage of unreliable information or a response with inadequate design (possibly leading to DoS, information leakage or sharing etc.), (ii) nefarious activity and abuse, including repudiation of actions, falsification of records, unauthorized actions, (iii) and damage to or loss of assets, including the loss of integrity of sensitive information or destruction of logs.

These threats have the potential to directly harm new technology assets arising from migration to an NFV infrastructure, and may also have adverse impacts on other NFV assets, such as VNFS and co-located tenants.

In this section, seven realistic attack scenarios are defined where the threats, in the context of the new technologies, cause at least one clear adverse impact.30

Assets

NFV architectures introduce new assets. For simplicity, we are using icons for each asset category, and considering assets particularly relevant to this risk:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Assets</th>
</tr>
</thead>
</table>
| Networking | • Internal switching assets local to a hypervisor, e.g., OVS  
| | • Internal distributed switching asset, e.g., multiple OVS with switching/routing agents  
| | • Internal virtual NIC cards, e.g., Qemu-emulated NIC  
| | • SDN controller, e.g., Nuage VSD, OpenStack Neutron  
| | • Internal tunneling protocols, e.g., VXLAN  
| | • Network traffic between VMs, e.g., east-west  
| | • Management traffic triggering configuration and actions, e.g., VMkernel traffic for VMware hypervisor management  
| | • VM migrations, e.g.,hot, cold, and evacuate  
| | • Hypervisor layer firewall, e.g., Nuage ACLs in VRS, OpenStack Security Groups in OVS |
| Computing | • vCPU, CPU pining  
| | • Virtual memory and physical memory |
| Storage | • Virtual disks  
| | • VM images, e.g., OpenStack glance images |
| Orchestration | • Orchestrator of multiple, composite NFV applications using templates, e.g., OpenStack Heat and HOT |

Threats and realistic attack scenarios

In line with the assets previously listed, here are three realistic threats—SEC-5.1, SEC-5.2 and SEC-5.3—and associated attack scenarios prefixed with A-5:

- Some scenarios are about troubleshooting and forensics being delayed or even prevented:
  - Massive logs generation from the VNF on the infrastructure side with attacks A-5.1.1 and A-5.1.2
  - Exploitation of cloud-intrinsic ephemeral resources, such as disks, to hide malicious actions with attack A-5.1.3
  - Exploitation of privileged access to the hypervisor to perform actions on the VNF without any logs due to missing logging features, using attack type A-5.2.1;
  - Time to process and “filter” infrastructure common logs to NFV operator-specific logs with attack A-5.2.2

- A-5.3.1 and A-5.3.2 are exploits based on poorly defined technical and organization boundaries, such as sensitive information leakage in the infrastructure logs, when delivered to the VNF operator. These scenarios are realistic, and could even be extrapolated such that sensitive information from one VNF operator is transferred to another VNF operator using the same infrastructure logs leak scenario.

For the interested reader, additional details are given below:

Table 6. Risk 5 threats, descriptions, impacted assets, and attack scenarios

<table>
<thead>
<tr>
<th>Threats</th>
<th>Descriptions</th>
<th>Impacted assets</th>
<th>Attack scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC-5.1: Repudiation of actions or unauthorized actions exploiting loss or destruction of logs</td>
<td>Loss or destruction of logs make repudiation and unauthorized adversaries actions possible; it is a security issue regarding availability and integrity.</td>
<td></td>
<td>A-5.1.1: One VNF application generates logs intensively on the hypervisor side, making other applications analysis impossible when logs have rotated and the early entries have been deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A-5.1.2: An adversary generates network traffic and therefore triggers instantiations and migrations of VMs, possibly generating many logs; this “noise” can slow a root-cause analysis of network troubleshooting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A-5.1.3: Shutdown or VMs reboot, using non-persistent disks to remove any traces.</td>
</tr>
</tbody>
</table>
### Threats | Descriptions | Impacted assets | Attack scenarios
--- | --- | --- | ---
SEC-5.2: Repudiation of actions or unauthorized actions exploiting the lack of logs | Lack of logs due to missing logs/features make repudiation and unauthorized adversaries actions possible; it is a security issue regarding availability. |  | A-5.2.1: A malicious hypervisor administrator executes commands (e.g., commands to the QEMU-monitor); these are not logged (not possible to log them as per today). A VM fails and logs are not rich enough to help the forensics and incident response team qualify the incident and its root cause. A-5.2.2: One VNF operator requests real-time remote access to IaaS logs for troubleshooting a networking issue. The operator receives the logs after a few hours delay, due to the number of logs requiring a longer processing time. When the logs are received, the unauthorized actions may be unveiled but only after the exploit has been performed. |
SEC-5.3: Information leakage due to the complexity of defining and reconciling logs’ logical boundaries (technical and organizational) | Failure of defining appropriate logs’ logical boundaries is a security issue regarding confidentiality. |  | A-5.3.1: Logs generated at the infrastructure level about an NFC failure leak sensitive information (e.g., OpenStack Nova logs with internal password leakage (CVE-2015-8749). A-5.3.2: One VNF operator requests logs generated at the infrastructure level (e.g., OpenStack Keystone) for a root-cause analysis, and the infrastructure provider inadequately filters the logs that contain information about its own internal passwords for its backends (CVE-2015-3646) |

### Next steps and going forward

Despite efforts to deliver a manageable and prioritized list of security risks, the previous sections provide a significant amount of information to process. Some of the attacks described are real whereas others are more speculative. The list, though, is not exhaustive. In an earlier section titled “Migration to NFV,” a number of phases were introduced, highlighting four possible types of deployments on the NFV migration path (see Figure 4).

When carefully considering the top five security risks with respect to each type, it became clear that the relevance of each risk-related security objective depended on the deployment type. In order to further refine guidance to the targeted audience, the evolution of the requirement for each objective was evaluated with respect to NFV maturity.
The evaluation was based on a 4-level scale:31

- **N/A**: Not Applicable
- **May**: This word means that the security objective is truly optional. The NFV community may choose to include the item because a particular marketplace requires it, or because it brings a differentiator.
- **Should**: This word means that there may exist valid reasons in particular circumstances to ignore a particular security objective, but the full implications must still be understood and carefully weighed before choosing a different course.
- **Must**: This word means that the security objective is an absolute requirement.

The evaluation is summarized in the Table 7 below. The value of the table is twofold. First, it provides a graded investment for each security objective as an organization moves on the NFV migration path. Second, when read vertically for each deployment type, the table gives the organization a clear set of objectives and a useful NFV migration risk dashboard.

Table 7. Risk mitigation priorities according to the four NFV deployment types

<table>
<thead>
<tr>
<th>NFV migration path</th>
<th>Type 1</th>
<th>Type 2</th>
<th>Type 3</th>
<th>Type 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sec. Objective 1: ensuring isolation</td>
<td>May</td>
<td>Should</td>
<td>Must</td>
<td>Must</td>
</tr>
<tr>
<td>Sec. Objective 2: validating topology</td>
<td>N/A</td>
<td>Should</td>
<td>Must</td>
<td>Must</td>
</tr>
<tr>
<td>Sec. Objective 3: meeting new regulatory compliance</td>
<td>N/A</td>
<td>May</td>
<td>Should</td>
<td>Must</td>
</tr>
<tr>
<td>Sec. Objective 4: protecting against DoS</td>
<td>Should</td>
<td>Must</td>
<td>Must</td>
<td>Must</td>
</tr>
<tr>
<td>Sec. Objective 5: tracking security incidents</td>
<td>May</td>
<td>Should</td>
<td>Must</td>
<td>Must</td>
</tr>
</tbody>
</table>

Finally, it is recognized that there is no pre-defined NFV migration path and that the 4 types illustrate rather than identify all possible deployment models. In order to further support organizations, another complementary input has been proposed for the NFV migration risk dashboard. This more precisely captures the actual position on the NFV journey, according to the six dimensions mentioned in the earlier “Migration to NFV” section (see Figure 3). Figure 6 illustrates this representation using a Kiviat chart. The grey line in the center represents the current legacy deployment model, and the outer green line represents the full NFV potential deployment reaching the best NFV attribute on each of the six dimensions. In blue, each organization is able to depict and monitor its current status, as it moves from legacy deployment (grey) to full NFV potential (green).

31 Radner, S.: Key words for use in RFCs to Indicate Requirement Levels. 1997.
In order to link the previous table and the Kiviat chart, the organization needs to define the acceptable level of risk for its current position on the migration chart. This representation is also useful to define minimum and maximum thresholds for each dimension. Those two inputs provide solid tools to embark on the NFV journey with confidence.

**Figure 6. NFV migration status and objectives**

![Kiviat chart](image)

**Concluding remarks**

After three years of intense NFV security activities with insights shared between customers and stakeholders, Nokia has formalized the security risks for telcos that are migrating from legacy environments to NFV. Support has been provided in the form of a detailed description and methodology to prioritize risk. In addition, possible paths forward on the NFV journey have been identified, as well as an assessment of the relevance of each identified risk. The resulting table provides solid input for an NFV migration risk dashboard.

At the same time, it is important to recognize that organizations are different and move at different speeds. As a result, each organization needs to adapt the approach to risk provided in this paper to match its particular culture (for change, for risk) and plans for NFV adoption by:
• Defining NFV migration phases (e.g., type 1-4)
• Performing the specific risk treatment step to reflect the approach to risk in the organization’s culture (Avoid/mitigate/accept or transfer risk)
• Investigating and defining the mitigation plan with associated resource levels
• Assigning the appropriate level of resources to match the acceptable level of risk for the organization.

And finally:
• Documenting and communicating the risk management policy.

If all these steps are taken, an organization will be able to successfully undertake its NFV migration journey with a clear picture of the associated security risks.

Acronyms

ACL       Access Control List
API       Application Programming Interface
APT       Advanced Persistent Threat
BU        Business Unit
CIDR      Classless Inter-Domain Routing
CMS       Cloud Management System
COTS      Commercial off-the-shelf
CPU       Central Processing Unit
CSP       Cloud Service Provider
CVE       Common Vulnerabilities and Exposures
DMA       Direct Memory Access
DoS       Denial of Service
FUD       Fear Uncertainty Doubt
HGFS      Host Guest File System
HLD       High Level Design
HOT       Heat Orchestration Template
HW        Hardware
IOMMU     Input/Output Memory Management Unit
ISO       International Organization for Standardization
IT        Information Technology
KPI Key Performance Indicator
KQI Key Quality Indicator
KSM Kernel Samepage Merging
KVM Kernel-based Virtual Machine
LCM (VNF) Life Cycle Manager (5620SAM)
MANO Management and organization
NFV Network Function Virtualization
OS Operating System
OSS Operations Support Systems
OVS OpenVSwitch
PCI Peripheral Component Interconnect
RAM Random-Access Memory
SR-IOV Single Root-Input/Output Virtualization
TPM Trusted Platform Module
VIM Virtualized Infrastructure Manager
VM Virtual Machine
VNF Virtualized Network Function
VNFM Virtualized Network Function Manager
VXLAN Virtual Extensible LAN

References


Gartner Hype Cycle. Available at http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp


Kernel-based Virtual Machine official website. Available at http://www.linux-kvm.org/page/Main_Page

Management and organization. Available at https://www.sdxcentral.com/resources/nfv/nfv-man/


Next Generation Mobile Networks. Available at http://www.ngmn.org/home.html

NFV in ETSI. Available at http://www.etsi.org/technologies-clusters/technologies/nfv


Open Platform for NFV (OPNFV) official web site. Available at https://www.opnfv.org/
OpenStack L3 Agent configuration. Available online at http://docs.openstack.org/admin-guide-cloud/content/install_neutron-l3.html

OpenStack official website. Available at https://www.openstack.org/

OpenStack Operations Guide. Available at http://docs.openstack.org/ops/

Radner, Scott. Key words for use in RFCs to Indicate Requirement Levels. 1997.


TM Forum the global industry association. Available at https://www.tmforum.org/zoom/


VMware vShield endpoint. Available at http://www.vmware.com/products/vsphere/features/endpoint.html


Wikipedia article on General Data Protection Regulation. Available at https://en.wikipedia.org/wiki/General_Data_Protection_Regression

Appendix

Existing mitigation techniques

The white paper, “Top 9 NFV Security Impacting Choices,” focuses on technologies and associated mitigation techniques in an OpenStack and KVM environment. The paper represents one point in time as all aspects of this issue are rapidly evolving. Existing—prior to NFV—security best practices (e.g., hardening, secure management, secure logging, secure patching, traffic isolation, network attack filtering and secure routing) are still valid. In particular, vulnerability management is key in the NFV environment. Indeed, infrastructure components are also continuously evolving (e.g., OpenStack). Consequently, performing careful vulnerability management using regular survey and patching of infrastructure components is crucial. This is especially the case regarding:

Hypervisors:
- Xen: http://xenbits.xen.org/xsa/
- VMWare: http://blogs.vmware.com/security/
- Others (KVM, and more): http://seclists.org/oss-sec

Cloud Management System:
- OpenStack vulnerability management:
  - It is recommended keeping up to date on security issues and advisories, as they are published. The OpenStack Security Portal (https://security.openstack.org) is the central portal where advisories, notices, meetings, and processes can be coordinated. Additionally, the OpenStack Vulnerability Management Team (VMT) portal (https://security.openstack.org/#openstack-vulnerability-management-team) coordinates remediation within the OpenStack project, as well as the process of investigating reported bugs, which are responsibly disclosed (privately) to the VMT, by marking the bug as ‘This bug is a security vulnerability’. Further detail is outlined in the VMT process page (https://security.openstack.org/vmt-process.html#process) and results in an OpenStack Security Advisory or OSSA. This OSSA outlines the issue and the fix, as well as linking to both the original bug, and the location where the where the patch is hosted.

SEC-1.1: Isolation failure by VM escape

OpenStack and KVM

Some security mitigation techniques are developed in the white paper titled “Top NFV Security Impacting Choices.”

---

32 NFV security: Top 9 security impacting choices. https://resources.nokia.com/asset/201089
33 Ibid.

---
VMware
- A-1.1.1: Disable virtual floppy
- A-1.1.2: Disable virtual optical drives
- A-1.1.3: Disable virtual parallel ports
- A-1.1.3: Disable virtual serial ports
- A-1.1.3: Disable virtual USB ports

SEC-1.3: Isolation failure by prejudicial data access
VMware
- A-1.3.1: Disable HGFS

SEC-4.1: DoS or DDoS by network flooding of public interface
Amazon EC2
- A-4.1.1 Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny-all mode and Amazon EC2 customers must explicitly open the ports needed to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain Routing [CIDR] block).
- A-4.1.1, A-4.1.2 CloudWatch Security: web service that provides monitoring for AWS cloud resources. Visibility into resource utilization, operational performance, and overall demand patterns, including metrics, such as CPU utilization, disk reads and writes, as well as network traffic. Customers can set up CloudWatch alarms to be notified when certain thresholds are crossed, or to take other automated actions, such as adding or removing EC2 instances, if auto-scaling is enabled
- A-4.1.1 Proprietary DDoS mitigation techniques are used. Additionally, AWS’s networks are multi-homed across a number of providers to achieve internet access diversity.

OpenStack Neutron
- «Security Groups» grants administrators and tenants the ability to specify the type of traffic and direction (ingress/egress) that is allowed to pass through a quantum port (belonging to a particular VM). A security group is a container for security group rules; each rule is based on source/destination IP and TCP ports.
- Since Havana release (November 2013), FWaaS has enriched security groups with the ability to express application characteristics, which some of the next-generation firewalls do.
SEC-4.2: DoS by internal network resource exhaustion

Amazon EC2

• A-4.2.1: CloudWatch Security: Web service that provides monitoring for AWS cloud resources. Visibility into resource utilization, operational performance, and overall demand patterns, including metrics, such as CPU utilization, disk reads and writes, as well as network traffic. Customers can set up CloudWatch alarms to be notified when certain thresholds are crossed, or to take other automated actions, such as adding or removing EC2 instances, if auto-scaling is enabled.

• A-4.2.1: EC2-VPC, Regular VPC: Can run instance on shared hardware or single-tenant hardware (dedicated instances)

• A-4.2.1, A-4.2.2, A-4.2.3: AWS firewalls (security groups) resides within the hypervisor layer - both ingress and egress

• A-4.2.1, A-4.2.2, A-4.2.3: Isolation of tenants using VPC: proprietary solution

VMware

• A-4.2.1, A-4.2.2, A-4.2.3, A-4.2.4: Several ways to provide QoS:
  – Hypervisor QoS—vSphere 5.5 announced features: Traffic filtering enhancements – the vSphere distributed switch now supports packet classification and filtering based on MAC SA and DA qualifiers, traffic type qualifiers (i.e., vMotion, Management, FT), and IP qualifiers (i.e., protocol, IP SA, IP DA, and port number).
  – Adapter-based QoS with hardware protocol offload—Moving the switching functions from the hypervisor to the adapter offers not only minimum bandwidth guaranteed QoS, but hardware-offload capabilities, which lower the server RAM and CPU utilization and maximize overall system performance. QLogic technology for switch-agnostic NIC Partitioning (NPAR) dedicates bandwidth and QOS specifically to individual applications, such as VM mobility, hypervisor management or storage traffic, along with the various applications running in the VMs that are being serviced, as recommended by hypervisor vendors, such as VMware.34
  – Adapter-based QoS with software initiators—In this case, the NIC handles the QoS, but the protocol processing is still performed in software running on the CPU, which affects the CPU's overall performance.
  – Rate limiting—Some QoS implementations support only a simple rate limiting paradigm, rather than intelligent QoS with a minimum bandwidth guarantee. With rate limiting, each application is assigned a specific amount of bandwidth that cannot be exceeded, regardless of whether the bandwidth assigned to other applications is being used.

• SDN NSX: NSX reproduces the entire networking environment, L2, L3, L4 to L7 network services, in software within each virtual network. NSX offers a distributed logical architecture for L2 to L7 services, including logical switch, router, firewall, load balancer and VPN. These logical network services are provisioned programmatically when VMs are deployed and move with VMs.

<table>
<thead>
<tr>
<th>QoS functions of VMware networking software - 2010</th>
<th>vSwitch</th>
<th>vDS</th>
<th>Nexus 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Marking</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Policing</td>
<td>Yes (outbound only)</td>
<td>Yes (outbound and Inbound, simple PQ mode)</td>
<td>Yes</td>
</tr>
<tr>
<td>Shaping</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**OpenStack Neutron**

• Since November 2013, a decision has been made to start with a simple API to manage QoS at the port level so there is no QoS at the tenant level for now. A first implementation of reference will be for the OpenvSwitch agents.

**SEC-4.3: DoS by CPU/Memory/Disk resource exhaustion**

**Amazon EC2**

• A-4.3.1, A-4.3.3 CloudWatch Security: Web service that provides monitoring for AWS cloud resources. Visibility into resource utilization, operational performance, and overall demand patterns, including metrics, such as CPU utilization, disk reads and writes, as well as network traffic. Customers can set up CloudWatch alarms to be notified when certain thresholds are crossed, or to take other automated actions, such as adding or removing EC2 instances, if auto-scaling is enabled.

**VMware**

• CPU

  • Resource allocation: Sharing profile, resource reservation, limit
    – Hyperthreading core sharing

• Memory

  • Resource allocation: Sharing profile, resource reservation, limit

• Disk

• Limit IOPs
Figure 7. ESXi CPU reservation configuration panel

Figure 8. ESXi advanced CPU options configuration panel
SEC-4.4: DoS by malicious misconfiguration

Amazon EC2

- A-4.4.1 AWS security monitoring tools help identify several types of DoS attacks, including distributed, flooding, and software/logic attacks.
- A-4.4.1 AWS access—The AWS production network is segregated from the Amazon corporate network and requires a separate set of credentials for...
logical access. The Amazon corporate network relies on user IDs, passwords, and Kerberos, while the AWS production network requires SSH public-key authentication through a bastion host.

• A-4.4.1 Account review and audit—Accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee’s record is terminated in Amazon’s human resources system. Windows and UNIX accounts are disabled and Amazon’s permission management system removes the user from all systems.

• A-4.4.1 Background checks—AWS has established formal policies and procedures to delineate the minimum standards for logical access to the AWS platform and infrastructure hosts. AWS conducts criminal background checks, as permitted by law, as part of pre-employment screening practices for employees and commensurate with the employee’s position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

• A-4.4.1 Credentials policy—AWS security has established a credentials policy with required configurations and expiration intervals. Passwords must be complex and changes to passwords are forced every 90 days.

• A-4.4.1 Secure design principles—AWS’s development process follows secure software development best practices, which include formal design reviews by the AWS security team, threat modeling, and completion of a risk assessment. Static code analysis tools are run as a part of the standard build process, and all deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Security risk assessment reviews begin during the design phase, and the engagement lasts through launch to ongoing operations.

• A-4.4.1 Change management—Routine, emergency, and configuration changes to existing AWS infrastructure are authorized, logged, tested, approved, and documented in accordance with industry norms for similar systems. Updates to AWS’s infrastructure are done to minimize any impact on the customer and their use of the services. AWS will communicate with customers, either using email, or through the AWS Service Health Dashboard (http://status.aws.amazon.com/) when service use is likely to be adversely affected.

• A-4.4.1 Infrastructure—Amazon’s corporate applications team develops and manages software to automate IT processes for UNIX/Linux hosts in the areas of third-party software delivery, internally developed software, and configuration management. The infrastructure team maintains and operates a UNIX/Linux configuration management framework to address hardware scalability, availability, auditing, and security management. By centrally managing hosts through the use of automated processes that manage change, Amazon is able to achieve its goals of high availability, repeatability, scalability, security, and disaster recovery. Systems and network engineers
monitor the status of these automated tools on a continuous basis, reviewing reports to respond to hosts that fail to obtain or update their configuration and software. Internally developed configuration management software is installed when new hardware is provisioned. These tools are run on all UNIX hosts to validate that they are configured and that software is installed in compliance with standards determined by the role assigned to the host. This configuration management software also helps to regularly update packages that are already installed on the host. Only approved personnel enabled through the permissions service may log in to the central configuration management servers.

**VMware**

- vCenter Configuration Manager tighted to vCenter
  - Change discovery and correlation
  - Change in VMs
  - Change in ESXi hosts
  - Compare configurations to third parties’ specifications for security reasons
  - Used for regulatory compliance
  - Used to harden the environment
- vCenter Operations Manager
  - Monitors trends – works with vCenter

**SEC-5.1: Security incidents identification and troubleshooting failure**

**Amazon EC2**

- Cloudtrail + SIEM (e.g., Boundary)