Requirements and Use cases system for Virtualized Network Functions platforms

Article · October 2014

26 authors, including:

Antonio Pietrabissa
Sapienza University of Rome
94 PUBLICATIONS **398** CITATIONS
SEE PROFILE

Jordi Ferrer Riera
i2CAT Internet and Digital Innovation in Cata...
46 PUBLICATIONS **158** CITATIONS
SEE PROFILE

Dora Christofi
Newcastle University
6 PUBLICATIONS **10** CITATIONS
SEE PROFILE

E. Pallis
Technological Educational Institute of Crete
131 PUBLICATIONS **593** CITATIONS
SEE PROFILE

Telecommunications System & Management

Research Article Open Access

Requirements and Use cases system for Virtualized Network Functions platforms

Editors: Antonio Cimmino[1] , Jorge Carapinha [2]

Contributors: Aurora Ramos, Felicia Lobillo (ATOS) [3], Thomas Pliakas (CLDST)[3], Antonio Pietrabissa, Donato Macone, Francesco Delli Priscoli, Martina Panfili (CRAT)[3], Yacine Rebahi (Fraunhofer)[3], Jordi Ferrer Riera (i2CAT)[3], Michael McGrath (INTEL)[3], Paolo Comi (Italtel)[3], Panagiotis Papadimitriou (LUH)[3], Eleni Trouva, George Xilouris (NCSRD)[3], António Gamelas (PTInS)[3], Dora Christofi, Georgios Dimosthenous (PTL)[3], Georgios Gardikis (SPH)[3], Athina Bourdena, Evangelos Markakis, Evangelos Pallis (TEIC)[3], Mamadou Sidibe (VIO)[3]

[1] ICCLAB Zurich University of Applied Sciences, Switzerland

[2] Portugal Telecom Inovação, Portugal

[3] T-NOVA Project [1] - WP2 Team

Abstract

Network Functions Virtualization (NFV) is an emerging technology approach, which refers to the migration of certain network functionalities, traditionally performed by hardware elements, to virtualized IT infrastructures, where they are deployed as software components. NFV leverages commodity servers and storage, including cloud platforms, to enable rapid deployment, reconfiguration and elastic scaling of network functionalities. This introduces a new framework, enabling providers not only to deploy Virtualized Network Functions (VNFs) for their own needs, but also to offer them as value added services to their customers. Virtual network appliances can be provided on-demand as-a-Service, eliminating the need to acquire, install and maintain specialized hardware like gateways, proxies, firewalls, transcoders and analyzers at customers' premises. The main goals of paper are the definition of basic use cases and the identification of the key system requirements for the design and deployment of "Network Functions as-a-Service (NFaaS) over virtualized infrastructures".

Keywords: NFV, ETSI, Cloud Computing, Service Provider, customers, performance, scaling, requirements, use cases, business roles.

I. INTRODUCTION

The transition from system centric architectures to virtualized architectures in the telecommunications domain requires a re-evaluation of the current business ecosystem and associated use cases. Virtualized architectures, based on cloud infrastructures, allow operators to deploy virtualized network functions for both their own needs and also to offer them to their customers, as value-added services. Virtual network appliances (gateways, proxies, firewalls, transcoders, analyzers etc.) can provide on-demand "as-a-Service" reducing the need to acquire, install and maintain specialized hardware at customer premises. Leveraging the NFaaS (Network Function as a Service) concept will facilitate diversification actors in the NFV scene as well as attracting new market entrants. This change in market dynamics will also facilitate the development of new business models with the introduction of concepts such possible as an "NFV Marketplace". The "Marketplace" is built around the concept of network services and functions being offered by a variety of developers, which can be purchased by customers or traded to meet customer needs. An NFV Marketplace enables customers to browse and select services and virtual appliances that best match their needs. Additionally a Service Level Agreement (SLA) with the required levels of service can be selected together with a corresponding billing model. The T-NOVA FP7 research project [1] which started in January 2014 is focused on addressing the needs of an NFV Marketplace through a work program that encompasses the entire design lifecycle of representative NFV services. However, the project is collecting evidence as to the benefits for each actor in a marketplace oriented business model (Network Operators, Network vendors, software developers, start-ups and customers). While T-NOVA's research program is its initial start-up phase the use cases outlined in the paper presented some early initial findings and learnings.

The structure adopted this paper reflects the approach that has been adopted by the T-NOVA consortium in elucidating the stakeholder, roles and requirements. The keys steps in this process were as follows

- Business analysis to define stakeholders, business roles and business scenarios.
- Definition of application scenarios with a focus on the potential benefits of NFV and practical appliances.
- Analysis of representative VNF's to be integrated in the new ecosystem.

- Use case specification describing the interactions between external actors and the system, based on identified business scenarios.
- Requirements specification, based on the use cases defined in the previous step based on focus areas like: Management and Orchestration, Elasticity, Security, Resiliency, Service Continuity, Operations, Market / Commercial operability.

II. Overview

Network Functions Virtualization [2] is rapid gaining traction in the telecommunications domain. It is focused on virtualizing functions within operator networks and migrating these functions to software-based appliances, deployed on top of commodity IT infrastructure.

The migration of most of the in-network operations from hardware to software modules leads to various benefits including: efficient management of hardware resources, rapid introduction of new network functions to the market, easy upgrade and maintenance, exploitation of existing virtualization and cloud management technologies for the NFVs, significant CAPEX and OPEX reduction.

The automation and deployment of these functions in carrier grade environments is received increasing attention from the research and industrial communities. As previously outlined, the dynamic provisioning of VNF can be further augmented by an innovative “NFV Marketplace” where network services and functions created by communities of developers can be published on an open-source basis, acquired and instantiated on-demand. The “Network Function Store” is similar conceptually to the very successful OS-specific “App Stores” for smartphones and tablets. However in the case of VNF’s, a key difference is the focus on “back-end” services of the brokerage, instead of mobile applications. A preliminary high-level view of the main building blocks of such an NFV ecosystem is depicted in Figure 1 which also introduces a global view of the marketplace. A more exhaustive description of roles is included in the section III. Section V provides examples of the marketplace in “action” based on representative use cases.

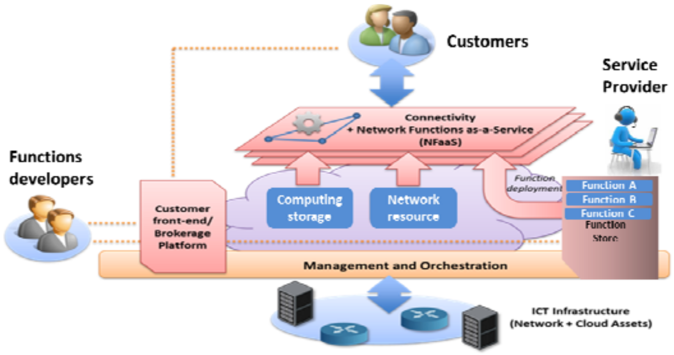

Figure 1 High-level visualization of the T-NOVA architecture

The T-NOVA system has the objective of implementing all the functionalities of a complete Network Function Virtualization Infrastructure (NFVI), as defined by the ETSI NFV working group [3] [8]. The involvement of diverse actors will be facilitated in the NFV framework enabling third party developers to implement NFs and publish them with their corresponding metadata.

III. BUSINESS ROLES AND BUSINESS MODELS

A stakeholder or actor can be defined as an individual, group of people, organization or other entity that has a direct or indirect stake in a system. These business entities may have more than one role. Role analysis is specifically focused on functionality and not on who in practice plays those functions, which is introduced at the end of this section.

A. *BUSINESS ROLES*

Several roles (Figure 2) are involved in NFV value chain and the authors propose the following definitions:

- End User (EU): The end consumer of the purchased service acquired from the Customer (C).
- Customer (C): Customer who purchases NFV services in B2B (Business To Business) scenario.
- Service Provider (SP): The SP provides a finished product to end customers. Services offered to end customers can be single network functions, or bundles containing a combination of functions from different Function Providers (FP).
- Function Provider (FP): The FP supplies virtual network appliances eliminating the need for the customer to acquire install and maintain specialized hardware. The FP can also be in the role of developer.
- Broker (B): The broker fetches offerings matching the customer requirements and, depending on the applicable trading-policies, carries out the necessary actions for the customer, the SP and the FP to agree on definite SLAs and prices to be applied.

- Cloud Infrastructure Provider (CIP): The CIP provides the cloud infrastructure where the NF will run on.
- Network Infrastructure Provider (NIP): The NIP provides the physical connection to the cloud infrastructure.
- Service Integrator (SI): The SI matches the suppliers providing the substrate for running the virtualized functions for the SP. The SI makes the match so that the service can finally be delivered.

Figure 2 shows the scenario where each actor has a single role. There are many real market cases where an organization will keep more than one business role.

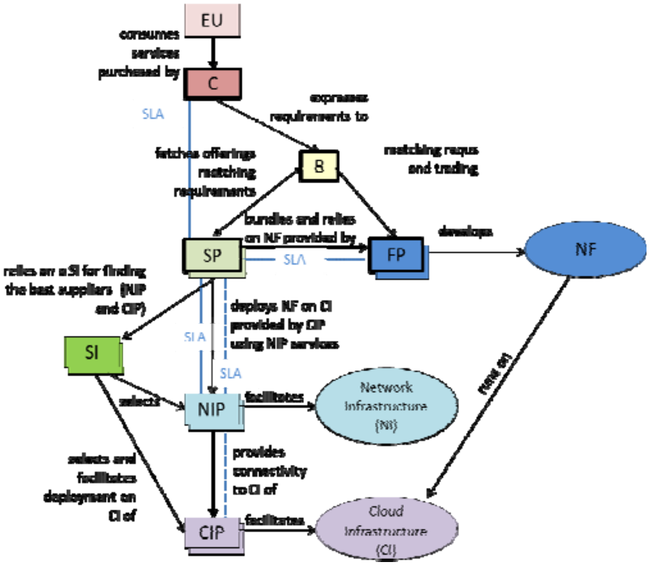
EU
consumes services purchased by
C
SLA
expresses requirements to
fetches offerings matching requirements
B
matching requs and trading
bundles and relies on NF provided by
SP
SLA
FP
develops
NF
relies on a SI for finding the best suppliers (NIP and CIP)
deploys NF on CI provided by CIP using NIP services
SLA
SLA
SI
selects
NIP
facilitates
Network Infrastructure (NI)
runs on
selects and facilitates deployment on CI of
provides connectivity to CI of
CIP
facilitates
Cloud Infrastructure (CI)

Figure 2 T-NOVA System Roles

In this figure we assume that the CIP has no direct relation with SP to negotiate the SLA, in the reality there may be two separate relationships with the SP. We also assume that the SLA requirements are published by the Customers, in their requests, and thus analyzed by the SP, NIP, and CIP chain in the bid proposal for negotiation.

B. BUSINESS MODEL and STAKEHOLDERS

There are a number of mandatory roles that will be played by different stakeholders, called basic stakeholders. The remaining stakeholders may or may not be included as appropriate. The key stakeholders in the NFV value chain are outlined in table 1.

Stakeholder name	Comment
Service Provider (SP)	Basic
Function Provider (FP)	Basic
Customer	Basic
Broker	Basic stakeholder if the business scenario has several SPs. Optional if there is only one SP. The SP can contract or not a third party to perform trading among FPs to purchase VNFs. If the broker is not contracted, the SP will perform itself the trading among different FPs.
Service Integrator	Optional (to be a function played by the SP)
Network Infrastructure Provider	Optional (to be a function played by the SP)
Cloud Infrastructure Provider	Optional (to be a function played by the SP)
End User	Optional (only in some specific scenarios)

Table -1- NFV Lifecycle Stakeholders

The most basic version of the business relation landscape encompasses only one SP and one FP; the SP can play the broker role trading its services, and the FP can trade their own NFs (unless the SP and FP prefer to contract a broker stakeholder to do it). The SP may also act in the role of the CIP and the NIP.

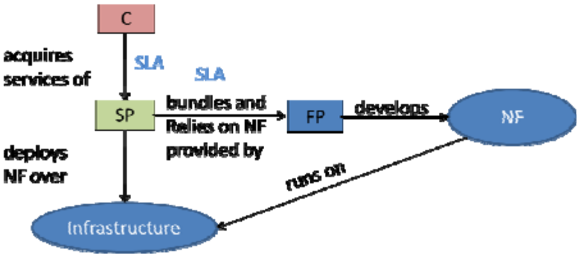

Figure 3 Simple business scenario

There is also a basic scenario where a network operator can provide NFs as Service over their own infrastructure (both cloud and network resources) as shown in Figure 3. Also, the role of the SI is most likely played by the SP.

There are a number of scenarios where several SPs have accessed to the NVF system to provide services with a broker role played by a third party entity (Figure 4). The broker offers the customer the best pricing options in the marketplace as a result of trading among different SPs. The broker is an intermediary player which selects the offerings and conditions that match the customer requirements considering the services provided by all the SPs.

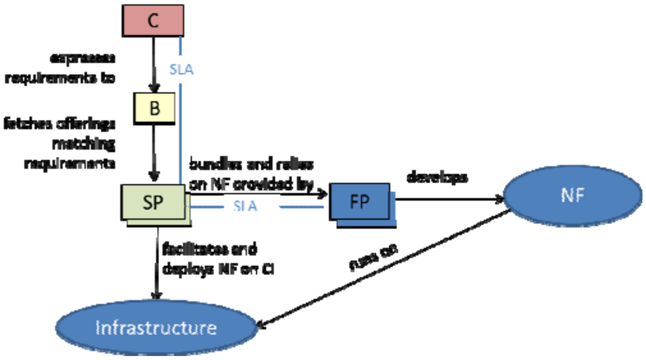
C
expresses requirements to
SLA
B
fetches offerings matching requirements
bundles and relies on NF provided by
SP
SLA
FP
develops
NF
facilitates and deploys NF on CI
runs on
Infrastructure

Figure 4 Broker between Customer and Service Providers

ISSN: 2167-0919 JTSM, an open access journal

In addition, other business scenarios can be identified for example: Broker stakeholder between Service Provider and Function Providers or Broker stakeholder with several SPs and several FPs. A detailed analysis can be found in [4].

IV. APPLICATION SCENARIOS

The first part of this section introduces two high-level scenarios, to illustrate implementations in two different environments – enterprise (A) and residential (B). The section then continues with a brief overview of the VNF architectures and examples for further development.

A. High Level Scenario- Enterprise version

A large organization that has offices spread geographically is planning to deploy a VPN that will interconnect all the branches with their corporate headquarters. Their intention is to have specific QoS guarantees for their cross-office traffic, coupled with high bandwidth Internet access. To decrease their operational costs they would like to deploy some of their security services running on leased infrastructure. Additionally, they have a requirement to provide a unified communication service for all their personnel, mobile or stationary. Some monitoring features are required by the IT department to control the infrastructure and to have access to granular data on the current traffic/services profile along with data leakage protection. The IT department administrator also requires a browser based interface for NFV service ordering and configuration (e.g. state-full firewall VNF, Session Border Controller (SBC) and a Deep Packet Inspection (DPI)). The ability to specify KPIs (Key Performance Indicators) related to the performance of the network infrastructure and those of the various VNFs via the interface is also specified.

The system will offer a list of possible solutions for the instantiation of the virtual architecture and the VNFs. The trading/bidding process among multiple actors is initiated with the mediation of a brokerage system.

B. High Level Scenario - Residential Version

The second use is case is focused on residential infotainment where, for example, a where a group of friends are interesting in playing a 3D online game together. Other occupants of the same house would be interested in consuming additional services. One person working at home may require audio/video conference capabilities to complete a business contract negotiation while another member of the household may require multimedia services in the form of a favorite education channel to be consumed via Smart TV in the living room or via a mobile device such as a tablet.

The NFV system offers a portal to select the appropriate virtualized Home Gateway that can fulfil the requirements of the three services to be used by each of the family members. An offer that attracts their attention is based on the service usage and post-payment. This offer also includes a virtualized DPI that could be used to segregate different traffic types and guarantee the quality of the audio/video conference connection with priority in the event of network saturation. The payment model can also be selected on a pay per use, inclusive of network security functions for the videoconference.

C. VNF architectures and examples

In the use case scenarios we have seen various interesting functions that could potentially be utilised. There are many others and ETSI [3] [5] provides a detailed path on how stakeholders can move towards virtualisation. In the next section we will illustrate some architectural elements required to realise the functionalities of the use cases.

Virtual Security Appliance

A Security Appliance (SA) is a device that is used to protect computer networks from unwanted traffic. It can deliver diverse security technologies including firewalling, Deep Packet Inspection, and Intrusion Detection. A Virtual Security Appliance (vSA) is a Security Appliance running in a virtual environment. The performance of these technologies is closely couple to that of the virtualized environment. Careful consideration therefore must be given the required performance level of the use case be implemented and the corresponding hosting virtualized infrastructural environment.

The vSA is offered to customers that require protection of their infrastructure. If the SA detects suspicious traffic, it will be dropped or redirected to another component for further investigation. The vSA can be deployed at the edges of the network, close to the customer premises or at other convenient locations within the virtual network slice that has been provisioned for this customer (see Figure 5).

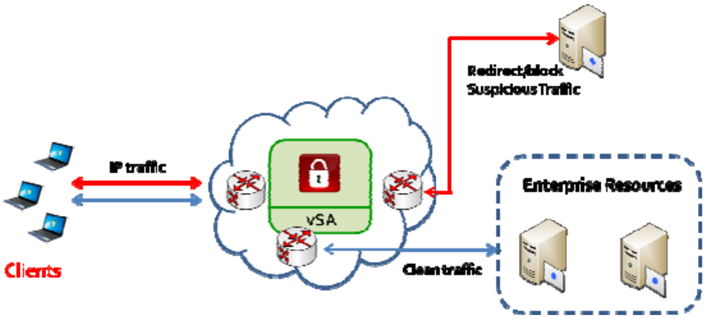

Figure 5 Virtual Security appliance

The vSA is able to detect potential dangerous or suspicious traffic and responding appropriately to either block it or redirect it to a traffic analysis/forensics virtual device for deeper attack pattern analysis and recognition.

Implications and requirements

Virtualization of the Security Appliance requires that the hypervisor which is the key enabling technology for supporting virtualization of the hosting compute resources is sufficiently performant. Packet forwarding performance (network challenge) between the physical network interface and the virtual network interface provided to the virtual machine should be optimized in order to support high traffic volume that needed to be analyzed. The scaling of the virtualized computing resources and the corresponding workloads pose challenges for the orchestration and virtualization layers.

Benefits
Beside overall benefit dealing with migration to virtualized function, for this appliance the security technology can be considered as on-demand plug-in (updatable and configurable) of a global security appliance. In traditional cases software packages or systems would need to be installed per each user network.

Virtualised Session Border Control

A Session Border Controller (SBC, figure 6) is a device used in multi-media telecommunication, providing network interconnection and security services between two IP networks whenever multi-media sessions are required between the two network. The SBC is usually deployed at the border of a service provider network or in a customer network.

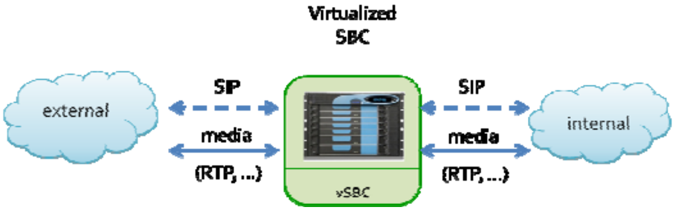

Figure 6 High level model of an SBC

The SBC incorporates the signaling procedures and the Border Gateway Function (BGF) for user data plane. Moreover, the SBC implements the signaling interworking and media adaptation (transcoding, trans-rating) functions for effective multimedia communication at the interconnection.

Implications and requirements
A possible use of a vSBC would be for companies that are spread across two or more sites located in different countries. In this use case, leveraging a VoIP solution that interconnects the two sites through the public Internet using a SBC at the edge of the each site’s local company network is of interest in helping to reduce telephone call costs.

Benefits
The same architecture can be used with an instance of a vSBC to provide a media transcoding service only for the duration of the video conferences. The vSBC is inserted into the path of the company's inter-site network connection on an as needed basis.
The benefit of T-NOVA is its ability to offer flexibility in the terms of purchasing and configuring virtualized network solutions in the most economical manner for customers, through a preferable billing modality.

Virtualized Deep Packet Inspector

Deep Packet Inspection is a technology that inspects IP packets at Layer 2 through Layer 7. This includes headers and data protocol structures as well as the actual payload of the message. It (Fig.7) is used to prevent attacks from viruses and worms at wire line speeds. The classified packets can be redirected, marked/tagged, blocked and reported to a reporting agent in the network.

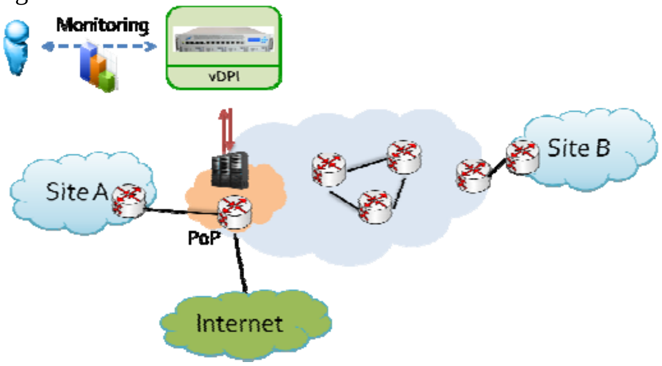

Figure 7 - vDPI

Both dedicated appliances and embedded Integrated Service Adapters (ISA) for IP security and packet analysis are included in this definition. Current market trends indicate that the DPI technology along with policy management frameworks will be deployed as an effective management and network enforcement technology to prioritize traffic, generate new sources of revenue and meet more stringent regulations on roaming.

Implications and requirements
DPI is a computational intensive activity. A virtualized DPI can elastically grow to meet its computational needs until a defined upper bound is reached. It is necessary to combine these goals with an intelligent memory and power consumption system, aimed at a network monitoring system, which will be able to obtain and process a large number of packets quickly, with no additional cost in terms of memory, or complexity.

Benefits
In the context of T-NOVA the DPI benefits can be summarized as follows::

- Increased flexibility in provisioning and speed of deployment of DPI capabilities within a network.
- Modularity and on-demand features/functionality during deployment.
- Separation of DPI gateway functions and the management of the DPI within the SDN framework.

Virtualized Home Gateway

Physical Home Gateways (HG) are now universally deployed in consumers’ house/enterprises. Their primary use is to connect a LAN to a WAN or the Internet. They also offer advanced network functionalities such as wireless access point, DHCP, NAT, QoS or Firewall. Internet Service Providers (ISP) tend to have a large portfolio of physical devices, depending on the hardware partnership contacts, mergers and acquisitions, device generations, type of Internet connection (xDSL, FTTx, etc.). This high level of fragmentation results in a variety of costs such as support hotlines, supply chain issues, inventory and slow deployment of new functionalities. Moreover, HG software is regularly updated, resulting in unexpected connection outages for customers.

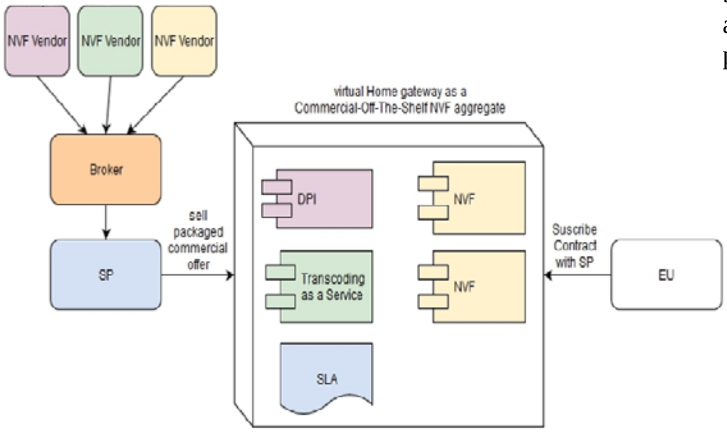
NVF Vendor
NVF Vendor
NVF Vendor
Broker
SP
sell packaged commercial offer
virtual Home gateway as a Commercial-Off-The-Shelf NVF aggregate
DPI
NVF
Transcoding as a Service
NVF
SLA
Suscribe Contract with SP
EU

Figure 8 vHome GW

Moreover, HG software is regularly updated, resulting in unexpected connection outages for customers. The virtual HG is illustrated in Figure 8. vHG is a virtual appliance offered as a VNF by T-NOVA.

Implications and requirements

The main challenge for the virtualization of a HG is transitioning gradually from a physical HG to a vHG and to scale the vHG to a very large numbers of instances. The signaling volume that needs to be supported in order to provision and manage vHG instances necessities careful consideration during design and implementation

Benefit

An ISP could use a cloud-based virtual HG (vHG) approach with the benefit of: scaling both technically (to a large number of vHGs, possibly in the order of millions) and economically, providing at least the same level of service experienced with current HGs, reducing fragmentation of deployment configurations, supporting rapid deployment of new functionalities/security updates.

V. USE CASES AND REQUIREMENTS

The goal of this section is to describe an initial set of requirements which will drive the definition of a suitable architecture for NFV's. This specification of requirements follows the business analysis and roles described in the previous sections. The scope is to specify a number of use cases, describing the interactions between external actors and the system, which are applicable to the business scenarios identified before. Secondly, to derive an initial set of requirements, addressing different associated domains.

A. *USE CASES*

Use cases describe the sequence of interactions that take place between the NFV system and the stakeholders involved (see section II), to achieve an outcome of value. Thus, each stakeholder is should have an association with at least one use case. As previously outlined, the use cases in this section have been specified based on the service lifecycle of VNF services and the associated business scenarios, as defined in the previous parts of the paper.

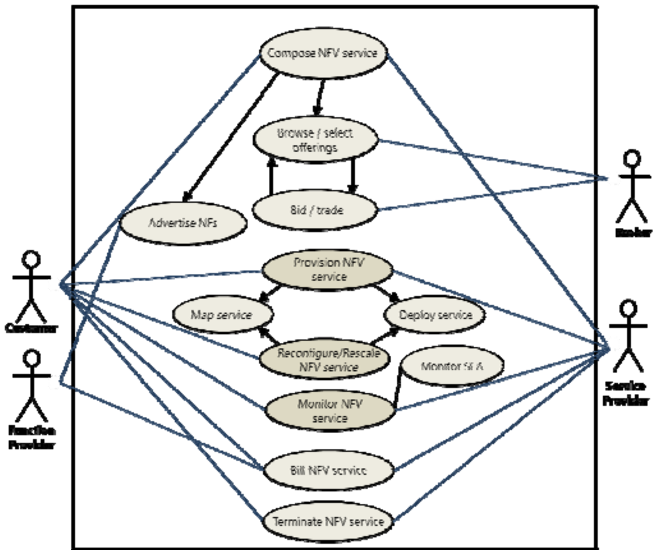

Figure 9 Overall Use case diagram

It is assumed that the business relationships between stakeholders have been established prior to the execution of the use cases, including the definition of the applicable service parameters and customer profiles. The UML [6] use case diagram, presented in Figure 9 , represents the roles, use cases (round grey blocks) and the relationships between stakeholders. Ultimately, it can also be seen as a representation of a VNF service lifecycle.

It is interesting to see how "typical features" of virtualized and cloud infrastructures are utilized as network function features or sub-use cases. The same features in system centric architectures would require scalability analysis and replication of physical machines or electronic boards.

The T-NOVA marketplace will play a fundamental role in the business of virtualized functions enabling the commercial activity and fluent interaction among all the different business stakeholders identified previously. It will be a trusted environment for communities of consumers, brokers and providers of technologies related to VNF. This environment will offer much functionality like certified portal, services storage platform, trading, contract management, SLA negotiation and billing.

Although there are many similarities with mobile app store we envisage that the complexity of NFV marketplace will be high due to the volume of actor roles anticipated, the diversity in their respective needs and that the virtualized functions are mainly back-end cloud appliance instead of end user mobile apps. The work on the architecture of T-NOVA marketplace is still progressing. In the composition of NFV, UC1 for example, the role of the marketplace will be the access to the available VNFs, brokerage tools to implement pricing mechanisms based on different SLA levels, and service composition interface. The latest can be used by customer or service providers to interact with the composition tools for complex NF appliances (interconnected VMs). In all other Use Cases Below we can identify a central role of the marketplace as infrastructure for NFV communities.

UC1 - Compose NFV services

This use case specifies the interactions that take place during the VNF service composition phase according ETSI NFV [5]. An example would be: The FP offers several smaller functions modules as part of a Security Appliance (i.e. Firewall, IPS, IDS). These basic VNFs can be composed in a single Security-oriented VNF, reducing the need for complex service chaining and Network Forwarding Graph calculations).

The Stakeholders involved are: SP, Broker, FP, (NIP).

There are sub-cases to compose the services like:

(i) Browse and select offerings

Defines how the customer selects the service among the offerings provided by the SP (service, SLA and pricing), and how the SLA agreement / contracts are established among the different involved parties. A contract is established between the Customer and Service Provider, and another between Service Provider and the Function Provider.

(ii) Advertise NFs and Bid & trade process.

This use cases are dedicated to the interactions required for a FP to publish and advertise a VNF. This use case also describes the procedure that is required to perform resource trading among the Stakeholders involved. There is an offline exchange of authorization information and certification for each FP, subject to bilateral discussions between the FP and the SP, acceptance of the Terms of Service etc.

UC2 - Provision NFV services

The Service Provider instantiates the appropriate infrastructure resources according to the customer request in order to fulfil the SLA.

Stakeholders involved: Customer, SP

The Customer has selected the service components and relevant parameters (UC1).

Related sub-case would be the:

(i) Map and deploy service

The VNFs are mapped into appropriate resources and then provisioned on the NFV infrastructure. The use case may be executed in two different manners – upon a new service request by the customer (UC2), or as a result of a service reconfiguration or rescaling (UC3).

UC3 - Reconfigure/Rescale NFV services

This UC is focused on the adaptation of the resources allocated to a specific service, optimizing resource usage, and/or modification of configuration parameters.

Stakeholders involved: SP, Customer

Related sub-cases with automations would be for scaling purposes to manage VMs / Storage due to (de)instantiation of new VNFs.

In particular:

(i) Scale-out/ scale-in VNF Service

- Scale-out of the NFV service results in additional VNF instances being added to an existing VNF instance.
- Scale-in removes VNF instances and their host VMs that are no longer required.

(ii) Scale-up/ scale-down VNF Service

- Scale-up results in the compute, network, and/or storage functionality allocated to a specific VNF instance being increased
- Scale-down operation results in the compute, network, and/or storage functionality allocated to a VNF service being decreased

(iii) Reconfigure VNF Service

- The configuration/parameters of the service are adjusted.

UC4 - Monitor NFV services

The resources consumed by a service and overall status are constantly monitored and measures are presented to SP and to the Customer. The established service is monitored in order to: Provide awareness to the SP and Customer about their service status, Provide awareness to the SP about infrastructure utilization, Check conformance to SLA, Facilitate billing, Detect / prevent faults and anomalies, Trigger reconfiguration / rescaling decisions (UC3).

Stakeholders involved: Customer, SP

Related sub-case would be for:

(i) Monitor SLA to define the procedures for evaluating the agreed SLA between the different parties and to take pertinent actions according to the results.

UC5 - Bill NFV services

This use case defines the billing procedure for a Customer, and the billing procedure for SP by the FP (and NIP/CIP) based on accounting and SLA fulfilment.

Stakeholders involved: Customer, SP, FP, (NIP, CIP)

The billing procedures will be associated with Customers and Service Providers.

UC6 - Terminate NFV services

This use case defines the procedures related to termination of a provisioned NFV service, either by Customer or SP and removal of a VNF from the catalogue of available and advertised services.

Stakeholders involved: Customer, SP, FP

B. REQUIREMENTS AND SYSTEM ARCHITECTURE

The identification of system-level requirements is driven by the use cases described in the previous section. The approaches utilized are in line with the IEEE guidelines for requirements specification [7]. By tracing requirements back to its originating use cases, it is possible to understand why every requirement is needed, which stakeholders are involved and which system components are affected. At this stage we will try to specify the functional requirements to describe the behavior that the system is expected to exhibit under specific conditions. With few exceptions, non-functional requirements, describing properties or characteristics to be exhibited, or constraints to be respected by the system, have been left to later stages of the project. The requirements specification deals with several thematic areas, namely: Management and Orchestration, Elasticity, Security, Resiliency, Service Continuity, Operations and Market / Commercial operability.

Deliverable D2.1 [4] includes a detailed specification of the T-NOVA [1] system requirements, which are considered to cover the full spectrum of functionalities required by the specified use cases. A total number of 61 requirements have been specified, covering the areas identified above.

The following list summarizes the main conclusions on requirements:

- NFV service request.

  Customers should be able to express NFV service requests, which will be subsequently submitted to the system. The specification shall be composed of a set of VNFs advertised by the SPs. Customer should browse the Function Store to select among available VNFs. NFV service request includes connectivity of VNFs and any bandwidth or delay requirements for the virtual links.

- NFV service mapping.

  The system should be able to map NFV service to the network and to the IT resource availability. This requires the mapping of virtual network topology to the substrate network, while satisfying any bandwidth and/or delay requirements, as well as the assignment of VNFs that comprise the service to substrate nodes that have the required computing and storage resources in order to satisfy each VNF functionality resource requirements and also the resources required for packet processing, forwarding and/or caching.

- NFV service deployment.

  Following the service mapping, the assigned computing, network and storage resources should be allocated for the deployment of the NFV service. In addition, the installation of packet forwarding entries is required to ensure that the customer’s traffic will traverse the NFVs in the exact order specified in the NFV service request.

- NFV service scaling.

  Existing NFV services should be scaled up or down, upon a customer’s request. In the case of up-scaling, this requires the discovery and allocation of new computing and network resources for the placement of additional VNFs and/or the allocation of more bandwidth in order to accommodate a larger volume of traffic. Conversely, NFV service down-scaling requires releasing allocated resources and possibly the reassignment/reconfiguration of the NFV service in order to achieve resource optimizations.

- Resource discovery.

  NFV service mapping raises the requirement for substrate network topology and resource discovery. Specifically, up-to-date information about the network topology, the bandwidth utilization as well as the utilization of the computing and storage resources across the network infrastructure is needed. The system should have detailed information about the specifications of the VNF hosts, such as the supported VNFs, the number of physical ports, virtualization technology, etc. However, the network infrastructure or connectivity can be provided transparently by the NIP without the need to discover the network topology.

- Resource isolation.

  Resource isolation is a significant requirement for any network services provided on top of shared infrastructures. As such, resources dedicated to collocated NFV services should be isolated from each other. Resource isolation can be achieved using CPU and traffic schedulers in hypervisors.

- Resource efficiency.

The computational requirements of VNFs can vary significantly, depending on the type of network function. Therefore, the consolidation of VNFs requires the knowledge of their requirements in order to allocate the required resources and achieve efficiency. This, in turn, raises the requirement for NFV workload profiling.

- Resource monitoring.

  Resource and traffic monitoring is essential in order to achieve resource efficiency and ensure that established SLAs are maintained. The system should periodically receive information about the bandwidth utilization as well as the computing and storage resources utilized by the instantiated VNFs. This information can be used to detect anomalies, billing, resources failures, or severe performance degradation. Such events shall trigger NFV service reconfigurations or reassignments.

- SLA monitoring.

  This is required in order to indicate the status of an SLA, the system should be able to compare the service metrics against the SLA requirements. Any violations in SLAs should be promptly reported in order to trigger the necessary actions (e.g., NFV service reassignment).

- Billing.

  NFV services will be offered to different types of customers, such as enterprise networks, service providers, and home network users. Therefore, billing should be tailored to different needs and to support diverse billing models, such as flat rate and pay-as-you-go billing.

- Secure communication and Broker authentication.

  NFV service brokerage requires the interaction of SPs with the Broker. To ensure secure communication between these two parties, the NFV system should support mechanisms for Broker authentication and authorization. The messages exchanged between the NFV Service Providers and the Broker should be encrypted, preventing traffic eavesdropping. However, authentication and authorization mechanism may be defined in any part of the on-line business communication between the actors of the model.

The T-NOVA project has already initiated the global architecture definition for the system. It will be organized into planes as shown in figure 10. It will include all the aspects identified by the uses cases and actor role models described in previous sections. This work is still on-going.

The Management and Orchestration planes (Figure 2) address two critical issues in Network Function Virtualization: automated deployment and configuration of NFs, and federated management and optimization of networking and IT resources for NF accommodation.

The Orchestrator is middleware that is able to deploy and monitor network services by jointly managing Wide-Area Network (WAN) network resources and in-network cloud (compute/storage) assets. It is the top level entity, which orchestrates network and IT assets for composing and provisioning of services.

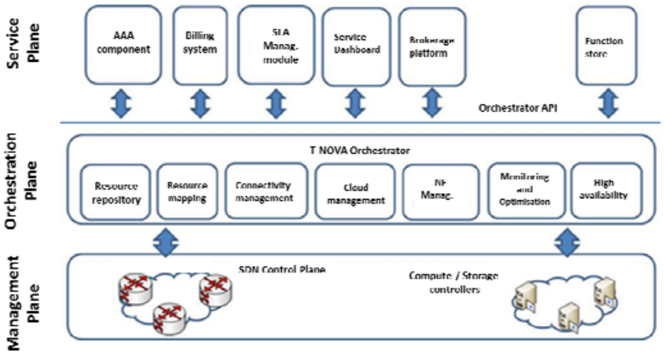

Figure 10 Orchestration platform, services, and interfaces

VI. Conclusions

The focus of this contribution has been the specification of use cases and requirements for the definition of basic stakeholders, as well as the description of a number of business-oriented application scenarios and associated value chain. These use cases and requirements illustrate how we envisage the deployment of VNF's in practice. One of the objectives of this paper is to establish common ground on which other architecture designs could consider appropriately. The output from T-NOVA presented followed a use case-driven approach, starting with the identification of the participating stakeholders and related business models, the basic use cases, and then evolving to the specification of applicable requirements

Acknowledgment: This work has been partially supported by the European Commission through the FP7 ICT Integrated Project T-NOVA [1] "Functions as-a-Service over Virtualized Infrastructures" INFSO-ICT- GA n.619520

VII. References

[1] FP7 ICT Integrated Project T-NOVA "Functions as-a-Service over Virtualized Infrastructures" INFSO-ICT- GA n.619520 – project portal: http://www.t-nova.eu/

[2] Network Functions Virtualization—Everything Old Is New Again - Frank Yue, Technical Marketing Manager, Service Provider f5.com

[3] ETSI NFV ISG. ETSI GS NFV 002 v1.1.1 Network Functions Virtualization (NFV); Architectural Framework. s.l. : ETSI, 2013.

[4] T-NOVA EU FP7 Project Deliverable 2.1 "System use cases and requirements".

[5] ETSI GS NFV 003 v1.1.1 Network Functions Virtualization (NFV); Terminology for Main Concepts in NFV. s.l. : ETSI, 2013.

[6] 7. Booch, G., Rumbaugh, J., and Jacobson, I. The UML Reference Manual. s.l. : Addison-Wesley, 1999.

[7] IEEE. IEEE Guide for Developing System Requirements Specifications. s.l. : ETSI, 1998. IEEE Std 1233.

[8] Technical white paper “Network functions virtualization”, HP - avaiable on line on http://www.hp.com/hpinfo/newsroom/press_kits/2014/MWC/White_Paper_NFV.pdf