Monitoring and Securing New Functions Deployed in a Virtualized Networking Environment

Mathieu Bertrand, Guillaume Doyen, Wissam Mallouli, Thomas Silverston, Olivier Bettan, François-Xavier Aguessy, Thibault Cholez, Abdelkader Lahmadi, Patrick Truong, Edgardo Montes de Oca

Monitoring and Securing New Functions Deployed in a Virtualized Networking Environment

Bertrand Mathieu, Guillaume Doyen, Wissam Mallouli, Thomas Silverston, Olivier Bettan, François-Xavier Aguessy, Thibault Cholez, Abdelkader Lahmadi, Patrick Truong, Edgardo Montes de Oca[1]

***Abstract*—Network operators are currently very cautious before deploying a new network equipment. This is done only if the new networking solution is fully monitored, secured and can provide rapid revenues (short Return of Investment). For example, the NDN (Named Data Networking) solution is admitted as promising but still uncertain, thus making network operators reluctant to deploy it. Having a flexible environment would allow network operators to initiate the deployment of new network solutions at low cost and low risk. The virtualization techniques, appeared a few years ago, can help to provide such a flexible networking architecture. However, with it, emerge monitoring and security issues which should be solved. In this paper, we present our secure virtualized networking environment to deploy new functions and protocol stacks in the network, with a specific focus on the NDN use-case as one of the potential Future Internet technology. As strong requirements for a network operator, we then focus on monitoring and security components, highlighting where and how they can be deployed and used. Finally, we introduce our preliminary evaluation, with a focus on security, before presenting the testbed, involving end-users consuming real contents, that we will set up for the assessment of our approach.**

I. INTRODUCTION

Network equipment is often designed for a specific usage, proprietary, and running on a specific hardware; making it very expensive to integrate (e.g. sizing, implementing, configuring and managing). Since the decision to deploy such a set of devices follows a logic based on RoI (Return of Investment), this drastically limits the ambition of network operators and the innovation in the network they operate. For example, network operators are reluctant to globally deploy a Named Data Networking (NDN) solution [1], a novel networking paradigm, proposing an Internet data plane that shifts from host-based network mechanisms to content-based ones, even if it could be considered as a solid alternative to the current IP stack.

[1] Bertrand Mathieu and Patrick Truong are with Orange Labs, Lannion, France.
Guillaume Doyen is with Charles Delaunay Institute, UMR CNRS 6281, France
Wissam Mallouli and Edgardo Montes de Oca are with Montimage, Paris, France.
Thomas Silverston, Thibault Cholez, Abdelkader Lahmadi are with Loria, Nancy, France
Olivier Bettan and François-Xavier Aguessy are with Thales Services, Palaiseau, France

A new trend in the networking area has emerged in the last few years: the virtualization of network functions. NFV (Network Virtualization Function), as defined by the European Telecommunications Standards Institute (ETSI) [2], is the key technology that leverages this concept. It involves implementing network functions in software that can run on a range of industry standard commodity server hardware. This initiative favors the progressive deployment of new network functions or protocols.

In this paper, we propose to push towards the adoption of these new standards by enabling a secure use of virtualized network equipment, which will ease the deployment of novel networking architectures. To illustrate our solution, we consider the case of NDN as an example of a new emerging stack. The co-existence of IP and NDN, and the progressive migration of traffic from one stack to the other in a virtualized environment are introduced, with a practical methodology consisting of setting up a real testbed. This testbed will allow end-users to access web sites (e.g., YouTube, Dailymotion, etc.) using the developed virtualized networking environment, hosting the NDN networking stack in parallel with IP. The testbed aims at proving the feasibility of the approach and also provides real traces, whose goal is to feed the monitoring and security aspects of our virtualized architecture. Indeed, monitoring and security are primary operator requirements that need to be assured before deploying new solutions. As such, we investigate how to design and deploy monitoring functions in such a virtualized environment. With the NDN specific use-case in mind, we study the type of information to monitor, the way to collect it and the way to analyze it. Leveraging a virtualized networking technology requires a full rethought of the way the security has to be designed, implemented and orchestrated. We focus here on the secure deployment, attack detection and mitigation, for protocols deployed in an NFV framework as network functions.

This paper is organized as follows: Section II presents our secured network architecture composed of virtualized network functions, with NDN use-case. Section III details our monitoring solution for such environment and its relationship with the security modules, so as to secure the system. Section IV introduces our preliminary evaluation as well as the testbed we will set up to assess our solutions. Section V presents the related work and Section VI concludes the paper.

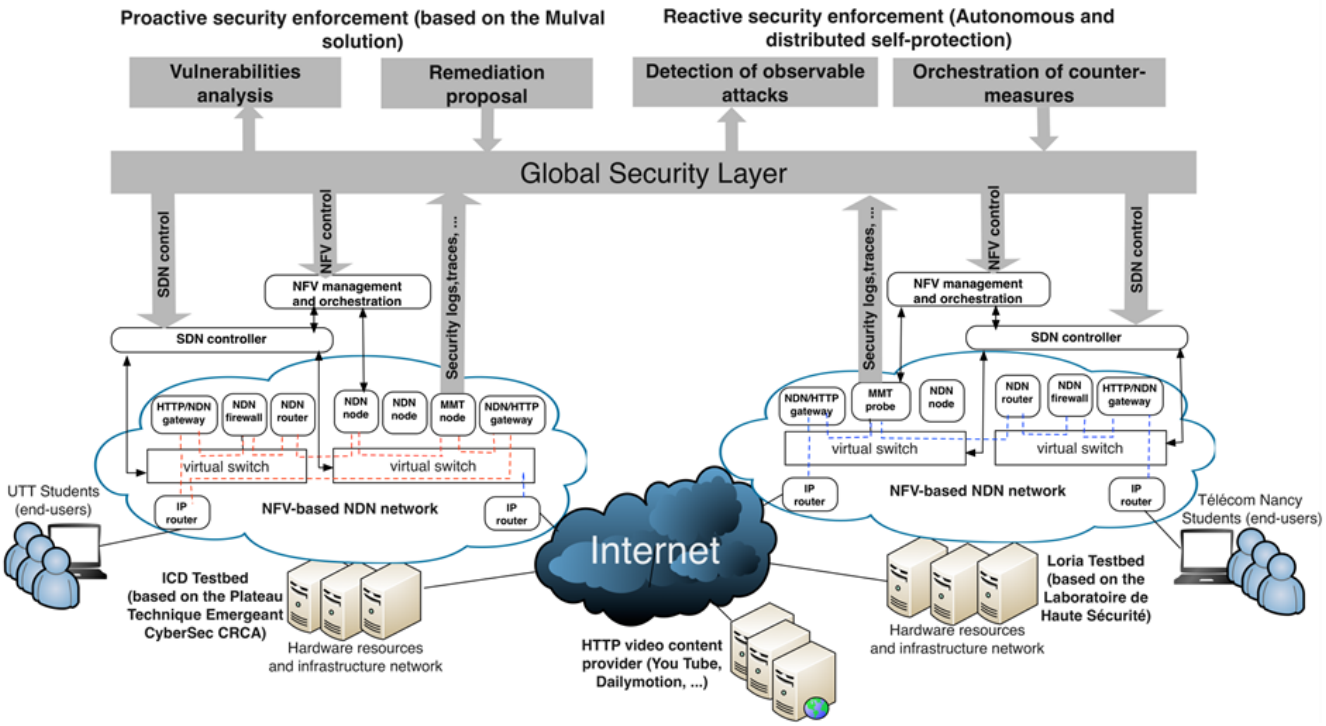

Figure 1. Overall virtualized secured functions-based network architecture

II. A SECURED ARCHITECTURE FOR VIRTUAL NETWORK FUNCTIONS: NDN USE-CASE

Leveraging the network virtualization to ease the deployment of new protocol stacks and functions appears as a strong mean to incite network operators to adopt these technologies. To reach this target, we propose in this paper an innovative secured virtualized network architecture (Figure 1). It is modular, as it is composed of a set of virtualized nodes that can host different protocol stacks (e.g. IP and NDN stacks in our use-case), network functions and validate their co-existence and correct behavior.

Named Data Networking (NDN) [1] is a novel networking paradigm, which proposes an Internet data plane that shifts from host-based network mechanisms to content-based ones. The match of requested content rather than the location of the endpoint that provides it thus dictates the establishment of a communication in NDN. Furthermore, NDN natively offers interesting features such as caching, multicasting, mobility, data integrity and authentication, etc.

However, even if very promising, network operators are reluctant to deploy such a novel data plane architecture, for the following reasons: (1) the huge initial investment costs it requires; and, (2) the security risk involved in introducing such a technical breakthrough and migrating from IP to the NDN paradigm.

In this context the architecture we propose, makes possible the deployment of such a NDN protocol stack in virtualized network nodes, thus avoiding any risk nor any additional hardware cost (the equipment is already deployed). Furthermore, it does not exclude the use of IP, since both can co-exist in the same physical node, each one having its own virtualized space. Thanks to a virtualized infrastructure, NDN can be deployed incrementally along with IP. More precisely, network operators can deploy NDN only in specific network locations (e.g. access networks, Point-of-Presence routers, mobile backhauling) and for specific services (e.g. social network applications, live video streaming, etc.) in selected nodes, which can help to improve the delivery of such services, with lower investment and risks.

For the NDN use-case, two deployment options are envisioned. First, the whole NDN stack is deployed as a single standalone component. This is the most straightforward way to deploy this NDN software. Second, the individual components forming the NDN node, such as the FIB (Forwarding Information Base), the PIT (Pending Interest Table) and the CS (Content Store) are deployed into the virtualized node as individual elements. The later allows composing the NDN nodes with components possibly coming from different providers (if one is more efficient for forwarding, while another provider offers a better caching mechanism for its CS). This second option allows more flexibility, and it was one of the main objectives at the beginning of the virtualization techniques, with more deployment options according to the NDN operators (low-cost operator, high quality operator, small-size operator dealing with few contents or on the contrary, large-size operator, etc.).

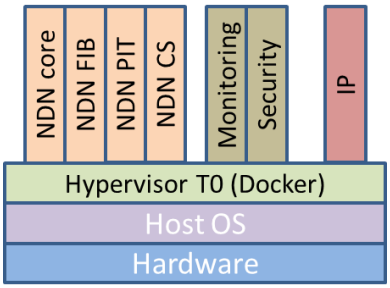

Figure 2. Virtualized node architecture

Together with the deployment of NDN, the monitoring and security aspects should be considered, since it is a necessary condition for its adoption. As compared to an IP stack, the case of NDN is highly challenging since, no solution exists for this architecture to (1) identify traffic, flows and link them to a particular activity; and, (2) probe, aggregate, correlate and disseminate monitored information in an efficient and scalable monitoring plane. The following section presents our defined monitoring and securing solution.

III. MONITORING AND SECURING FUNCTIONS IN VIRTUALIZED ENVIRONMENTS

A. Location of the monitoring component

Our solution introduces virtualized networks and functions that need to be monitored. To be able to ensure end-to-end QoS and security, a monitoring architecture needs to be defined and deployed in order to measure and analyze the network flows at different observation points that could include any component of the system, such as physical and virtual machines. Setting up several observation points will help to better diagnose the problems detected. With SDN (stands for Software Defined Network) [22], it is possible to create network monitoring applications that collect information and make decisions based on a network-wide holistic view. This enables centralized event correlation on the network controller, and allows new ways of mitigating network faults.

The monitoring probes can be deployed in different points of the system.

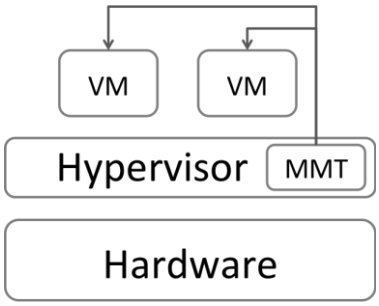

Figure 3. Network-based protection

Let's consider a single hardware entity that is controlled by a hypervisor that manages the virtual machines. A first approach consists of installing the monitoring solution, MMT (Montimage Monitoring Tool) [3] in the host system (hypervisor) that operates and administers the virtual machines (see Figure 3), in this way providing a global view of the whole system. This approach requires less processing power and memory to perform the monitoring operations, since the protection enforcement is located in a central point. In this way, network connections between the host and the virtual machines can be easily tracked allowing early detection of any security and performance issue. The main problem of this approach resides in the minimum visibility that the host machine has inside the virtual machines, not being able to access to key parameters such as the internal state, the intercommunication between virtual machines, or the memory content.

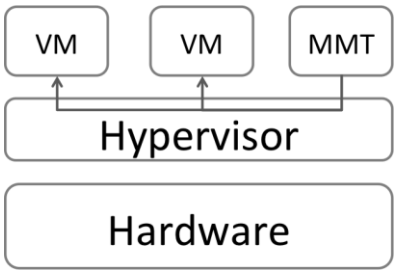

Figure 4. Virtual machine introspection

Monitoring probes can also be located in a single privileged virtual machine that is responsible for inspection and monitoring of the rest (see Figure 4). This approach is called Virtual Machine Introspection (VMI) [18] and offers good performance since the monitoring function is co-located on the same machine as the host it is monitoring and leverages a virtual machine monitor to isolate it from the monitored host. In this way, the activity of the host is analyzed by directly observing hard-ware state and inferring software state based on a priori knowledge of its structure. VMI allows the monitoring function to maintain high levels of visibility, evasion resistance (even if host is compromised), and attack resistance (isolation), and even enables the manipulation of the state of virtual machines. Unfortunately, VMI based monitoring software is highly dependent on the particular deployment and requires privileged access that cloud providers need to authorize.

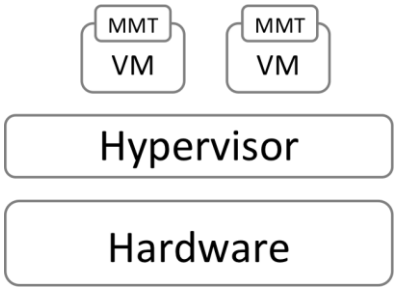

Figure 5. Host-based protection

The approach that offers the best security performance is the deployment of the monitoring tools in every virtual machine (see Figure 5). In this way robust protection can be achieved since the security software has a complete view of the

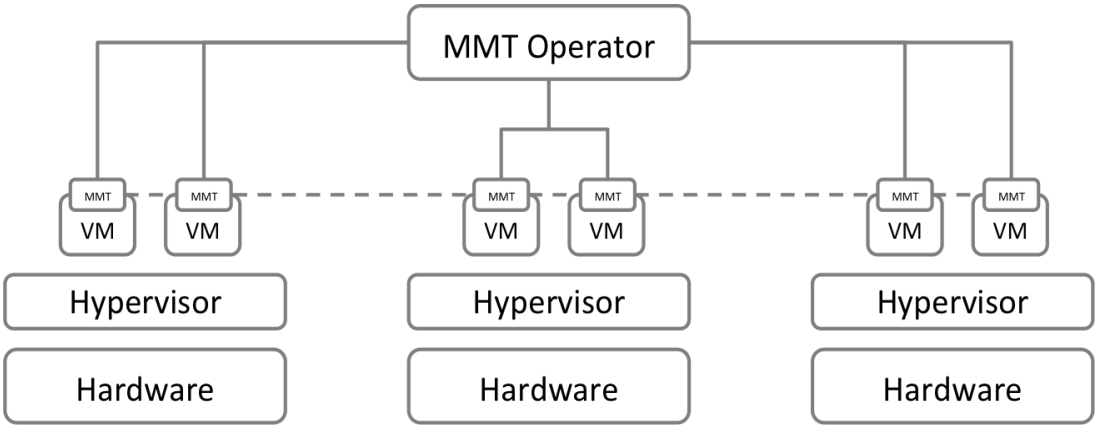

Figure 6. MMT architecture deployment for SDN

internal state of every virtual machine, as well as the interactions with the host or any other virtual machine.
This third solution offers the best performance in terms of security. Here, the processing power and memory required are distributed among the virtual machines. Furthermore, its deployment is simpler than other approaches since it can be included in the software image of the virtual machine, so it is automatically initiated when instantiating each virtual machine with no further configuration needed.

B. SDN-based Monitoring Architecture

Despite of the individual probes installed on each virtual machine, there is the need of a global monitoring coordinator that supervises the monitoring tasks of each probe installed on each virtual machine. For this, each probe must be able to directly interact with any other probe, as well as with the monitoring coordinator. Local decisions can be taken by the individual monitoring probes installed on each virtual machine, and the monitoring coordinator can perform coordination, orchestration and complex event detection.

Considering the different monitoring deployments presented in the previous section, herein, a whole architecture integrating monitoring probes and coordinator is presented.

C. Coordinating Security and Monitoring

Network security must be considered parallel to the traffic management and as an integral part of the network management. In SDN, due to its dynamic nature, this becomes even more critical since a security lapse of the centralized controller will adversely affect setting the traffic flow rules on other data path elements managed by the same controller. Similarly, network security policies and procedures must be updated in the case there are changes in the architecture or topology. The combination of proactive and reactive techniques synchronized with traffic management leads to a better security framework. Proactive operations help minimizing security lapses and service degradation; thus favoring a controllable usage of resources.

Figure 6 represents a possible deployment scenario for MMT in an SDN environment. As depicted, MMT probes capture performance and security meta-data from each virtual machine. These data are also to perform countermeasures to mitigate attacks and security risks (see section IV). MMT probes have the capacity of P2P communication, so they can share relevant information with the aim of increasing the efficiency of the mechanisms and, thus, ensure the correct operation of the whole system. To perform coordination and orchestration of the whole monitoring system, a central MMT Operator will receive information from the distributed MMT probes. The MMT Operator is also in charge of correlating events to create reports to inform network managers of the system activities, attacks avoided and countermeasures taken. Furthermore, it will be able to globally analyze the information provided by individual MMT probes with the ultimate objective of detecting complex situations that may compromise the system.
The architecture detailed in Figure 6 shows the deployment of MMT (MMT probes and MMT Operator) over a set of physical hardware platforms. The MMT Operator will be in charge of coordinating the diverse probes deployed in each virtual machine and provide a global view.

Reactive mechanisms have to be adequately located to avoid an impact on the performance even when providing a fine-grained control to access the resources. Synchronization in SDN is possible since the controller has a global view of all the network elements, flows and their security requirements and all the security policies. It is necessary to assure, for instance that: the traffic from data-path elements does not stop due to controller failure because of attacks through other data-path elements under the jurisdiction of the controller; and, the security (e.g., access control and firewalls) is configured and active as soon as the flows are directed to new routes (e.g., due to changes in topology).
The following two section present our solution for proactive and reactive security, for the NDN use-case.

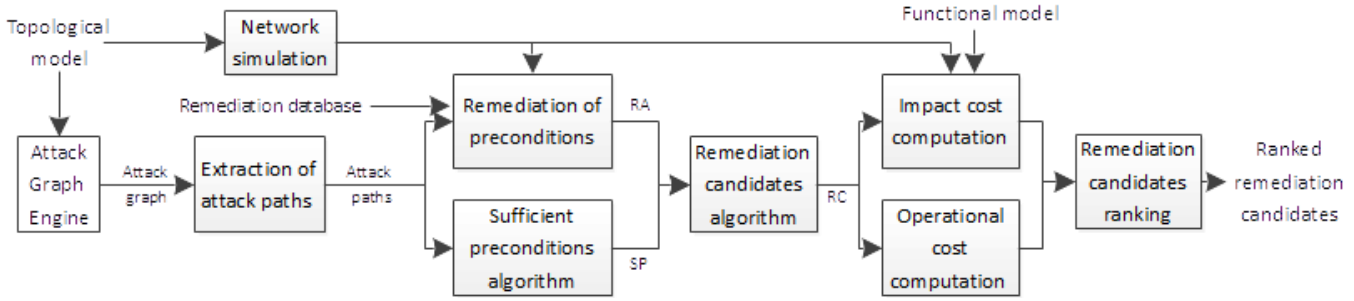

Figure 7. Vulnerabilities identification and remediation management

1) Proactive security mechanism

Virtualizing the deployment of NDN may lead to new threats that need to be identified and mitigated. The investigation of these threats and their impact is performed using a dedicated tool for risk analysis based on attack graphs, which is part of the proactive security mechanism in our architecture. This tool is benefiting from the Software Defined Networking (SDN) built-in capability to provide exhaustive topological information and application network requirements, needed as inputs to compute an efficient vulnerability analysis.

The attack graph engine, based on MulVAL [4], is configured to take into account vulnerabilities specific to virtualized NDN such as cache poisoning or polluting, or Interest Flooding attack, in addition to the IP-based vulnerabilities that are already provided. Interest Flooding attack consists, for an attacker, to generate malicious Interest packets for non-existing data in the Internet. As a consequence, nodes tables (and especially Pending Interest Tables) grow up to the time where legitimate Interests can no longer be stored, leading to the node resources exhaustion. The consequences of the exploitation of such vulnerabilities (for example the change or deletion of cache content, or the Deny of Service of components) are described in the rules used by the attack graph engine, to be able to see their effects on the global architecture. This allows seeing how attacks specific to NDN may spread to IP or vice versa.

This proactive security analysis is used to determine the most likely and impacting multi-steps attacks and propose different remediation strategies in order to increase the level of security of the infrastructure, following the process described in Figure 7 [5].

The first step of this process is to score the impact and probability of attack paths, extracted from the attack graph taking into account both IP and virtualized NDN vulnerabilities. Each path is then processed to compute remediation candidates allowing to mitigate or prevent it. Such remediations are for example the deployment of Virtualized Network Functions (VNF), such as virtualized monitoring probes, or the reconfiguration of the network by benefiting from the SDN. It is also possible to dynamically reconfigure the MMT probes, to have the attacks described in attack paths detected by them. The remediation candidates are then ranked using their operational and impact cost known thanks to the topological information and application network requirements collected through the SDN. In order to have an insight of the effects that a remediation candidate has on the whole information system, the chosen candidate is then applied on a simulated network, and a new security analysis is done and compared with the current one. This process of remediation proposal allows enhancing proactively the security of the network and configuring the MMT probes to detect the possible attacks.

2) Reactive security mechanism

Besides the potential vulnerabilities affecting virtualized NDN, models for the known attack scenarios (called attack patterns) are generated to be able to deduce for each attack path the characteristics of traffic, caches or forwarding tables, which are potential evidences that an attack is occurring or progressing. By identifying the main vulnerabilities and threats tackling our virtualized network, we define the metrics and indicators to be collected for dynamic security monitoring and assessment, thanks to dedicated virtual probes based on MMT. MMT can be deployed in several strategic network observation points to perform local analysis. Besides, locally collected data are shared among the different monitoring entities providing thus a distributed knowledge plane. The data is then processed by virtualized components running detection algorithms. The choice of the detection method (e.g. statistical model, learning methods, etc.) is adapted to the considered attack scenario characteristics and to the observed elements (e.g., traffic, routing tables, caches etc.).

By integrating MMT and MulVal, the detection of vulnerabilities becomes a dynamic process which constitutes an important added-value for the assurance of security in such virtualized environment. The scalability of the solution is guaranteed by limiting the attack path analysis to only the dynamically detected protocols and applications, and by providing MMT with the set of properties that are needed for a given situation

Besides, dedicated components allow identifying a set of countermeasures that can be engaged over the virtualized networking architecture to stop or mitigate an attack and allow the system to return to normal behavior (for example, by configuring a virtualized Firewall, or deploying new rules for virtual Intrusion Detection Systems). On the basis of this identification, for each of the detected attacks provided as an output of MMT, a set of automated or semi-automated control actions will be selected and orchestrated in a distributed manner. For this, a decentralized orchestration plane, relying on autonomous components is implemented over virtualized MMT. Cooperative algorithms potentially

relying on the peer-to-peer paradigm are considered to deal with the scalability and dynamics of the system. Also, the configuration changes made on controlled components are achieved through a SDN approach.

IV. Preliminary evaluation

A. Reduce CAPEX and OPEX costs

Network Functions Virtualization offers the potential for both enhancing service delivery and reducing overall operating expenses (OpEx) or capital expenses (CapEx). By enabling NFV with Software-Defined Networking (SDN), network operators can realize even greater benefits from this promising new use of cloud technology.

The first evaluations of the virtualization of the NDN concept target the estimation of this cost reduction that is evident since the proposed architecture allows to dynamically deploy network functions on existing network infrastructure with minimum CAPEX costs. The adoption of the SDN concept to orchestrate the different virtualized components (e.g. NDN nodes) makes their management more flexible (dynamic configuration, counter-measures, etc.) and as a consequence reduces the OPEX costs.

B. Risk-based monitoring solution

The proposed architecture also include proactive and reactive security enforcement based on risk analysis to detect potential security vulnerabilities using the MulVal tool (proactive) as well as a continuous monitoring to detect and mitigate intrusions and attacks using the MMT tool (reactive). This integration between these tools allows to increase the detection capabilities of MMT in NDN based networks as well as its performance. Indeed, the risk analysis provides valuable information to the monitoring tool that activates relevant security proprieties to be checked according to a deployment context and discards irrelevant ones. This improves security analysis efficiency and intrusion detection and prevention performance (estimated to +20%).

The demand for safe and secure networks, that are becoming more and more complex, is growing and requires integrated methodologies. It is expected that the evaluation results obtained, applied to NDN-based networks, will allow a reduction of monitoring costs and development time, improve reliability and lower time-to-market compared with competing products that are complex, expensive and difficult to deploy and adapt. These virtualized networks are often complex, involve multi-vendors and stakeholders, and need to evolve in a very dynamic way. All this introduces vulnerabilities related to the dynamically changing configurations and versions of the software and hardware products. These characteristics make it necessary to introduce self-configuration, self-maintenance, self-healing and self-protection capabilities.

The solution proposed will help detect vulnerabilities during operation, based on the identification of attack paths and the use of data from different sources (i.e., vulnerability scanners and database, application/system traces, network behaviour and pattern analysis, etc.). In this way the self-* capabilities can better be addressed in this kind of virtualized networks.

C. Testbed

Together with the proof of the feasibility, one of our main objectives is to evaluate our solution in a real configuration environment. For this, we will set up a testbed, interconnecting end-users, consuming contents from web sites (as depicted in Figure 1).

Our testbed is divided into two sites (campus of Troyes and campus of Nancy, both in France). At each site, virtualization technologies enable the hosting of network functions carrying NDN nodes or components. The testbed of both sites will be interconnected so that to reproduce the case of two autonomous systems operating independent NDN domains, thus leading to basic inter-domain routing. Students of the site campus will be involved to feed the testbed with real traffic they generate. Collected traces are of a long term so that they enable the design of realistic traffic models for NDN. From a technical perspective, HTTP flows will have to be redirected toward the testbed and a dedicated gateway will be implemented. Existing proposals and implementations in that area will be considered, such as [6].

As a first objective, through the use of the monitoring tool, the testbed will allow us to measure, collect and analyse the quality of service of NDN traffic for real video flows. Additionally, satisfying polls of end-users will enable the cross-analysis of QoS metrics against their perceived quality of experience. That way, it will allow us to provide a concrete feedback to network operators on the use of an emerging protocol stack such as NDN for a selected traffic over customizable network topologies.

The second objective of the testbed is related to the overall security of the architecture. Here, we propose to consider both the virtualization layer and NDN to deal with potential vulnerabilities of these combined technologies and also leverage the virtualization to control the NDN network functions. As a use-case, we consider the case of Interest Flooding attack that is one of the acknowledged security issue of NDN, as introduced in section II.A.

Through the implementation of this testbed coupled with real end-users, we expect to provide valuable feedback on the use of our approach.

V. Related Work

The concept of virtualization has already been studied in several research fields including operating system virtualization [7], application resource virtualization [7], Link and node virtualization [8] and Data center virtualization [10].

Now, network virtualization is largely discussed. Amongst the most promising network virtualization effort, the ETSI group NFV [2] proposes to implement network functions in software that can run on a range of industry standard commodity server hardware. We can distinguish 3 types of network virtualization: 1) type 2 where virtualization is applied for applications with a guest OS running over an

hypervisor on top of the host OS: VMware Fusion or VirtualBox are typical examples, 2) type 1, where virtualization is applied with an hypervisor running directly on the host's hardware to control the hardware and to manage guest OS. (it includes a mini OS): examples are VMware Vsphere, KVM ; and 3) type 0, where there is no hypervisor and virtualization is performed with containers with kernel level isolation. LXC (Linux Container), Docker, Rocket are examples of such low-level virtualization techniques. Solutions of type 0 offer a better performance in terms of packet and data processing [21]. The 2 others techniques are more generic but less adapted for our networking needs. Rocket takes into consideration security aspects, but not for the network functions as we propose.

The paper [12] presents an overlay testbed (named CUTEi), dedicated to ICN assessment, with LXC containers and CCN container. Compared to our work, the virtualized testbed CUTEi does not provide any tool for network or application monitoring, and security considerations are missing from the architecture design.

As another related work, we can also mention specific works such as [13], where the authors proposed ClickOS, a high performance NFV platform with small footprint virtual machines optimized for middlebox processing, but not addressing our objectives.

For monitoring, type 2 and 1 virtualization techniques offer some tools for managing virtual network functions, but limited to their lifecyle and do not manage the entire network neither address security issues we investigate. Monitoring systems for virtual machines have appeared over the last decade targeting specific technologies (Xen, VMWare, etc.) [14][15]. A recent IETF initiative [17] proposes building a generic management interface for Virtual Machines Monitoring. This takes the form of an SMI Management Information Base providing the necessary abstractions and objects of interest for monitoring hypervisor based virtual machines.

Regarding virtual machine security, work has been done building on introspection capabilities to identify security incidents [18]. Approaches like CloudSec [19] follow this path by offering in depth memory inspection of the monitored virtual machine. Other systems, like Revirt [20], operate below the operating system for doing both the logging and log-based intrusion detection on hypervisor-built logs.

To conclude, if all the related work presented above aims at addressing the individual challenges a complete NDN over NFV infrastructure has to deal with, none of these efforts address them as a whole while bringing efficient and secured global infrastructures is a key aspect to enable their adoption by involved stake-holders. As such, the Doctor takes part of that effort.

VI. CONCLUSIONS & FUTURE WORK

In this article, we described an architecture using Network Functions Virtualization (NFV) that makes possible the deployment and securing of new functions and protocols in virtualized environments. This architecture is modular and composed of a set of virtualized nodes hosting different protocol stacks. It allows, firstly, proactive security through an attack graph approach for risk analysis and, secondly, responsiveness thanks to the monitoring tool. We preconized base implementations to allow a gradual migration from IP to NDN while enabling the co-existence of both technologies. We finally introduced the testbed that will be deployed on real life use cases, for end-users, to assess and take full advantage of this novel architecture's deployment costs and risk reduction benefits. NFV having been identified as a main programmable network technology to be leveraged in future 5G networks, this work will have to stay aligned with the coming 5G challenges, especially: flexibility, privacy by design, QoS and Quality of Experience for end-user, location and context information, manageability and multi-tenancy to provide service solutions across different infrastructure ownerships, with the different co-existing networks.

ACKNOWLEDGEMENT

This work is partially funded by the French National Research Agency (ANR), DOCTOR project, <ANR-14-CE28-0001>, started in 01/12/2014 and supported by the French Systematic cluster.

REFERENCES

[1] V. Jacobson, D.K. Smetters, J.D. Thornton, M.F. Plass, N.H. Briggs, R.L. Braynard, "Networking Named Content", ACM CoNEXT 2009

[2] ETSI Whitepaper "Network Functions Virtualisation - An Introduction, Benefits, Enablers, Challenges & Call for Action", October 2012

[3] Wissam Mallouli, Bachar Wehbi, Edgardo Montes de Oca, Michel Bourdelles, *Online Network Traffic Security Inspection Using MMT Tool*. In the 9th workshop on system testing and validation (STV). Paris, France, October 2012.

[4] Ou, X., Govindavajhala, S., Appel, A.W.: Mulval: A logic-based network security analyzer. In: Proceedings of the 14th conference on USENIX Security Symposium, Volume 14., p.8-8, July 31-August 05, 2005, Baltimore, MD

[5] Aguessy, F.X., Gaspard, L., Bettan, O. & Conan V. Remediation Logical Attack Paths Using Infromation System Simulated Topologies, To be published in *C&ESAR 2014.*

[6] Sen Wang, Jun Bi, Jianping Wu, Xu Yang, and Lingyuan Fan. On adapting HTTP protocol to content centric networking. In *Proceedings of the 7th International Conference on Future Internet Technologies* (CFI '12). pp1-6. ACM, 2012.

[7] Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield. Xen and the art of virtualization. In Proceedings of the nineteenth ACM symposium on Operating Systems Principles (SOSP19), pages 164-177. ACM Press, 2003.

[8] Fox, Armando, and R. Griffith. "Above the clouds: A Berkeley view of cloud computing." Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Tech. Rep. UCB/EECS 28 (2009)

[9] André Vitor de Almeida Palhares, Marcelo Anderson Santos, Patricia Takako Endo, Jonatas Vitalino, Moisés Rodrigues, Glauco Estacio Gonçalves, Djamel Sadok, Azimeh Sefidcon, Fetahi Wuhib: Joint Allocation of Nodes and Links with Load Balancing in Network Virtualization. AINA 2014.

[10] Martin Valdez-Vivas, Nicholas Bambos, John G. Apostolopoulos: Dynamic resource management in virtualized data centers with bursty traffic. In the proceedings of ICC conference, pages 4287-4293. 2014.

[11] Daniel Turull, Markus Hidell, Peter Sjödin: Performance evaluation of openflow controllers for network virtualization. HPSR 2014:50-56.

[12] Asaeda Hitoshi, Li Ruidong and Choi Nakjung. Container-Based Unified Testbed for Information-Centric Networking, IEEE Network Magazine, Issue 6, Nov.-Dec. 2014.

[13] João Martins, Mohamed Ahmed, Costin Raiciu, Vladimir Andrei Olteanu, Michio Honda, Roberto Bifulco, Felipe Huici: ClickOS and the Art of Network Function Virtualization. NSDI 2014:459-473
[14] Payne, B.D., de Carbone, M.D.P., Wenke Lee, "Secure and Flexible Monitoring of Virtual Machines », ACSAC 2007.
[15] Menon, JR Santos, Y. Turner, G. Janakiraman, W. Zwaenepoel, Diagnosing performance overheads in the xen virtual machine environment, VEE '05 Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments.
[16] A. Kivity, Y. Kamay, D. Laor, U. Lublin, & A. Liguori, KVM: the Linux Virtual Machine Monitor, Proc Linux Symposium 2007.
[17] https://datatracker.ietf.org/doc/draft-ietf-opsawg-vmm-mib/
[18] T Garfinkel, M Rosenblum - A Virtual Machine Introspection Based Architecture for Intrusion Detection., Proc. NDSS, 2003
[19] Ibrahim, A.S. ; Hamlyn-Harris, J. ; Grundy, John ; Almorsy, M. CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model , 5th International Conference on Network and System Security (NSS), 2011
[20] GW Dunlap, ST King, S Cinar, MA Basrai , P. M. Chen , ReVirt: enabling intrusion analysis through virtual-machine logging and replay, Proc. ACM SIGOPS Operating Systems Review - OSDI '02.
[21] Wes Felter Alexandre Ferreira Ram Rajamony Juan Rubio, "An Updated Performance Comparison of Virtual Machines and Linux Containers", IBM Technical Paper RC25482, July 2014
[22] "Software-Defined Networking: The New Norm for Networks". White paper. Open Networking Foundation. April 13, 2012. Retrieved April 13, 2015.