Towards automatic deployment of virtual firewalls to support secure mMTC in 5G networks

Salva-Garcia, Pablo; Chirivella-Perez, Enrique; Bernal Bernabe, Jorge; Alcaraz-Calero, Jose M.; Wang, Qi

Published in:
IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)

DOI:
10.1109/INFCOMW.2019.8845183

Published: 23/09/2019

Salva-Garcia, P., Chirivella-Perez, E., Bernal Bernabe, J., Alcaraz-Calero, J. M., & Wang, Q. (2019). Towards automatic deployment of virtual firewalls to support secure mMTC in 5G networks. In IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 385-390). IEEE. https://doi.org/10.1109/INFCOMW.2019.8845183

Towards Automatic Deployment of Virtual Firewalls to Support Secure mMTC in 5G Networks

Pablo Salva-Garcia*, Enrique Chirevella-Perez*, Jorge Bernal Bernabe†, Jose M. Alcaraz-Calero* and Qi Wang*

*School of Computing, Engineering and Physical Sciences
University of the West of Scotland

†Department of Communications and Information Engineering, University of Murcia

***Abstract*—Internet of Things (IoT) has emerged as the main enabler to deal with challenging use cases that require massive Machine-Type Communications (mMTC), and mMTC has been recognized as one of three use case types for the Fifth Generation (5G) and beyond networks. In IoT networks, it is prohibitive to rely on just one firewall where hundreds of thousands of rules need to be installed in order to provide security countermeasures to each of the IoT devices. To fill this gap, this paper proposes an automatic deployment of virtual firewalls by leveraging Network Function Virtualisation (NFV) Management and Orchestration (MANO) to protect NB-IoT mMTC communications. The main idea underneath is to use NFV to deal with efficient rule distribution across VNFs-based firewalls to achieve scalability in the number of managed IoT devices. Empirical results have validated the design and implementation of the proposed scheme and demonstrating its advantageous performance and scalability. In particular, the deployment time for this VNF-based firewall service is highlighted to meet the requirement of a 5G Key Performance Indicator (KPI).**

Keywords–5G; NB-IoT; Security; Firewall; Automatic Deployment; VNF; MANO; NFV.

I. Introduction

The European 5G Public Private Partnership (5G PPP) [1] has defined ambitious Key Performance Indicators (KPIs) to be fulfilled in 5G networks. One of these KPIs is to achieve 1 million devices per square kilometer [2]. This KPI is associated to massive Machine-Type Communications (mMTC), one of the three use cases defined by ITU [1] regarding the novel capabilities that 5G networks should support. This high-density scenario is traditionally associated to cheap insecure IoT sensors and actuators, which cannot enforce proper security mechanisms. To enable secure mMTC in 5G networks, the network infrastructure needs to be ready to deal with diverse kinds of cyber-attacks.

To dynamically mitigate those cyber-attacks in a 5G-enabled IoT network, both the Edge and the Core of the 5G network need to filter, mirror, divert and differentiate IoT packets. Nonetheless, dealing with those attacks requires deploying a large number of firewall rules on each of these radio access points in order to deal with the control and security of the devices. Using hardware-based approaches for this large number of rules will impose a significant increase in the costs of the network elements mainly due to the memory requirements associated. In contrast, using software-based and Virtual Network Functions (VNFs) approaches will reduce costs but would impose challenges to deal with the scalability of the rules.

[1]https://www.itu.int/md/R15-SG05-C-0040/en

Our previous paper [3] has performed an empirical evaluation to determine how many firewall rules can be deployed inside a VNF virtual firewall to deal with NB-IoT traffic crossing the 5G network without decreasing the Quality of Service (QoS) of the transmission. The increasing number of filtering rules attached in each VNF firewall downgrades its performance since more computational processing is needed to check all the rules for the traffic in this software-based solution. Therefore, a balance in terms of capacity and performance has been determined.

This paper further explores a distributed VNF firewall architecture, where the system can either insert a new firewall rule inside an existing VNF firewall or deploy a new VNF firewall to provide more computational resources to handle scalability. To allow a cognitive network management system to make efficient decisions on actions, a deep understanding of the problem is needed. Whilst the previous paper focused on firewall rule configuration times and optimal number for maximum rules per VNF, this paper investigates VNF deployment times to perform the automatic deployment of a new VNF Firewall and configuration times of the VNF. The main aim is to provide an architecture that is able to deal with the high-density number of devices imposed in mMTC scenarios by making an efficient distribution of firewall rules among different VNFs. The design has been empirically validated in a realistic 5G multi-tenant infrastructure.

This paper is organized as follows. Section II reviews existing service deployment orchestration techniques and IoT security systems. Section III outlines the management framework. Section IV describes the virtualized 5G infrastructure deployed for a realistic NB-IoT testbed. Deployment of new VNFs with the proposed virtual IoT firewall as a service is presented in Section V. Section VI reports the experimental results in terms of efficiency, suitability and scalability. Finally, conclusions and future work are included in Section VII.

II. Related Work

5G-PPP has highlighted autonomous and cognitive network management as a key enabler in 5G networks for handling complex networking scenarios, especially when manual management is prohibitive such as in mMTC [4].

A. 5G Service Deployment Orchestration

Autonomous and cognitive network management requires automated orchestration in interacting with different Application Programming Interfaces (APIs) that control, manage and configure resources and services. Following the Mobile

Edge Computing (MEC) [5] architecture, an orchestrator to control a large number of distributed machines requires capabilities in operating system provisioning, NFV provisioning, resource life-cycle control, NFV life-cycle control, multi-tenancy support, multi-zone support, service location awareness, workflow dependencies resolution and parallel deployment optimization, among other features.

OpenMano [6] delivers an open source management and orchestration (MANO) stack aligned with ETSI NFV Information Models. It covers resource and service life-cycle management. OpenBaton [7] is an extensible and customizable framework capable of orchestrating network services across heterogeneous NFV Infrastructures. It uses OpenStack to control the underline infrastructure. OpenMANO and OpenBaton cover mainly NFV life-cycle management, resource management, multi-tenancy support, and multi-zone support. Chirivella et al. [8] provides an inclusive solution for the complete life cycle of 5G service deployment over multi-tenant 5G MEC infrastructures, based on Juju, MaaS and OpenStack. Our research work presented in this paper is based on this orchestration software, which has been extended to perform the automatic deployment of the architecture proposed. The virtual firewall is wrapped to be manageable by the orchestrator to allow the automatic deployment of VNF firewalls.

B. *Existing NB-IoT Attack Mitigation Systems*

Parakovic et al. [9] describe how the volume of attacks has increased by 651% in the last two years, mainly due to the increasing number of IoT devices connected. The Mirai attack in 2016 has motivated the community to better research how to defence against DDoS attacks (e.g., [10]) and new autonomic schemes for thread mitigation are consequently being defined (e.g., [11]). Despite the considerable number of related studies in the area of IoT security, there is still no solution to protect NB-IoT devices connected to the 5G infrastructure, where the new infrastructure entails novel mechanisms able to deal with nested traffic encapsulation produced, e.g., by multi-tenancy and mobility support. In [12], Hsieh et al. propose Virtual MEC (vMEC) to increase IoT applications' Quality of Service (QoS). Miettinen et al. [13] present Sentinel, a system capable of automatically identifying types of devices being connected to an IoT network and enabling enforcement of rules for constraining the vulnerable communications. Meng [14] proposes an Intrusion Detection System (IDS) that can be automatically deployed in the server to perform trust computation based on traffic features. In [15] a multi-level DDoS mitigation framework (MLDMF) for Industrial IoT (IIoT) is proposed, which includes the cloud computing, fog computing, edge computing and Software Defined Networking (SDN) for improving access security and efficient management of IIoT. Saraim et al. [16] introduce NETRA, a Docker-based architecture for virtualizing network functions to provide IoT security by deploying security functions at the network edge.

Moreover, a comparative study of different IoT malicious traffic mitigation systems has been conducted in [3]. The conclusion is that existing work is based merely on either detection or mitigation of such traffic. Little work has considered a complete detection and mitigation control loop for 5G IoT networks. Furthermore, as far as we know, there is barely any existing deployment and configuration strategies integrated as part of the actuation in a cognitive 5G IoT management framework. These gaps have motivated this research work.

III. Overview of 5G IoT Management Framework

NB-IoT deployment in 5G networks imposes challenging management requirements, such as multi-tenancy (differentiation of traffic from different network operators, carriers or verticals sharing the same physical infrastructure), scalability (support of a massive number of IoT devices), and dynamic network management of the traffic according to security policies and the current context obtained from real-time monitoring. These requirements demand novel security management frameworks that can rely on software defined network (SDN) management and Network Function Virtualization (NFV) technologies for handling the dynamic and scalability, thereby deploying or decommissioning, on-demand, virtual network security functions such as virtual firewalls (vFirewalls).

Figure 1 shows the general architecture of the security management framework employed in this paper and was presented in our previous work [3]. The architecture is split into three main planes. The Admin Plane includes the GUI and tools for security management, including security policy tools. The Security Orchestration Plane endows the framework with the proper cyber-situational awareness, intelligence and orchestration tools to make security and network decisions dynamically according to the circumstances. To this aim, it interacts with the Monitoring module to gather network and system information from physical and virtual agents deployed either in the edge or in the core of the network. Moreover, in this plane, the Reaction/Cognitive module embraces a decision support system that provides the required intelligence to generate the proper reaction plan and countermeasures that need to be deployed in the system to address misbehaviour in the system, e.g., in an event of an attack. The Security Orchestrator manages the security plan and orchestrates the enforcement of the security countermeasures in the systems. For this purpose, it instructs the Security Enforcement Plane, which is in turn, is composed of the IoT Controller, SDN Controller and NFV MANO to deploy and (re)configure the VNFs. NFV-MANO is responsible for secure placement and management of VNFs and Security VNFs over the virtualized infrastructure managed by the Virtual Infrastructure Manager (VIM) component. Thus, it is in charge of realizing the scalable and dynamic deployment of vFirewalls required in our solution. The vFirewall can be deployed at the edge close to the Radio Access Network (RAN) or in the core of the 5G network. In addition, the SDN Controller upon an orchestration command coming from the North-bound API can add or update filtering rules in the vFirewall.

IV. Virtualized 5G Infrastructure

Figure 2 shows an overview of the experimental infrastructure deployed for conducting the validation of the proposed framework. A virtualized LTE-based architecture, which also includes several 5G features, is presented and explained in this section. 10 Computers with Ubuntu 16.04 operating system and OpenStack Mitaka compose this infrastructure. The deployment utilizes Neutron and OpenDayLight

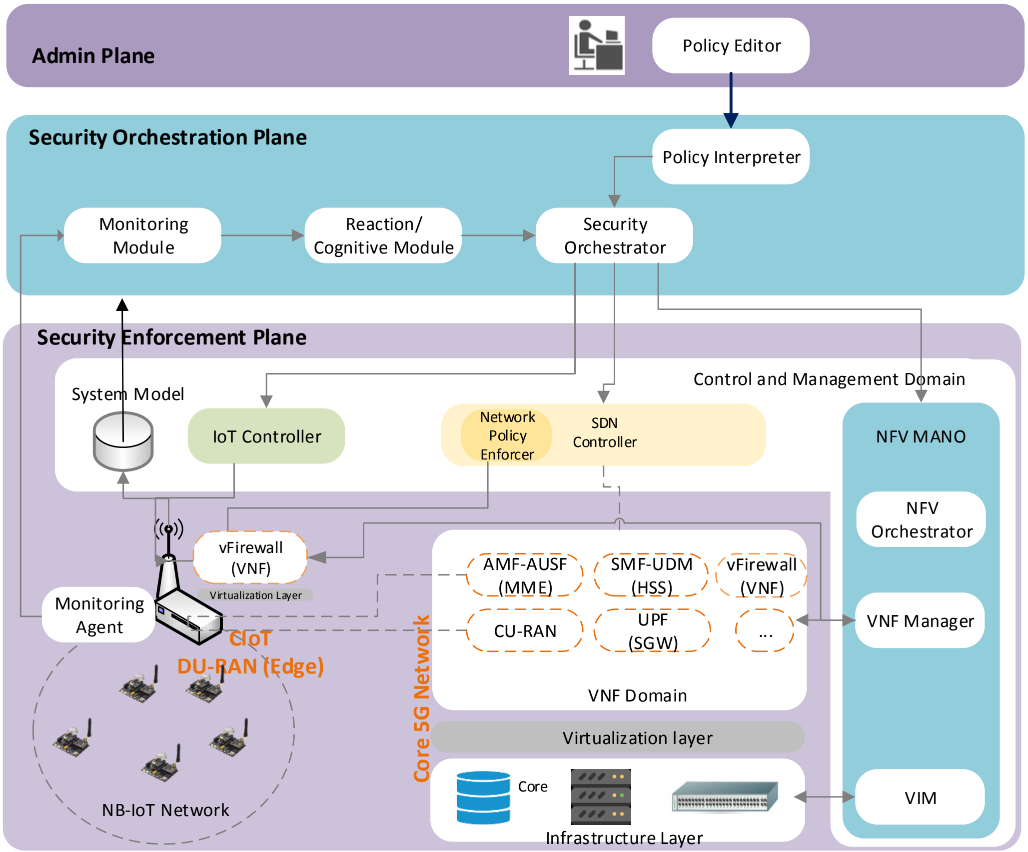

Figure 1. Management architecture for the proposed system

as the SDN Controller. OpenDayLight uses OpenFlow and OVSDB for controlling the Open Virtual Switch (OVS) software, which, in turn, controls the data path of virtual machines. As can be seen from the figure, different colours (blue and purple) represent different tenant/administrative domains, and each one has used a completely different set of VNFs along the 5G network. By using the last release of the Mosaic5G [2] project, a decoupling between DU and CU on the RAN side has been achieved. Although the components in the Evolved Packet Core (EPC) still use the MME, HSS and SGW/PGW terminology, they are fully virtualized and running in VNFs in line with the 5G vision. Those VNFs provided by Mosaic5G, which is an evolution of OpenAirInterface [3], have been deployed by using a VIM such as OpenStack [4]. OpenStack controls those virtual resources and allows the sharing of physical resources by more than one tenant. In addition, a Service Infrastructure Manager (SIM) deploys services over virtual layers, controls the life-cycle of the services and allows functionalities such as redeployment, reconfiguration, upgrading, start and stop. The SIM employed in this research is the one referred to as VNFM in the ETSI MANO architecture, i.e., Juju [17]. Following the same approach, the VIM deploys new virtual machines when required and add them to the vFirewall stack of a specific tenant. Later on, by using the SIM, those virtual machines are configured as NB-IoT services. This workflow is further explained in more detail in section V.

It has been previously demonstrated [3] that the proposed NB-IoT vFirewall is not only able to deal with IoT protocols but also 5G network traffic with nested encapsulation such as Virtual eXtensible Local Area (VXLAN) and/or General Packet Radio Service (GPRS) Tunneling Protocol (GTP) to provide features such as mobility, tenant isolation, admission control and so on. Since 5G packets travelling along this infrastructure are encapsulated by different encapsulation protocols depending on the network segment, this is a perfect scenario to allow investigating and analyze NB-IoT traffic throughout all different network segments.

V. Scalable Deployment of vFirefalls Design

The designed approach is focused on automatical deployment of NB-IoT vFirewalls when required from the security policies in the framework. Each VNF instantiated for this purpose will have a different set of rules for multi-tenancy, device mobility and NB-IoT compliance for handling traffic crossing the infrastructure. Those rules represent specific traffic that needs to be mitigated for security reasons. In order to speed up the service configuration process, the split of rules between different VNFs is carried out using, like a splitting criterion, the source IP address where a mask is applied to determine to which VNF should be installed. There is an inventory with the number of VNFs currently deployed and a modulus is applied over the result of the

[2]http://mosaic-5g.io/
[3]http://www.openairinterface.org/
[4]https://www.openstack.org/

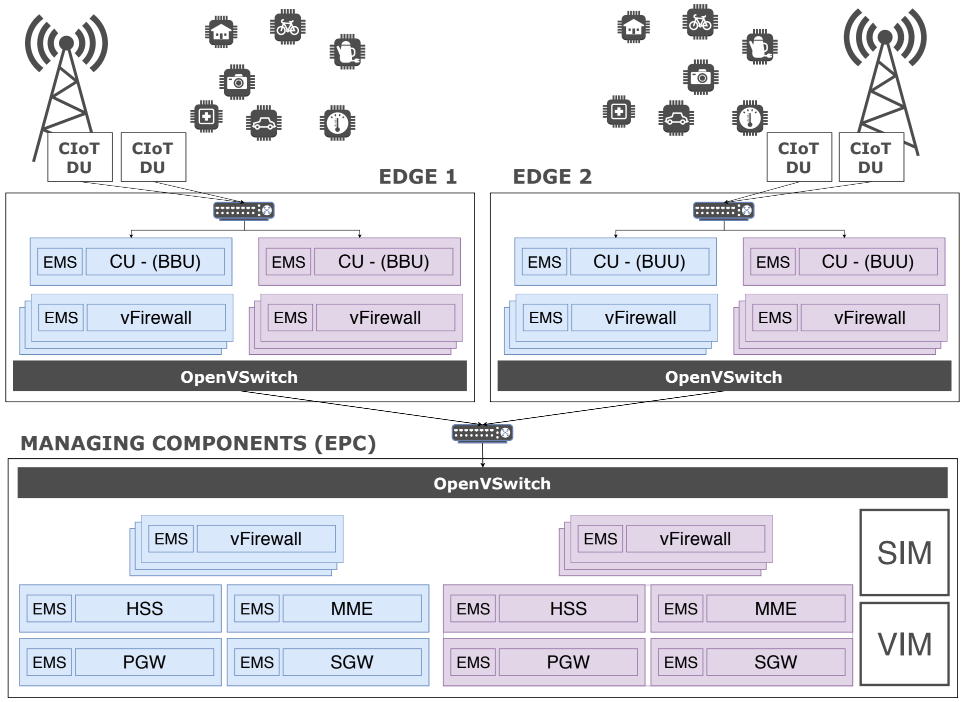

Figure 2. Network infrastructure with vFirewalls for the proposed system

marking in order to determine the associated VNF. Therefore, when the Orchestrator triggers the action of deploying a new vFirewall for a specific tenant, the vFirewall already knows how to perform the loading of rules as this is instructed by the configuration service parameters.

The following describes the required steps for deploying a new VNF with a 5G vFirewall acting as a service. Figure 3 defines a workflow diagram, which represents different phases since the Orchestrator sends the command to add a new virtual NB-IoT Firewall.

In the first step, the Orchestrator sends a deployment request to the SIM for deploying a new VNF. That request message is triggered when the framework described in section III detects that there are not enough advisable resources on existing vFirewalls for applying a new set of rules or because those vFirewalls are handling a different NB-IoT device domain. Subsequently, the SIM (Juju) interacts with the VIM (OpenStack) to start the installation of the operating system. The VIM returns a success response to the SIM once that process is finished. Secondly, once the operating system has been installed, the SIM sends a request to the previously created VNF for installing the Element Managed System (EMS), which is able to control the life-cycle of each service deployed including actions such as start, stop, re-install, uninstall, redeploy, reconfigure and so on. When the EMS installation is completed, the same VNF notifies the SIM (Juju), which in turn does the same with the Orchestrator. Finally, the Orchestrator starts the installation procedure of the 5G vFirewall service by sending this request to the SIM. Consequently, the SIM performs the installation and initial configuration of the VNF service, and notifies the Orchestrator. After that, the Orchestrator will select the rule set given by the upper layers and will interact directly with the new VNF vFirwall in order to load the configuration therein. Finally, the Orchestrator configures OpenStack (Neutron) in order to redirect the traffic to the new VNF Firewall created.

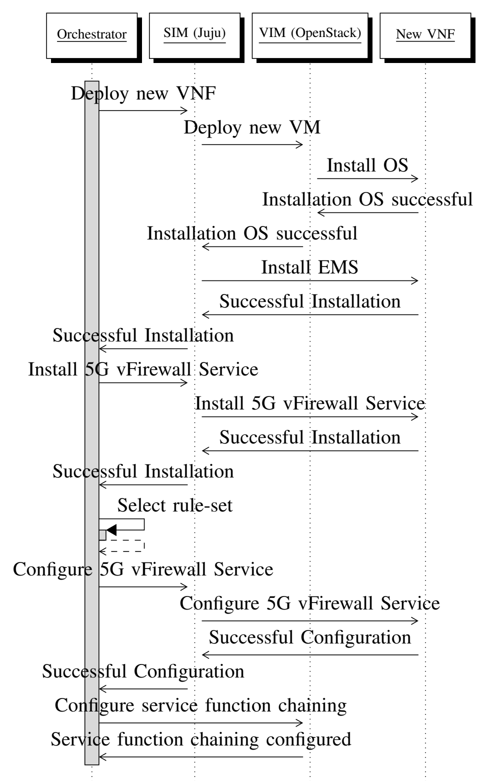

Figure 3. Sequence diagram to deploy a new vFirewall

VI. Performance Evaluation

A. Testbed description

The following testbed has been created to empirically validate the proposed design and evaluate the service deployment times by measuring the performance of the installation of vFirewalls as VNF services in the proposed 5G infrastructure. The testbed has been built by employing 6 physical machines as managed computers, each one with 8 cores, 24 Gbytes of RAM, and 4x1Gbps Ethernet NICs + IPMI Ethernet. Each physical machine contains up to 8 VMs. Therefore, the managed infrastructure consists of up to 48 machines. These machines are managed by a physical machine with an Intel Xeon Processor E5-2630 v4 with 32GBytes and 3x10Gbit Ethernet NIC, acting as a management plane. Although it is known that nested virtualization has a negative impact on performance, this testbed has allowed us to demonstrate the scalability of the proposed system with a large number of managed resources. Therefore, better performance results can be expected at production grade deployments. It is worth mentioning that the infrastructure presented in Figure 2 matches the deployment carried out in our testbed.

B. NB-IoT Virtual Firewall Capacity Test

Figure 4 provides the configuration times of a VNF firewall from scratch when all filtering rules have to be loaded to the system at once to provide the initial configuration of the vFirewall. In order to figure out a trade-off in terms of scalability, a set of experiments were carried out by applying a different number of filtering rules in the initial configuration. As seen in the figure, a base two exponential stressing test has been conducted. The results show that 4096 filtering NB-IoT rules are the maximum that each vFirewall can load at its configuration time without surpassing 1 second. Beyond that point, the configuration time increases over limits that would not be efficient enough in terms of response time, delay and packet losses.

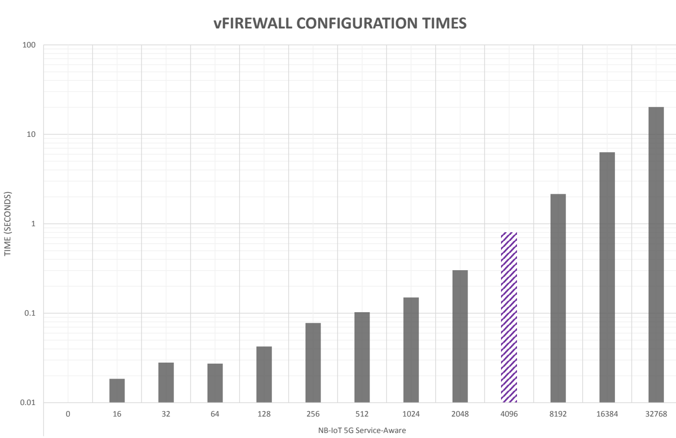

Figure 4. Configuration time of adding NB-IoT service-aware 5G multi-tenant Infrastructure rules

In addition to configuration times, Table I shows Packet Loss Ratio, Transmission Time Overhead and Jitter when 4096 simultaneous NB-IoT devices are being inspected in real-time from one vFirewall. It should be noted that these experiments have been conducted by assuming a homogeneous set of IoT devices with specific features. However, the proposed solution would also be able to deal with heterogeneous IoT environments as long as those devices comply with the specs herein defined. For a deeper analysis of heterogeneity in terms of IoT devices, we refer to our previous work in [3]. For a deeper analysis of heterogeneity in terms of IoT devices, we refer to our previous work in [3]. As can be seen in the third column, the performance of all of the metrics are within reasonable ranges. There is no packet loss or transmission time overhead and the Jitter is acceptable for NB-IoT applications. Therefore, this test has proved the feasibility of the proposed solution.

TABLE I. Statistics when 4096 flows are being simultaneously handled

Measured Feature	*Units*	*Value*
Packet Loss Ratio	Percentage	0.00%
Transmission Time Overhead	Seconds	0
Average of Jitter	Milliseconds	0.2414
Configuration Time	Seconds	0.8

C. Scalability and Stress Results

This section validates the scalability results achieved when different stress methods are applied to the proposed system. Figure 5 provides the deployment times by increasing the scale of the vFirewalls deployment scenario exponentially from 2 VMs up to 48 VMs with each VM performing a loading a 4096 rule set. It leads to a scenario supporting from 4096 NB-IoT to a maximum of 196,608 NB-IoT devices. Moreover, it is noted that for each of these scenarios, different ramping times have been executed. The ramping time is defined as the time elapsed between two requests for the instantiation of a new vFirewall each time. Therefore, the lower the ramping time is, the higher the system is stressed since it means that all the NB-IoT devices have been very rapidly connected to the system and the time for requests between different VNFs is very low. The results show four different levels of stress: 0s, 1s, 5s and 10s, 0s being the most stressed one, meaning that all the NB-IoT devices (196,608 devices for the largest scenario analyzed) are simultaneously connected.

At a glance, Figure 5 shows linear trends in deployment times regardless of the number of vFirewalls deployed and also regardless of the level of stress of the system (ramping time). These results clearly validate the scalability of the proposed system. It is noted that in order to emulate this large number of NB-IoT devices, we have gathered Packet Captures (PCAPs) from the real infrastructure and replicated them with different IP addresses to generate the traffic associated to each of the NB-IoT devices and thus stress the data path.

Figure 5 shows three different times stacked. The first time is the time spent on the installation of the VM itself, which is around 4s taking in all the cases. The second one represents the time consumed in installing the EMS and the vFirewall component in this VM, which is always around 3s. Finally, the third time is the loading time of all the firewall rules related to all the NB-IoT devices inside the vFirewall. It can be concluded that the system scales with respect to the number of VNFs and also with respect to the ramping time,

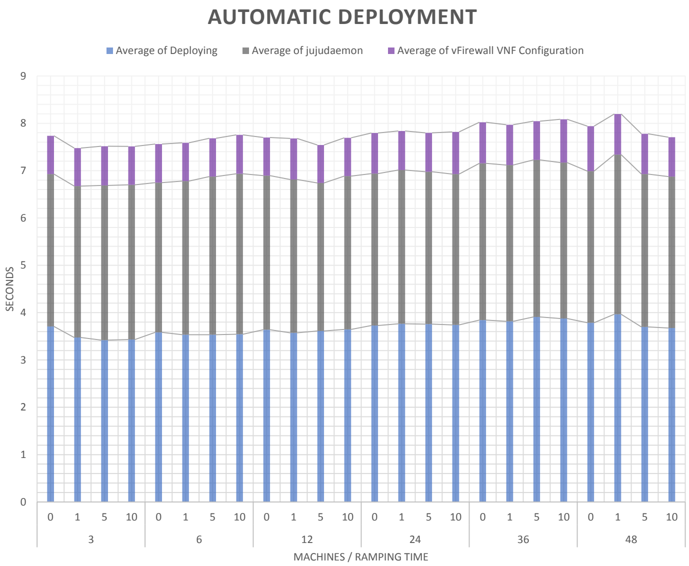

Figure 5. Deployment times of vFirewalls with different number of machines and ramping times

which implies that it scales with a large number of NB-IoT devices.

It is worth noting that there is a fourth measured time that is the time required to configure OpenStack in order to redirect the traffic to the newly create vFirewall in order to include it into the data path. However, this negligible time is not shown in the figure since it is less than 1ms and it cannot be seen in the graph with the scale in seconds.

VII. Conclusion

This paper has proposed a new virtual firewall based IoT security solution and its automatic deployment scheme for 5G mMTC scenarios. The solution performs a smart trade-off between configuring rules in an existing VNF firewall and performing the deployment of a new VNF firewall, configuring the virtual firewall into the data plane and allowing splitting the large rule set between the existing ones. Experimental results have validated the maximum number of NB-IoT multi-tenant rules that can be managed by each of the virtual firewalls. Moreover, empirical deployment results have displayed a clear linear trend in the deployment times of new VNFs when the scenario scales up, thereby validating the proper scalability of the architecture. In addition, performance results have shown the feasibility to deal with close to 200,000 NB-IoT devices, through the automatic deployment of 48 virtual firewalls in less than 6.4 minutes (i.e., only 8 sec per firewall on average).

In future work, we will investigate other kinds of virtual network security functions such as virtual Channel-Protection, to be deployed at the edge of the NB-IoT network, in order to protect and isolate further traffic among users, carriers and verticals in different network slices.

Acknowledgment

This work was funded in part by the European Commission Horizon 2020 5G-PPP Programme under Grant Agreement Number H2020-ICT-2016-2/761913 (SliceNet: End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks). In addition, it has been partially supported by a postdoctoral INCIBE grant "Ayudas para la Excelencia de los Equipos de Investigacin Avanzada en Ciberseguridad" Program, with code INCIBEI-2015-27363.

References

[1] "5G-PPP. The 5G Infrastructure Public Private Partnership," 2019. [Online]. Available: https://5g-ppp.eu/

[2] E. David Kennedy, "Euro-5g-Supporting the European 5G Initiative D2.6 Final report on programme progress and KPIs," 5G-PPP, Tech. Rep., 2017. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2017/10/Euro-5G-D2.6_Final-report-on-programme-progress-and-KPIs.pdf

[3] P. Salva-Garcia, J. M. Alcaraz, Q. Wang, J. Bernal-Bernabe, and A. Skarmeta, "5g nb-iot: Efficient network traffic filtering for multi-tenant iot cellular networks," Security and Communication Networks, vol. 2018, Nov. 2018.

[4] 5G PPP Architecture Working Group, "View on 5G Architecture," White paper, no. July, 2016.

[5] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computinga key technology towards 5g," ETSI white paper, vol. 11, no. 11, 2015, pp. 1–16.

[6] R. Mijumbi, J. Serrat, J.-L. Gorricho, S. Latre, M. Charalambides, and D. Lopez, "Management and orchestration challenges in network functions virtualization," IEEE Communications Magazine, vol. 54, no. 1, 2016, pp. 98–105.

[7] G. A. Carella and T. Magedanz, "Open baton: a framework for virtual network function management and orchestration for emerging software-based 5g networks," Newsletter, vol. 2016, 2015.

[8] E. Chirivella-Perez, J. M. A. Calero, Q. Wang, and J. Gutiérrez-Aguado, "Orchestration architecture for automatic deployment of 5G services from bare metal in mobile edge computing infrastructure," Proc. Int. Wirel. Commun. Mob. Comput. Conf., vol. 2018, Nov. 2018.

[9] D. Peraković, M. Periša, and I. Cvitić, "ANALYSIS OF THE IoT IMPACT ON VOLUME OF DDoS ATTACKS," 2015. [Online]. Available: http://postel.sf.bg.ac.rs/simpozijumi/POSTEL2015/RADOVI PDF/Telekomunikacioni servisi - kvalitet i ekonomski aspekti/5. Perakovic-Perisa-Cvitic.pdf

[10] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, jun 2017, pp. 10–28. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804517301455

[11] Q. M. Ashraf and M. H. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things," Journal of Network and Computer Applications, vol. 49, mar 2015, pp. 112–127. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804514002732

[12] H.-C. Hsieh, J.-L. Chen, and A. Benslimane, "5G virtualized multi-access edge computing platform for IoT applications," Journal of Network and Computer Applications, vol. 115, Aug. 2018, pp. 94–102.

[13] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi, and S. Tarkoma, "IoT SENTINEL: Automated Device-Type identification for security enforcement in IoT," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Jun. 2017, pp. 2177–2184.

[14] W. Meng, "Intrusion detection in the era of IoT: Building trust via traffic filtering and sampling," Computer, vol. 51, no. 7, Jul. 2018, pp. 36–43.

[15] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things," IEEE Communications Magazine, vol. 56, no. 2, 2 2018, pp. 30–36.

[16] R. Sairam, S. Sankar Bhunia, V. Thangavelu, and M. Gurusamy, "NETRA: Enhancing IoT Security using NFV-based Edge Traffic Analysis," Tech. Rep., May 2018. [Online]. Available: https://arxiv.org/pdf/1805.10815.pdf

[17] B. Karakostas, "Towards autonomic cloud configuration and deployment environments," in Cloud and Autonomic Computing (ICCAC), 2014 International Conference on. IEEE, 2014, pp. 93–96.