SDN/NFV-enabled Security Architecture for Fine-grained Policy Enforcement and Threat Mitigation for Enterprise Networks

Benedikt Pfaff, Johann Scherer, David Hock
Infosim GmbH, Wuerzburg, Germany

Nicholas Gray, Thomas Zinner, Phuoc Tran-Gia
University of Wuerzburg, Germany

Raphael Durner, Wolfgang Kellerer
Technical University of Munich, Germany

Claas Lorenz
genua GmbH, Kirchheim, Germany

CCS CONCEPTS

• **Networks** → **Network security**; *Firewalls*; *Network manageability*; *Network monitoring*;

KEYWORDS

SDN, NFV, Firewalling, Security, Management

ACM Reference format:
Benedikt Pfaff, Johann Scherer, David Hock, Nicholas Gray, Thomas Zinner, Phuoc Tran-Gia, Raphael Durner, Wolfgang Kellerer, and Claas Lorenz. 2017. SDN/NFV-enabled Security Architecture for Fine-grained Policy Enforcement and Threat Mitigation for Enterprise Networks. In *Proceedings of SIGCOMM Posters and Demos '17, Los Angeles, CA, USA, August 22–24,2017,* 2 pages.
https://doi.org/10.1145/3123878.3131970

1 INTRODUCTION

Today, network security in enterprises is mainly enforced by firewalls guarding the perimeter of the network against an ever increasing number of cyber threats. While inspecting and enforcing security policies on every flow entering or leaving the network, Perimeter Gateway Firewalls (PGF) provide hardly any defense against attacks originating from and targeting the inside of the network. Thus, once the perimeter is breached attackers and malware can easily compromise additional hosts as we have seen in the recent outbreak of the WannaCry worm [5].

To mitigate such outbreaks, enterprises usually rely on costly Intrusion Prevention Systems (IPS) and a centralized update management to install security updates in a timely manner. Both systems aim to minimize the window, in which the enterprise network is susceptible to attacks. Yet, this is a tedious process as the IPS requires an attack signature and changes to the software stack demands thorough testing. Furthermore, in the case of ZeroDay attacks no signatures and updates are available. Hence, this often results in a widened window in which the network remains vulnerable and an increased risk.

A complimentary approach to alleviate these threats is to quarantine malicious hosts on a network level, as this can be deployed immediately and is independent from the update procedure. To accomplish this, a fine-grained flow selection and security control is needed. Whereas architectures such as Ethane [1] and more recent technologies like Software-defined Networking (SDN) and Network Function Virtulization (NFV) provide this required granularity [4], the adaptation of these technologies in enterprise networks remains limited. This is due to the fact, that the integration of new technologies into an existing network infrastructure is a highly complex task, as the compatibility with systems such as network management and cloud management has to be assured for production environments.

In this work, we demonstrate the prospects of seamlessly integrating SDN and NFV based security operations into the existing enterprise network infrastructure to provide state-of-the-art stateful firewalling for advanced packet filtering as well as on-demand fine-grained flow separation and isolation for the exterior and interior network. This is achieved by levering an omnipresent firewall (cf. [3]) which is based on cloud principles enabling enhanced scalability and resilience, while simultaneously cutting down on Operation Expenses (OpEx). We illustrate the advantages of the implemented security architecture by the example of the Bring-Your-Own-Device use case.

In the following, we present the involved architectural components and outline the planned demonstration detailing fine-grained access control, firewall offloading for further optimization and the integration into a network management system.

2 DEMO SETUP

The setup of the demo is depicted in Fig. 1 and shows the separation into a management and a data plane. The management plane is composed of the ONOS SDN-Controller which handles the configuration of the SDN switches, the network management system StableNet is used for monitoring all critical systems, and the virtualized infrastructure manager OpenStack governs the cloud resources. Whereas the main responsibility of the SDN-Controller is the separation of all users and the management of forwarding decisions in the network, the Cloud Management monitors and orchestrates the virtual firewall instances. Finally, the Network Manager connects both parts and serves as an unified point of administration.

The data plane consists of a mobile device, which is used for the BYOD scenario and an IP camera, which resembles a service provided by the enterprise network. In addition to the camera, an auxiliary service is running within the cloud, which initializes the authentication procedure of the mobile device upon connection. To enhance the security of the network every connection between the mobile device and service is forwarded separately in an on-demand

SIGCOMM Posters and Demos '17, August 22–24,2017, Los Angeles, CA, USA

ACM ISBN 978-1-4503-5057-0/17/08.
https://doi.org/10.1145/3123878.3131970

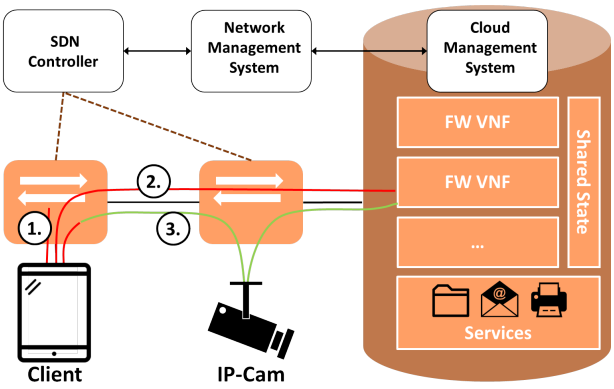

Figure 1: Considered enterprise architecture and course of events for the showcase *fine-grained access control*

virtual network and re-routed via a Firewall Virtual Network Function (FW-VNF). The implemented FW-VNF solution is based on a centralized state to provide an enhanced scalability and reliability (cf. [2]). As this approach leads to an increased load on the firewalls regarding the required data rate and the number of rules at traffic spikes, the capabilities of the enterprise cloud infrastructure may be exceeded. Thus, our solution provides the possibility to offload selected trusted flows directly to the switches, where they are processed at line rate and reduce the load on the VNFs.

3 SCENARIO AND DEMO PRESENTATION

In the presented scenario a mobile device is connected to the enterprise network and accesses the video stream provided by an IP camera. For this scenario the demonstration focuses on three main parts which are discussed in more detail in the following, e.g., SDN-enabled fine-grained access control, firewall resiliency and traffic offloading for performance optimization.

Fine-grained access control. After connecting a mobile device to the wireless access point of the presented architecture, the user's access to the network is restricted and only includes access to a captive portal, which handles the initial authentication. Once authenticated the user has to actively request a service, which is represented by the video stream of an IP camera in our demonstration. This triggers the SDN controller to dynamically deploy the appropriate flow rules on each device along the path to provide the connectivity to the requested service, hence resulting in a fine-grained access control. As the connectivity of the host is restricted to actively requested services by the user the attack surface is drastically reduced and malware can only spread in this time frame and has to use one of these services as attack vector. In the case of the WannaCry worm, if the user has not requested the SMB service, no connectivity would have been provisioned and thus no further infection would have been possible. In addition, all packets are redirected to the firewall VNFs for stateful packet inspection before reaching the service. This adds an additional layer of security by further restricting access to provided services. For monitoring purposes all user-to-service relations are illustrated within the network management system and are depicted as an informative view to the network operator.

Resiliency. By separating and outsourcing the local state from the firewall VNF core to a shared state table, which is accessible by all firewall VNFs, we achieve a scalable and resilient firewall solution. Having the state decoupled, the main firewall VNF functions as mere compute instance which eases the configuration of the firewall cluster and allows for fast adaptation which is required for quarantining outbreaks before they reach a critical mass of infected hosts. In addition, it reduces the complexity of failover scenarios, as no state has to be migrated. In our demonstration, we illustrate this by manually shutting down the VNF instance, which is handling the user's video stream. As a result, the system immediately detects the failure and redirects the affected traffic to a standby VNF capable of handling the connection directly without interruption due to the shared state. Hence, the user experiences no or just minor service degradation while watching the video stream until the handover is completed.

Offloading. In times of ongoing attacks and traffic spikes firewalls are pushed to their capacity and can quickly become the bottleneck of the network. Thus, the proposed security architecture is able to offload trusted flows directly to the switching hardware to ease the load on the firewalls. To demonstrate the performance impact of the offloading mechanism in our demonstration, we increase the number of concurrent video streams until the firewall VNFs start overloading. Thus, packets of the user's video stream are delayed or dropped, resulting in a service degradation. By offloading trusted video streams and while redirecting potentially malicious flows via the firewall VNFs, the load on the VNF decreases, which is reflected in the network management system and hence the quality of the IP camera's video stream normalizes.

ACKNOWLEDGEMENTS

This work has been performed in the BMBF framework KMU-Innovativ in the project SarDiNe (Project ID 16BP12308). The authors alone are responsible for the content of the paper.

REFERENCES

[1] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker. Ethane: Taking control of the enterprise. *SIGCOMM Comput. Commun. Rev.*, 37(4):1–12, Aug. 2007.
[2] N. Gray, C. Lorenz, A. Müssig, S. Gebert, T. Zinner, and P. Tran-Gia. A priori state synchronization for fast failover of stateful firewall vnfs. In *Workshop on Software-Defined Networking and Network Function Virtualization for Flexible Network Management (SDNFlex 2017)*, Göttingen, Germany, 2017.
[3] C. Lorenz, D. Hock, J. Scherer, R. Durner, W. Kellerer, S. Gebert, N. Gray, T. Zinner, and P. Tran-Gia. An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement. *IEEE Communications Magazine*, 55(3):217–223, March 2017.
[4] S. Scott-Hayward, S. Natarajan, and S. Sezer. A survey of security in software defined networks. *IEEE Communications Surveys & Tutorials*, 18(1):623–654, 2016.
[5] SecureList. Wannacry ransomware used in widespread attacks all over the world. https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/. called on May 16, 2017.