Stateful Firewall with SDN and NFV
Claas Lorenz, genua mbh, clorenz@genua.de

Index Terms—Software Defined Networking, Network Function Virtualisation, Firewalls, Security.

I. MOTIVATION

Software Defined Networking (SDN) enables an increased decoupling of the logical from the underlying physical network topology. This comes along with the abolition of the classical network separation enforced by perimeter firewalls. To ensure a high level of security it is crucial to enforce firewall functionality by suitable mechanisms of the network. These so-called field firewalls allow the usage of every network switch as a firewall to enforce a global security policy. The high degree of control in SDN also improves the ability to defend against network attacks like ARP-spoofing and different kinds of Denial-of-Service threats. While stateless packet filters may be realized by OpenFlow-switches stateful firewalls remain a challenge.

This document introduces three approaches to realize stateful firewalls in the context of SDN and Network Function Virtualisation (NFV). Also, there is an outlook towards further improvements.

II. APPROACHES

The implementation of stateful firewalls with SDN and VNF can be realized by three major approaches. The first one focuses on the SDN-controller. The second one is based on the exclusive usage of Virtualized Network Functions (VNF) for the classification as well as for the filtering. The third tries to combine the advantages of the other approaches in a hybrid way.

A. Controller centric

This approach relies on a reactive controller pattern. If an unknown flow is introduced the controller is provided with a copy of the triggering packet and can decide how to handle the flow. This allows the filtering concerning a given policy. If the flow is permitted a new rule is installed on the switch to forward the traffic of the connection. Additionally, an alarming rule for the disconnection is placed. The state of the connection is tracked in the controller which allows the removal of the forwarding rules while disconnecting.

The biggest advantage of this approach is the limitation on pure SDN techniques and therefore a good portability between networks. On the other hand there is a significant overhead by involving the controller on each connection establishment. If many new connections are requested the controller may become a bottleneck. Another drawback is the memory consumption of the rules. Especially hardware switches are quite limited in that regard. Though it is possible to save space by utilizing wildcards there remains a linear worst-case space complexity in the amount of connections.

B. VNF centric

The VNF centric approach relies on routing the network traffic via special virtualized network functions which filter the traffic and maintain a distributed state table concerning the security policy. The advantage of VNF lays in their great scalability. This allows a safe usage even in heavy load scenarios. A disadvantage may be caused by long distances while routing within the network. An improper placement of VNF may therefore cause a significant additional latency.

C. Hybrid

The hybrid approach combines the scalability of VNF with the great throughput of dedicated rules on the switch. At first, all traffic is rerouted through the VNF. When a connection lasts for a certain period of time a dedicated rule is established on the ingress switch. This allows a normal handling of the connection by the network. The overall throughput of data intensive services (e.g. video streams) can be improved while keeping the initial latency low.

III. IMPROVEMENTS AND FUTURE WORK

While writing this document the functionality of the first and second approach has been implemented prototypically for the ping protocol. The next steps include the following aspects:

a) Extension: The filtering of stateful protocols should be extended to support TCP connections.

b) Performance: The performance of the different approaches needs to be quantified to estimate their usefulness.

c) Machine Learning: The decision to switch from VNF to a dedicated rule on the SDN switch may be improved by using machine learning. This allows a flexible and self-adapting reaction to new load scenarios.

d) Application-Level-Filtering: Stateful firewalls deliver an important contribution for the security of a network. But, a very high degree of protection cannot be reached without enforcing filtering on the application level. Thus, an integration into the hybrid approach remains an additional challenge.