week34

FLOWNAC:A REAL EXPERIENCE EXPLORING NOVEL NFV ARCHITECTURES



VNF design alternative selection criteria

FLOWNAC illustrates the applicability of NFV architectures described above with a real example, FlowNAC, a flow-based network access control. This solution has already been deployed over the OpenFlow-based EHU-OEF infrastructure and demonstrated at several conferences like IEEE GLOBECOM 2013. The following analysis performed over the FlowNAC example focuses on one hand on SDN-agnostic and SDN-aware NFV architectures, as both share the same compute-based approach for VNF design, and on the other hand SDN- enabled NFV architecture.

FlowNAC is a NAC system for services that can be identified as flows, inspired by the IEEE 802.1X port-based NAC, which is a basic NAC solution enforcing the access control at the port level (i.e., the physical port of the network node). The main difference between both approaches is the granularity of each solution: port vs. flow.

The traffic originated in the user can be classified in three categories:

\*a-type: Authentication and authorization

(AA) traffic that must be processed by the FlowNAC VNF to keep the state associated with each AA process. Being related to the AA process, it will be limited in time and volume.

\*b-type: Data traffic for the authorized services that must be granted access to the network. It will depend on the actual service provided, which can be bandwidth-intensive (e.g., multimedia services) or time-sensitive. This traffic must be evaluated by the FlowNAC VNF to enforce the access control functionality.

\*c-type: Data traffic for non-authorized services (the remaining traffic generated by the user), which must be denied access to the network. This traffic completely depends on the user and its operating sys- tem, running applications, viruses, and so on. Similar to b-type traffic, the FlowNAC VNF must enforce the access control, but in this case to prevent these frames accessing the resources.

Following the compute-based design of the first two approaches to the NFV architecture (SDN-agnostic and SDN-aware NFV architectures), FlowNAC can be implemented as a soft- ware package running on a single VM. It could also be decomposed into different lower-level functions running on separated VMs, but for simplicity we assume just one element.

All the traffic from users must be redirected to the VM by the network infrastructure. The AA traffic is processed, authorized data traffic is allowed back into the network to reach the authorized service, and non-authorized data traffic is dropped.

This approach has several benefits like its ease of implementation and deployment, as the FlowNAC VNF relies solely on computing resources and is deployed by simply instantiating one VM and redirecting all the traffic from the user to it. Migration of the FlowNAC VNF is also straightforward as it is based on legacy computing virtualization technology with well-known interfaces, and the functions are completely isolated from the underlying infrastructures.

On the other hand, this architecture also has several drawbacks. As with any other VNF, the scalability is improved by virtualization techniques, which allow more or fewer computation resources to adapt the processing capacity to the actual demand. However, the scalability would be limited by the availability of computing resources.