Certification of Virtual Network Functions

November 2017

THE WHITEPAPER FROM XENA NETWORKS AND CRITERION NETWORK LABS DISCUSSES THE APPROACH FOR TESTING AND CERTIFYING VIRTUAL NETWORK FUNCTIONS USING THE MULTI-VENDOR NFV FRAMEWORK FROM CNLABS AND THE LAYER 4-7 TRAFFIC GENERATOR FROM XENA NETWORKS.

THIS IS A TWO PART PUBLICATION, THE FIRST PART DISCUSSES TEST CONSIDERATIONS FOR VALIDATING VIRTUAL NETWORK FUNCTIONS, FRAMEWORK AND TOOLS USED, TEST METHODOLOGIES AND OUTCOMES , THE SECOND PART WILL ADDRESS VALIDATION OF COMPLEX USE CASES USING NETWORK SERVICE ORCHESTRATORS THAT EMPLOY SERVICE CHAINED VIRTUAL NETWORK FUNCTIONS.

AN EVALUATION OF THE PERFORMANCE OF AN OPEN SOURCE FIREWALL WITH DIFFERENT TEST CONFIGURATIONS IS INCLUDED. TESTING WAS CONDUCTED AT CNLABS, AN ISO 17025 ACCREDITED VENDOR NEUTRAL INDEPENDENT TEST LAB AT THE LAB'S TEST FACILITY IN BANGALORE.

Challenges with testing Virtual Network Functions

There is an increasing ask for network operators to introduce cost savings and agility in their networks through virtualization, network programmability and cut down on service deployment times. Complexities of the VNF deployments are increasing and customers have started using VNFs not just for simple functionalities like firewall or load balancer in enterprise data centers, but considering VNF deployments for replacing core functions in complex carrier grade network environments.

As customers use Virtual Network Functions (VNFs) for realizing agile service deployments for complex network use cases, these solutions are very often realized using multi-vendor products. It is not uncommon for a customer to have a need to ensure that virtual network functions can work on solutions that have the NFV Infrastructure (NFVI), Service Orchestrators and Cloud Controllers from different vendors.

To certify VNFs it is essential to look beyond simple functionality and throughput testing, adopt comprehensive test methodologies that take into account all dimensions and test with real world traffic conditions to ensure that VNFs achieve consistent performance for intended service deployment while interoperating with existing network components to ensure that the customer's deployment, monitoring and operational needs are met. Continuous integration (CI) testing is essential to ensure that the VNF performance and solution goals are met as constant upgrades are made to various components of the solution.

Factors that need to be considered for VNF certification include

- VNF functionality and complexity
- Performance of VNF on different virtual network infrastructure configurations
- The hardware infrastructure on which the virtual network services are being deployed
- VNF interoperability with the Virtual Infrastructure Management Platform
- Lifecycle management – onboarding, configuration, scaling and management with VNF Managers
- Use case considerations and interactions with devices internal or external to cloud

To ensure that a comprehensive view can be taken to evaluate the stability and reliability of VNF testing, it is very important to have a flexible NFV Test Framework that can quickly create multiple test configurations, test suites with comprehensive test methodologies and traffic generators that can emulate real world test conditions and can be deployed in physical or virtual network environments.

This white paper demonstrates how some of the goals listed above be realized by using Xena's L4-7 traffic generator on configurations orchestrated by CNLabs NFV Test Framework . The open source firewall pfSense is used as the Virtual Network Function. Considerations include

- Creation of on-demand test beds with different test-bed configurations
- Measure peak throughput on Virtual Firewall using TCP/UDP/HTTP & Real-world traffic conditions
- Usage of external traffic generators in cloud test environments
- Characterize VNF performance using different NFV Infrastructure configurations and evaluate resources required to achieve target performance levels