NFV ISG PoC Proposal –VNF Router Performance with DDoS Functionality

1. NFV ISG PoC Proposal

1.1 PoC Team Members

Include additional manufacturers, operators or labs should additional roles apply.

PoC Project Name: VNF Router Performance with DDoS Functionality

Network Operators/ Service Providers:

AT&T	Contact: Steven Wright, sw3588@att.com
Telefonica	Contact: Diego Lopez, diego@tid.es
Architect/Coordinator (Vendor A): Brocade	Contact: Ram (Ramki) Krishnan, ramk@brocade.com Others: Robert Bays, Muhammad Durrani, Stephen Hemminger
Vendor B: Intel	Contact: Trevor Cooper, trevor.cooper@intel.com
Vendor C: Spirent	Contact: Rajesh Rajamani, rajesh.rajamani@spirent.com

The Real-time Layer 2-4 DDoS Mitigation in NFV Framework PoC will be implemented using Brocade and Intel technologies including Brocade virtual router product and Intel®DPDK [DPDK]. Spirent will provide the physical and/or virtual test platforms.

AT&T will contribute expertise in use-case requirements, design of test-cases and oversight of solution characterization/analysis.

We are open to inclusion of other vendors/operators in our process subject to resource constraints.

1.2 PoC Project Goals

Motivation

ETSI GS NFV 004 (Network Functions Virtualization (NFV); Virtualization Requirements) [NFV-REQ] describes the need for appropriate security countermeasures to address security vulnerabilities introduced by the virtualization layer. Behavioral security threats such as Distributed Denial of Service (DDoS) attacks are an ongoing problem in today's Data Centers and are expected to pose even greater challenges to network operators deploying NFV infrastructures.

This problem is expected to be most acute in multi-tenant DCs providing Virtual Network Function as a Service. This use-case is described in ETSI GS NFV 001 (Network Functions Virtualization (NFV); Use Cases) [VNFaaS]. Specifically "Services provided by the vE-CPE may include a router providing QoS and other high-end services such as L7 stateful firewall, *intrusion detection and prevention* and more".

Goals

PoC Project Goal #1: This PoC aims to characterize the performance impact of implementing intrusion detection and prevention in a router VNF. The POC will demonstrate various Layer 2-4 DDoS attacks being handled in real-

time using an integrated VNF router. If this approach is successful, it will be highly complementary to the overall behavioral security threat strategy in NFV DCs.

1.3 PoC Demonstration

Venue for the demonstration of the PoC: The PoC is planned to be hosted in Brocade Communications Systems, Inc. San Jose, California, USA (additionally in Intel's Comms. Infrastructure Solutions lab in Hillsboro, Oregon) and can be accessed remotely from any location with reliable Internet service. We propose to use the latter capability to demonstrate the PoC at industry events in 2014, yet to be finalized.

1.4 Publication

PoC results will be documented in the form of participating company technical collateral (e.g. white paper) and made available to ETSI members. We also intend to use the PoC for public demos at trade-shows and appropriate industry events.

1.5 PoC Project Timeline

- What is the PoC start date?
    - The project is already underway as an internal project with the vendors.
- First PoC Report target date: February, 2014
- First Demonstration target date: Open Networking Summit (ONS), March 2nd - March 5th 2014, Santa Clara, CA, USA
- When is the PoC considered completed ? Once performance characterization data is published

2. NFV PoC Technical Details

2.1 PoC Overview

Layer 2-4 based DDoS attacks are an ongoing problem in today's networks. Examples of Layer 2-4 based DDoS attacks are [FDDOS]:

- SYN Flood Attack: Fake TCP connections are setup which result in table overflows in stateful devices.
- UDP Flood Attack: Servers are flooded with UDP packets which results in consumption of bandwidth and CPU. These can be used to target specific services by attacking, e.g., DNS servers and VOIP servers. These can also be amplification attacks – the common ones are NTP and DNS.
- Christmas Tree Flood Attack: TCP packets from non-existent connections with flags other than the SYN flag sent to servers result in consumption of more CPU than normal packets because of the effort required to discard them.

Typically, the above attacks are not from a single host or source IP address; multiple hosts with different source IP addresses working in tandem instigate these attacks – hence the term Distributed DoS or DDoS.

Real-time Layer 2-4 DDoS mitigation involves automatically recognizing large flows [OPSAWG-large-flow] and performing various types QoS actions such as drop, rate-limit on the recognized flows based on configured policies [I2RS-large-flow].

We plan to demonstrate various Layer 2-4 DDoS attacks (not limited to the ones being described above) being detected and mitigated in real-time by a Virtual switch/router (Brocade Vyatta vRouter 5600) which is running on an Intel x86 server as part of an NFV infrastructure. The Virtual switch/router will employ scalable inline line-rate algorithms for automatically recognizing the large flows which are the cause of DDoS attacks; this should ensure that the Virtual switch/router performance is not impacted.

As part of this PoC we plan to investigate x86 and DPDK features that enhance performance of this use case. This includes DPDK QoS features which will be used for DDoS mitigation actions.

2.2 PoC Scenarios

Figure 1 below depicts the various functional blocks of the data path processing pipeline of a Brocade Vyatta 5600 Virtual Router. Specific PoC objectives in the context of the data path processing pipeline of are described below.

Scenario 1 - Study the performance impact and benefits of the Layer 2/3/4 DDoS detection (large flow detection) block on packet processing.

Scenario 2 - Study the performance impact and benefits of the QoS block used for Layer 2/3/4 DDoS mitigation.

Various tests which will be performed are summarized below.

Test 1: For normal traffic, measure packet latency/jitter/throughput without the Layer 2/3/4 DDoS detection and mitigation blocks.

Test 2: For normal traffic, measure packet latency/jitter/throughput with the Layer 2/3/4 DDoS detection and mitigation blocks.

Test 3: For DDoS + normal traffic, measure packet latency/jitter/throughput without the Layer 2/3/4 DDoS detection and mitigation blocks.

Test 4: For DDoS + normal traffic, measure packet latency/jitter/throughput with the Layer 2/3/4 DDoS detection and mitigation blocks.

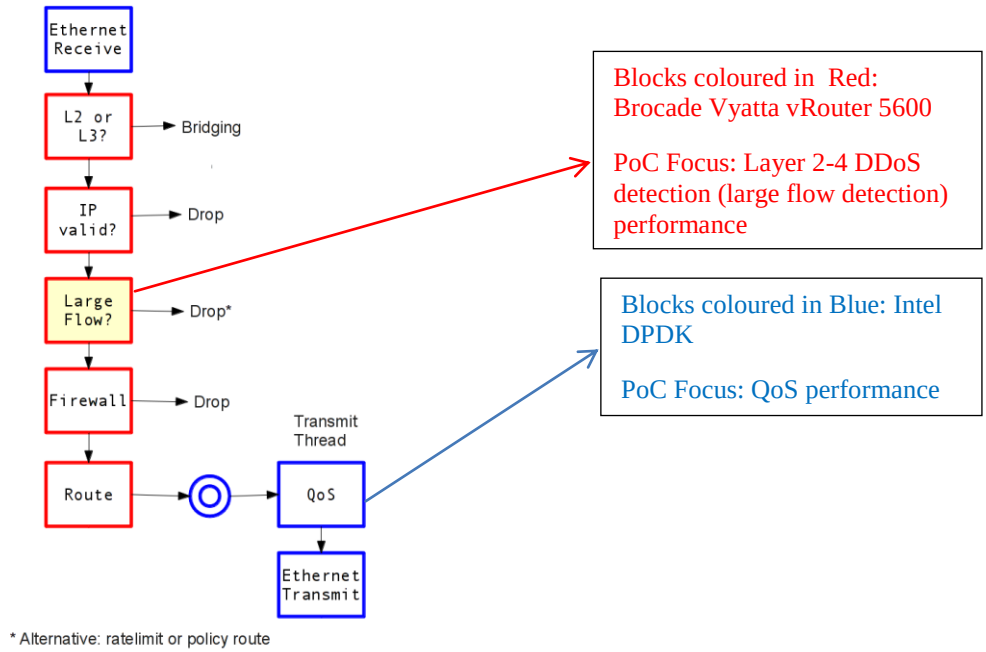

Figure 1: Data path processing pipeline of the Brocade Vyatta 5600 Virtual Router

2.2.1 PoC Test Setup

Figure 2 below describes the PoC setup which comprises of a single vRouter running over x86 Server Platform and describes how it maps into NFV Architectural Framework [NFV-ARCH]. The NFV vRouter, which is running on a single VM, is the DDOS victim and will be flooded with attack traffic such as UDP Flood along with normal traffic. vRouter will detect the attack and will take appropriate action in real-time while forwarding the normal traffic without any impact. SRIOV [SRIOV] capability in the NIC is enabled to maximize performance.

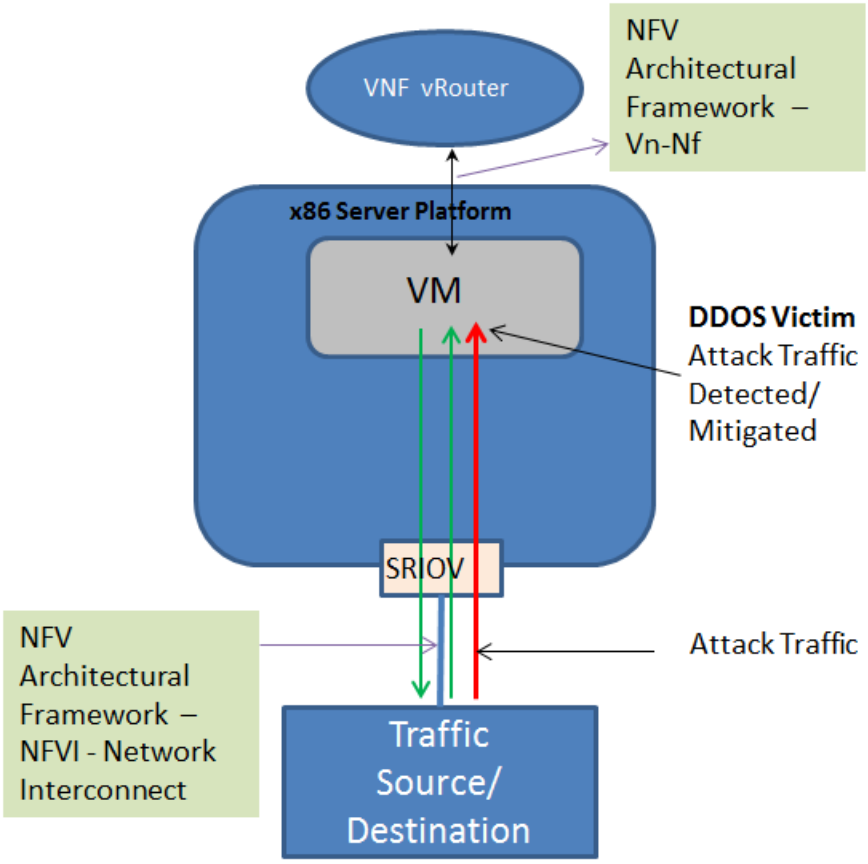

Figure 2: PoC Test Setup

2.3 Mapping to NFV ISG Work

This PoC will demonstrate a VNF using a flexible and scalable platform for rapid innovation. Some of the DDoS detection/mitigation schemes described above could be implemented in specialized hardware. However, challenges include 1) long implementation and verification times 2) lack of flexibility in provisioning for new types of DDoS attacks. 3) lack of flexibility to scale capacity based on performance needs.

The architectural blocks in the NFV reference architecture framework [NFV-ARCH] which are relevant for this PoC are depicted in Figure 3; these are 1) VNF vRouter which is managed by the VNF Manager 2) Virtual Compute and Virtual Network which are part of NFVI.

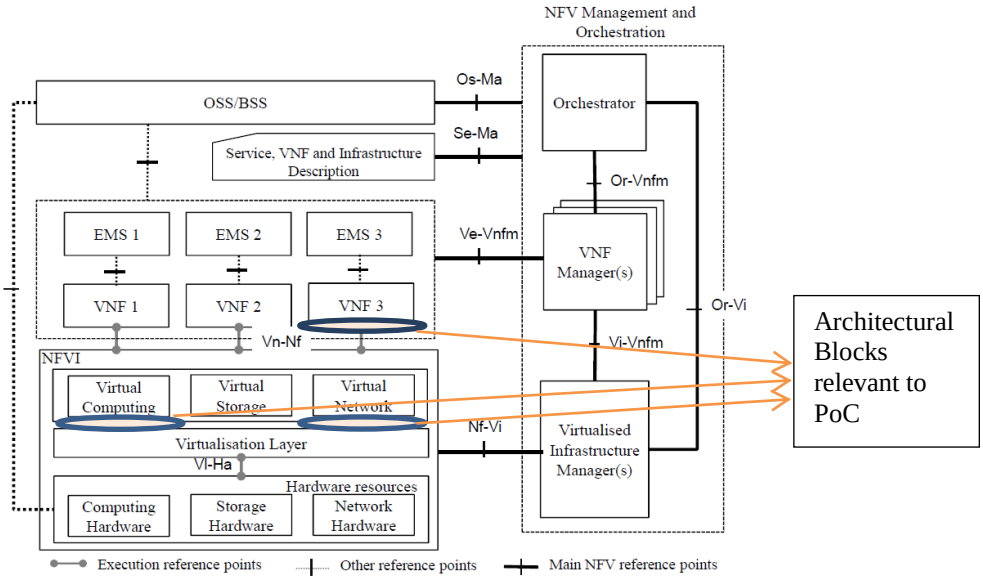

Figure 3: Mapping to NFV Architecture

	Use Case	Requirement	E2E Arch	Comments
Scenario 1	UC#2 VNFaaS		Vn-NF, NFVI	Demonstrates the performance impact and benefits of the Layer 2/3/4 DDoS detection block on packet processing in a VNF vRouter which is part of the vE-CPE service
Scenario 2	UC#2 VNFaaS		Vn-NF, NFVI	Demonstrates the performance impact and benefits of the QoS block used for Layer 2/3/4 DDoS mitigation in a VNF vRouter which is part of the vE-CPE service

2.4 PoC Success Criteria

Our goal is to implement a DDoS scenario using the Brocade virtual router and characterizing performance with DDoS functionality added to the router. Success criteria include demonstrating the concept and collecting performance metrics to understand potential bottlenecks and performance limitations on this virtualized solution.

2.5 Expected PoC Contribution

This PoC is expected to provide the following contributions

- PoC Project Contribution #1: VNF DDoS mitigation (new contribution) to NFV Group SEC EG
- PoC Project Contribution #2: NFV Performance & Portability Best Practises (ETSI GS NFV-PER 001) – VNF as a Service to NFV Group PER EG
- PoC Project Contribution #3: Performance evaluation of a vRouter with intrusion prevention/detection (new contribution) to NFV Group PER EG

3. References

[FDDOS] David Holmes, “The DDoS Threat Spectrum”, F5 White paper 2012

[OPSAWG-large-flow] Krishnan, R. et al., “Mechanisms for Optimal LAG/ECMP Component Link Utilization in Networks,” February 2014.

[I2RS-large-flow] Krishnan, R. et al., “Large Flow Use Cases for I2RS PBR and QoS,” April 2014.

[NIST-CLOUD] Mell, P. et al., “The NIST Definition of Cloud Computing” , September 2011.

[DPDK] Intel®DPDK open source project http://dpdk.org/

[VNFaaS] ETSI GS NFV 001Network Functions Virtualization (NFV); Use Cases
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

[NFV-ARCH] NFV Architectural Framework
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf

[SRIOV] http://www.intel.com/content/dam/doc/application-note/pci-sig-sr-iov-primer-sr-iov-technology-paper.pdf

[NFV-REQ] NFV Virtualization Requirements:
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/004/01.01.01_60/gs_NFV004v010101p.pdf