VNF BOF
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

S. Hares
Huawei

July 4, 2014

Use Cases for Resource Pools with Virtual Network Functions (VNFs) draft-hares-vnf-pool-use-case-02

Abstract

This draft describes use cases the author has observed in demonstrations or deployments for virtualized network functions (VNFs) supported by VNF Pools. Several of these demonstrations combined VNF Pools into VNFsets. The use cases were: cloud bursting, parental controls, load balancer for multipath (L1-L7), WAN optimization that runs either between access nodes and Data Centers, WAN optimization between mobile phones and Data Centers (through access nodes), application placement optimization, and optimized placement of web applications utilizing minimal data transfer.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 5, 2015.

Table of Contents

1. Introduction

This draft focuses on providing one person's observations on the deployment of Virtualized Network Functions which are supported by VNF Pool where the VNF Pools may be grouped into VNF Sets. This version of the draft no longer needs to explain the basic architecture and problems since [I-D.zong-vnfpool-problem-statement] provides an excellent description of the following:

- Terminology of VNF, VNF Pools, elements of VNF Pools, VNF Pool Managers, and VNF Sets;
- Challenges to the reliability of VNFs (without Pools);
- Challenges to reliability within VNFs (redundancy and state synchronization),
- Interactions with Service Control Entity managing the VNF functions
- and the needs for reliable transport

This document simply introduces unique terms, and then describes authors experience the VNF Pools and VNF Managers when the VNF Pools contain only one type of function. The VNF Pools may operate in a

set of VNF Pools. This document no longer examines VNF Set management because is out of the scope of the VNF Charter.

Virtual Network functions supported by Virtual Network Pools and organized into Virtual Sets have been observed to be more reliable and be able to expand (or contract horizontally). By being more reliable, this author observed that individual failures of virtual functions due to software or system constraints (load) were survived by switching over to another NFV function within the VNF Pool. For example, with compatible software functions running, the current and previous software ran a network applications (E.g. open source NAT or open source DPI), a failure on one VNF running the current software could quickly be replaced by a "hot standby" in the Pool running the previous version. Upon increased traffic, one VNF function (for firewalls) could be expanded to multiple firewalls each handling a portion of the traffic. In a sense, the VNF expands horizontally to handle the increased traffic. In the same way, as traffic diminished, this VNF can contract.

This document describes each use case by describing the application and how the VNF function when operating within VNF Pools within the VNF Set that makes up the application. While some of these use cases had multiple VNF Sets, VNF Set management is outside of the scope of the VNF Pool work. Therefore, the explanations have been simplified to consider all the VNF Pools into one set.

One final note, the author knows she has only provided abstract descriptions of these deployments, but out of respect for products and companies the abstract description is best.

2. Terms

The VNF Problem statement [I-D.zong-vnfpool-problem-statement] defines the terms reliability, VNF, VNF Pool, VNF Pool Element, VNF Pool User, VNF Pool Manager, and VNF Set. This draft uses these definitions. The following definitions are not defined within the VNF problem statement: Cloud Bursting, Stateful parental controls, WAN optimization, and application placement. These terms are defined below.

Cloud Bursting: the ability for Virtual processing to burst through the limits of one virtual environment and automatically transfers a portion of the processing to another virtual environment.

Stateful parental controls: the ability for network access devices to have content filters that react to traffic, location, and user. These controls follow the user across multiple access points within a home network, or in a carrier network.

WAN optimization: the ability to optimize traffic across a Wide-Area network. WAN optimization often makes use of TCP FLOW optimizations (with IETF TCP features) and TCP de-duplication of packets,

Application placement: ability for coordinating software to place applications based a combination of compute resources, data storage, network service, and security concerns. Application placement may involve movement of some application data, movement of some applications (data and compute), and movement of network resources to service the applications. One type of network resource movement is the movement of virtual network functions (VNFs) which are defined, created, allocated with resources in a way to provide an integral unit to the application placement control software.

OTT (Over the Top): This industry terms implies an overlay network that is overlaid on existing networks as a virtual network.

Shared risk group (SRG): Shared risk groups occur when different VNFs in a VNF Pool all exist upon the same instance of a virtual form or hypervisor. When a hypervisor fails, all the VNF instances on the same hypervisor will fail,

3. Use Case List

The use cases described in this draft are:

- Cloud Bursting
- stateful parental controls implemented in access nodes and firewalls (stateful and regular)
- load balancer doing multipath (supports L1-L7 optimization),
- WAN optimization between access nodes and Data Centers,
- WAN optimization between mobile phones through access nodes to/ from Data center (E.g Riverbed WAN),
- Application placement optimization using optimized DNS and DCHP VNFs,
- Application placement optimization to minimize data transfer.

The uses cases are done in the order of VNF sets to VNF single operations. The Cloud bursting obviously takes a set of VNF Pools to lift up services in a cloud environment and move these to another cloud environment.

Deployment of VNF functions into critical network functions requires that multiple sources exist to reduce risk of software or hardware issues, and to respond to economic pressure to continually improve while reducing prices. Multi-vendor sources for these VNF, VNF Pools, and VNR sets comes at the price of designing (or adopting an existing) interoperability VNF Pool manager for VNF Pools.

4. Cloud Bursting Use Case

Description:

Three cases of cloud bursting exist. Public clouds adding more resources upon demand. Private clouds adding more resources upon demand from private cloud resources. Private clouds adding more resources from the public cloud. In the public/private cloud, the orchestration system looks within pools of additional resources to fit the request for more resources for a particular time. Verizon provided examples of cloud bursing at ONS 2012, and Terremark utilizes cloud bursing to obtain more resources (http://www.terremark.com/services/it-infrastructure/cloud-services/enterprise-cloud/architecture/) operating over open-source hypervisors (2012, 2013).

VNFs within the VNF Pools operate as management systems and networks router/switches (virtual switches, routers, end systems) to spin up additional transport process (TCP/STCP) and move work jobs via standard interfaces (libvirt, CLI, REST, and JASON), and provide standardized value-added functions. These value-added functions include the following:

- VNFs in VNF Pools of system monitoring and orchestration
- VNF in VNF Pools for virtual firewall to protect the data
- VNF in VNF Pools for DPI or DDOS during
- VNF in VNF specialized DNS that controls private/public cloud move
- VNF in VNF WAN applications that create a large pipeline for for movement of data and applications within Cloud (Private/Public) or between clouds
- VNFs in VNF Pools for smart access to the could

Why VNF in VNF Pools for network router/switch or host system functions

VNFs in VNF Pools allow cloud bursting to temporarily expand horizontally to take the load as the processing groups move between clouds. Each of the functions has a scaling within its own pool which allows the bursts of effort to grab or release the amount of functions. The VNFs doing system monitoring of the move and the orchestration are also included in the features that grab or release functions.

Why VNF Pools:

Bursty nature of action of Cloud Bursting requires being able utilize VNFs within Pools to expand horizontally for the estimated cloud bursting activities. However, if the cloud bursting expands beyond the resources estimated by the orchestration software then the VNFs within the pool can expand the service.

Why Multi-vendor interoperable VNF Pools?:

Cloud bursting is a critical business infrastructure which needs highly reliable software that can be maintained by Cloud operations. Critical infrastructure requires multi-sources. Either the Cloud operations creates a team to maintain VNF Pool software from Open Source code bases, or the equipment vendors provide interoperable VNF Pool Managers and VNF Pools that run across multiple platforms.

5. Stateful Parental Controls

Description:

Parental content filters are targeted filters that are installed based on an identification of a user. When the centralized controller detects the User (via traffic pattern, role identification (ABFAB, HTTP)), an orchestration manager installs the appropriate software to guarantee filters. Two types of security exist: authentication and authorization. In authentication, ACL and other port based filtering is set per customer for the user. This filtering may block, prioritize, or transfer to a black hole recording device different traffic. In authorization, the systems create a web of trust via an identity server (for HTTP 1.0 SAML template defined by OASIS and IETF ABFAB information for non-http).

The following is a list of some of the VNF functions found in VNF Pools in the Stateful Parental Control Model

- VNF Pool for the specialized Access filters

- VNF Pool for open source DPIs (snort, etc.) to find "inappropriate" material,

- VNF Pool for specialized DPI inspection,
- VNF Pool probes on hyper-visors,
- VNF POol for management functions depositing configuration in Open Flow switches, Ethernet Switches, Virtual switches, routers, firewalls, and access nodes.
- VNF Pool for access firewall
- VNF Pool for spam filters for mail
- VNF Pool for DDOS software,
- VNF Pool for DNS/DHCP servers that allow the linking of the the Public services to a instantly created VNFs for specialized access
- VNF Pool to move filters within Cloud (Private/Public) or between clouds in anticipation of the persons movement (If in central London, spread to other access nodes along public transportation (Tube) lines or to hotels.).
- VNF Pool to do additional user identification of the systems

Why VNF Pools

The bursty nature of user access is dependent on the detection of the movement of the user. At the moment the public software identifies the user, this VNF Pool set operates to expand horizontally to provide the necessary service to provide these parental features. The VNF Pools allow groups of these parental ' families to be instantiated.

Why inter-operable VNF Pool Managers

The VNF functions may go between the mobile devices the user moves with (E.g. Android Pad or Android Phone) and the local network systems supported by the Carrier, the hotel, or the airport systems. Inter-operable VNF Pool Managers means that some NVF functions may move from Android Pad /Android Phone to carrier's equipment.

6. Load balancer

Description:

Load balancers (such as Riverbed or Cisco) look to balance traffic in different layers of the stack (L1-L7). SDN meta controllers (OpenDaylight, Vyatta) monitor work with the time-critical OTT

control process (which creates and manages the OTT VPNs (L2/L3/MPLS)) to determine where the load is at any specific time, and to track it over time. The SDN orchestration devices work with the SDN OTT control process to adjust to readjust the load at L1-L7.

The VNF functions that use VNF Pools in the load balancing service are:

- VNFs for network probes in all devices (mobile phone, ipad, access devices, vswitch, vrouter, tcp optimizer, DPI, hypervisors, VMs dumming storage, VMs creating the network;
- VNFs for depositing configuration in Ethernet switches (open-flow or IEEE 802.1), routers, firewalls, access nodes;
- VNFs for firewall;
- VNFs to do Traffic capacity/load balance calculation;
- VNFs running orchestrator monitor/change algorithms; and
- VNFs to users or specific traffic to aid in load balancing.

Why VNF Pools:

True end-to-end Load balancing requires load balancing across multiple layers with VNF pools to support different functions. Multi-vendors solutions will allow meta controllers to balance traffic to reduce costs in networks. Current Enterprise customers find the load balancing operates with TCP WAN optimization to utilize all network bandwidth effectively.

Why inter-operable VNF Pool Managers

Network probes, network traffic capacity calculation, and configuration of changes operate either when traffic thresholds are exceeded or upon period timers. Each of these functions has bursty needs needing the ability to expand horizontally.

Firewalls are traffic based which may be bursty or steady state depending on the application profiles. VNF Pools allow for the horizontal expansion during bursts.

Long lived traffic flows may be identified by looking for users or application traffic patterns. This type of processing function has a "DPI-Like" processing quality that make require quick examination of some data. VNF support in VNF Pools allows the assurance of this type of support

7. Android phone TCP WAN optimization

Description:

Android phones and Android tablets often communicate across the LTE/ WiFi connections. Optimization of the link for the low-bandwidth of LTE or Wifi connections, and the switch between LTE and WiFi requires monitoring of traffic, choosing link, optimizing TCP (Window and removing duplicates).

The VNFs that are aided by VPN Pools in this application includes:

- VNFs for probes in all devices (mobile phone, mobile pads, Wifi enabled nodes, LTE IP RAN notes)
- VNFs for depositing configuration in SDN access nodes (Wifi or LTE)
- VNFs for to handle remote phone parameter adjustments;
- VNFs to do firewalls (E.g traffic not allowed over LTE due to customer policy);
- VNFs for TCP data de-duplication process;
- VNFs for Traffic capacity/load balance calculation (see Football stadium problem below);
- VNFs for best processing of Video traffic or best network to pull Video traffic from;
- VNFs to identify user or user traffic and
- VNFs to interface to secure data processes.

One scenario to consider is the football stadium scenario. A person takes the IPAD to watch the close up replays or send email. During fourth quarter, the person receive an urgent call to go home and walks with the IPAD down the street to the metro-system to return home. On the way, the person is utilizing the IPAD to send mail, watch the football game, and do Skype calls.

This scenario is similar in needs to the parental controls. The differences are TCP data de-duplication to improve WAN traffic and specialized Video traffic handling, plus the mobile phone management and security.

Why VNF Pools:

The football user case illustrates how the network functions are used in bursts. The VNF Pools allow these functions to expand out to fit the users needs. The football example also shows how events can cause massive numbers of these bursty users to occur at the same time. Again, the expansion out for these events without reducing service is key to the quality of user experience for mobile phone or mobile pad users.

Why Inter-operable VPN Pools handled by VPN Pool Managers:

Phones systems do not want a single vendor for all features. Multiple interoperable access nodes and Android pad/tablet implementations require these VNF pools. The football stadium may require that several mobile operators or mobile or cable operators work together to provide this service.

8. SOHO device optimization

Description:

SOHO devices using SDN VM technology must balance traffic movement between small cells (WiFi or femtocells). Access policies must be configured for restriction on this policy.

The VNFs that VNF Pools in this application are:

- VNFs for probes in all devices (mobile phone, mobile pads, WiFi enabled nodes, LTE or femtocells)
- VNFs for VPN to user identification and security.
- VNFs for depositing configuration in access nodes (Wifi, L),
- VNFs for handling remote phone parameter adjustments;
- VNFs for firewall (traffic not allowed over LTE);
- VNFs for TCP data de-duplication process;
- VNFs for Traffic capacity/load balancing over single/multiple soho links;
- VNFs to allow applications load balance across internal soho links based on traffic needs and use policy; and
- VNFs for VPN to user identification and security.

Why VNF Pools:

SOHO devices will have limited resources for handling probes to find local devices, change configurations in access devices, adjust remote phone parameters, firewall traffic, and perform WAN optimization (TCP de-duplication, prioritizing of traffic (like phones) or load balancing). However, SOHOs may only need the probes, configurations changes, and phone adjustments when users arrive into the home. The data related VNF functions will occur as the SOHO office begins to transfer data. The VNF pools allow the VNF function to scale up/down via horizontal expansion.

VPN Pool Growth/Shrinking:

The VPN Pool Manager can handle increasing or decreasing the VNF Pool size. Cooperating VNF Pool Managers can be seen to be useful in this use case, but the cooperating VNF pool managers are outside the scope of the VNF within a VNF Pool.

9. Application Scaling

Description:

Applications may be placed in a variety of hypervisors. The rapid deployment of applications on services may allow millions of applications to be available within the cloud. Creating a effective lookup for the applications or redirecting applications takes an Network Virtual environment that controls DCHP, DNS, and http access rapidly. 2 Million URI references for each access node is possible given the current growth.

VNF within the cloud must scale up to handle the VNF services required by the network infrastructure. This includes the network information functions of DNS, DCHP, URL processing, AAA (Diameter/ Radius). Fast enactment of these network functions allows an on-demand creation of a multi-tenancy overlay (IETF NV03).

The VNFs operate in VNF Pools in this application are:

- VNFs for AAA functions (Diameter, Radius);
- VNFs for DNS functions;
- VNFs for DCHP functions
- VNFs for specialized URL/URI processing;
- VNFs for handling remote probes on these virtual information functions;

- VNFs for handling remote configuration of these virtual information functions;
- VNFs for Traffic capacity/load balance calculation;
- VNFs for determine optimum placement of application (and application's backup services) to optimize CPU compute, storage or data
- VNFs for VPN to user identification and permissions to use data; and

Wny VNF in VNF Pools

User load patterns or access patterns will impact how much load the network information VNF functions (DNS, DHCP, URL processing, AAA (Diameter/Radius) encounter. The VNF Pools with a good VNF Pool manager can spread the load locally or between different systems.

The applications and the application usage will also determine how loaded the VNF Function is that monitors CPU utilization, storage, and network resources. Again, the VNF supported by VNF Pools can expand or shrink horizontally.

The rest of the VNF functions needs for VNF Pools have been described above.

10. IANA Considerations

This document includes no request to IANA.

11. Security Considerations

This document has no security issues as just contains use cases.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

12.2. Informative References

[I-D.zong-vnfpool-problem-statement]
Zong, N., Dunbar, L., Shore, M., Lopez, D., and G. Karagiannis, "Virtualized Network Function (VNF) Pool Problem Statement", draft-zong-vnfpool-problem-statement-06 (work in progress), July 2014.

Author's Address

Susan Hares
Huawei
7453 Hickory Hill
Saline, CA 48176
USA

Email: shares@ndzh.com