Hillstone CloudEdge For Network Function Virtualization (NFV) Solutions

Introduction

With the advancing technologies, business applications and operations naturally have become more dynamic in order to adapt. New applications or business operations are created almost every day. In addition to adding new applications, removing or modifying applications and operations happen at a similar speed. However, traditional hardware-based data centers and networks could not meet the requirements of these highly dynamic changes, as hardware infrastructure cannot be adjusted at the same speed as applications.

Virtualization became the best solution to meet these dynamic requirements. Computing, storage, and network switching have all been virtualized and provided as virtual services, but that does not cover every component in a data center. In traditional networks and data centers, there are many other devices which run at Layer 3 to Layer 7. These devices include firewalls, routers, load balancers and more, and are necessary and critical for customer experience and security.

To virtualize all the network services in a data center, Network Function Virtualization (NFV) was proposed. Under the NFV architecture, all network functions (including L3 to L7) are virtualized. In the conversion from physical to virtual, many critical issues such as performance, compatibility with hypervisor, multitenancy support, and elastic management have had to be resolved.

To ensure networking could meet the demands of highly dynamic business operations, data center operators and network service providers needed to adjust their network service alongside customers' virtual machine (VM) or business applications. Therefore, they first started the trial and production deployments of NFV in specific sectors, such as Virtualized Data Center (VDC), Software Defined Data Center (SDDC), virtual Customer Premises Equipment (vCPE), and virtual Evolved Packet Core (vEPC).

Virtualized Network Function (VNF) is the basic building block in the NFV architecture. When the router, firewall, IPS and WAF devices are virtualized, they become a VNF. As a security solution provider, Hillstone Networks has been actively working on providing VNF solutions for NFV deployments.

This white paper provides an in-depth discussion on challenges to overcome when providing a VNF module for NFV architecture and VNF solutions from Hillstone Networks.

Challenges in VNF Implementations

The major functional differences between traditional network functions and virtualized network functions reside in the following areas:

- Self-service
- Self-configuration
- Elasticity

In addition, virtualized functions must provide a northbound API to be integrated by higher level management software.

Key features required by NFV architecture on VNF are discussed in the following sections.

Automatic Deployment and Compatibility

Automatic deployment and configuration are necessary to enable and support self-service and self-management. Without the intervention of data center administrators, customers or tenants should be able to achieve self-service and self-management, similar to the services provided by public clouds such as AWS, Azure, or other cloud providers.

Deployment using image or template

VNF has to provide VM image or deployment templates to achieve rapid deployment when customers need to start a new service quickly to address a business demand.

Support for multiple cloud platforms

Hybrid-cloud and heterogeneous-cloud services will stay in business for a long time. On the management side, cloud management platforms are capable of managing multiple cloud platforms. For example, one management platform can manage a VMware data center, an OpenStack data center, and AWS as well. To provide a single solution to a cloud operator, VNF has to support multiple cloud platforms, which usually include VMware, OpenStack, AWS, Azure, Ali Cloud, among others.

Embedded automatic configuration

After being deployed through one single VM image or template, multiple VNF instances will contain the same configurations, such as interface IP, route, username, or password. This makes them unusable by multiple customers or tenants. It is necessary to automatically customize certain configurations after a VNF is deployed.

There are multiple approaches to implement an automatic configuration, like updating the configuration file before VNF boots up, embedding a startup agent (VMware and Azure), or reading a user specific configuration (AWS and OpenStack) during boots up.

Scalability and Elasticity

Since business applications and operations may change over time through expansion or reduction, services provided by VNF must scale up or down as necessary.

To provide the above scalability, VNF needs to provide overall performance scaling by adjusting virtual resources (virtual CPU and memory) on a single VNF VM, and avoid redeploying it. Similar performance scalability requirements are also applied on VNF network interfaces. The VNF interface has to support Single Root I/O Virtualization (SR-IOV) and hot plug-and-play.

If certain features or the performance of VNF are controlled by a license, license management has to be scalable as well; otherwise it will block performance scaling.

Open API and Software Orchestration

VNF module is managed by other orchestration software. The orchestration software can be NFV Management and Orchestration (MANO) software or VNF Manager (VNFM).Orchestration software includes OPEN-O, OSM, Tacker, etc. Since SDN does not follow the standard defined by European Telecommunications Standards Institute (ETSI), it is not classified as NFV orchestration software. The management software is capable of orchestrating multiple types of, and multiple instances of NFV modules through a centralized console. It not only supports the daily operations of a cloud administrator, but also implements service chains and ensures continuous deployment and upgrades.

Since the orchestration software needs to configure VNF and manage its execution, VNF needs to provide the northbound interface for upper management software, like SOAP, XML or REST API.

VNF Solution from Hillstone Networks

The goal of NFV is to improve the efficiency of deploying new services and adjusting existing services to meet the demands of highly dynamic business operations. Compatibility, elasticity, high performance, and open API are all crucial to an NFV solution. Besides the above features, automatic orchestration and license management are also key functions in the service orchestration process. Orchestration ensures each VNF module can be deployed and configured automatically, including initial and customized configuration based on each specific service. License management ensures VNF modules can automatically enter operation mode.

How Hillstone NFV solutions address these requirements is discussed in the following sections.

Hillstone VNF is Highly Compatible

Hillstone provides a highly compatible virtual firewall, which can support four major hypervisors: ESXi, KVM, Hyper-V, and Xen server.

Hillstone's VNF solution also supports multiple cloud platforms, including VMware, OpenStack, AWS, Azure, and Ali Cloud. It has been integrated into the cloud solutions from multiple cloud providers, like 99cloud (OpenStack Gold Member), EasyStack (OpenStack Gold Member), ZTE, Inspur, and HUAWEI.

Figure 1 shows the partners and compatible cloud providers of Hillstone VNF.

Figure 1. Partners and compatible cloud providers

Automatic Deployment and Initial Configuration

For different cloud platforms, Hillstone provides multiple formats of VNF images (ova, vhd, qcow2) to meet various customer requirements. Virtual resources for the virtual firewall have been pre-configured to ensure a fast and successful deployment.

An embedded agent is used to retrieve the initial configuration during the boot-up process to customize each VNF module based on customer requirements. Hillstone has integrated vmtools, cloud-init, Qemu Guest Agent into the VNF module. With embedded agents, the interface IP, route, username, and password can be injected into the VNF during the module boot up process.

Automatic License Management

After the automatic deployment and initial configuration is complete, the VNF module is not yet fully functional because its features are also controlled via a license. To ensure VNF modules can closely follow user requirements to start, adjust, or shut down, license management also needs to implement automatic dispatch and recycle mechanisms.

Hillstone released the License Management Server (LSM) to provide a license management solution for VNF deployments. When a Hillstone VNF module requires a license during start up, it will connect to the LSM. The LSM can assign certain licenses to the module based on pre-configured rules. When VNF's configuration needs to be adjusted to meet user requirements, it can get updated licenses from LSM. When a VNF completes its service and is being terminated, LSM can recycle its licenses and the licenses can subsequently be re-assigned to other VNF modules.

With the help of LSM, licenses are automatically assigned or recycled whenever the VNF module starts, adjusts, or terminates. This ensures network services scale along with customer requirements.

Elasticity and High Performance

Besides scaling out by automatically deploying more VNF modules, a single VNF module is also capable of scaling up to meet the requirement based on network topology changes and performance.

When new virtual networks are created based on a business need through the interface plug-and-play feature, a single VNF module can provide more network interfaces at run-time to connect to newly created VM virtual networks.

Hillstone VNF also provides the capability to automatically adjust virtual resources. Without re-deploying the VNF module, more resources can be utilized after new resources (vCPU and memory) are assigned and a new license with higher capacity is loaded.

Increasing virtual resources (like vCPU and memory) can help to increase the VNF performance to a certain extent. When this approach reaches its limit, VNF can enable the support of SR-IOV and further improve the interface throughput close to line rate.

REST API

Customers typically need to manage multiple types of network services from cloud platforms to fulfill business requirements. To improve the user experience and reduce operational complexity, cloud service providers usually provide a single management portal and integrate management and configuration on multiple virtual services and resources on that portal. To be managed and configured by the management portal, the VNF module has to provide northbound interface to upper level management software. Thus a cloud user can manage all services from a single portal.

REST API is a popular interface standard, and major cloud management platforms (AWS, Azure, and OpenStack) support it. To integrate with a cloud management platform or other types of management software, Hillstone VNF provides REST API for module management and service configuration. Through REST API, cloud service providers can push configurations to VNF modules and provide a self-management service to cloud users through its management portal.

Currently, Hillstone VNF REST API supports system configuration, security policy configuration, interfaces and network configurations. Figure 2 shows a portion of the Hillstone VNF REST API specification.

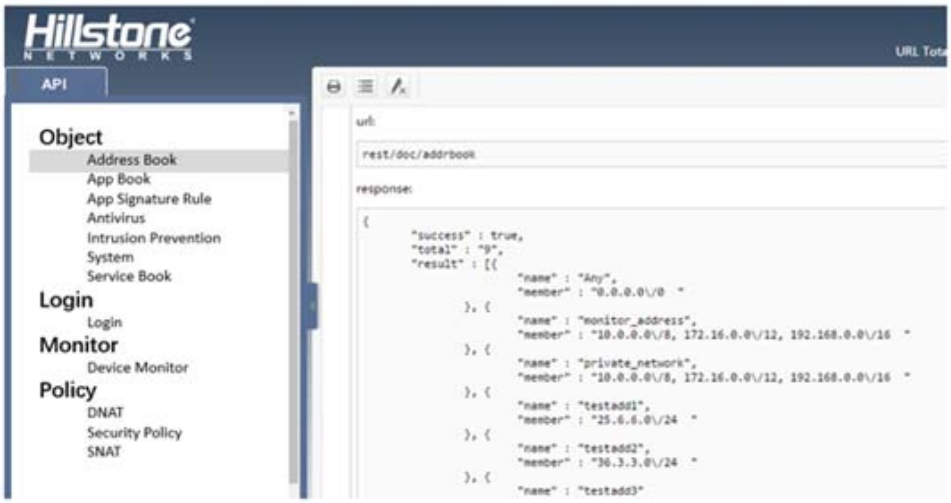

Figure 2. Hillstone VNF REST API specification

NFV Orchestration

In the standard NFV framework from ETSI, NFVO uses VNFM to orchestrate VNF services. VNFM uses info from VNFD to request resources from VIM, deploy VNF, and manage virtual networks. Figure 3 shows the standard ETSI NFV framework.

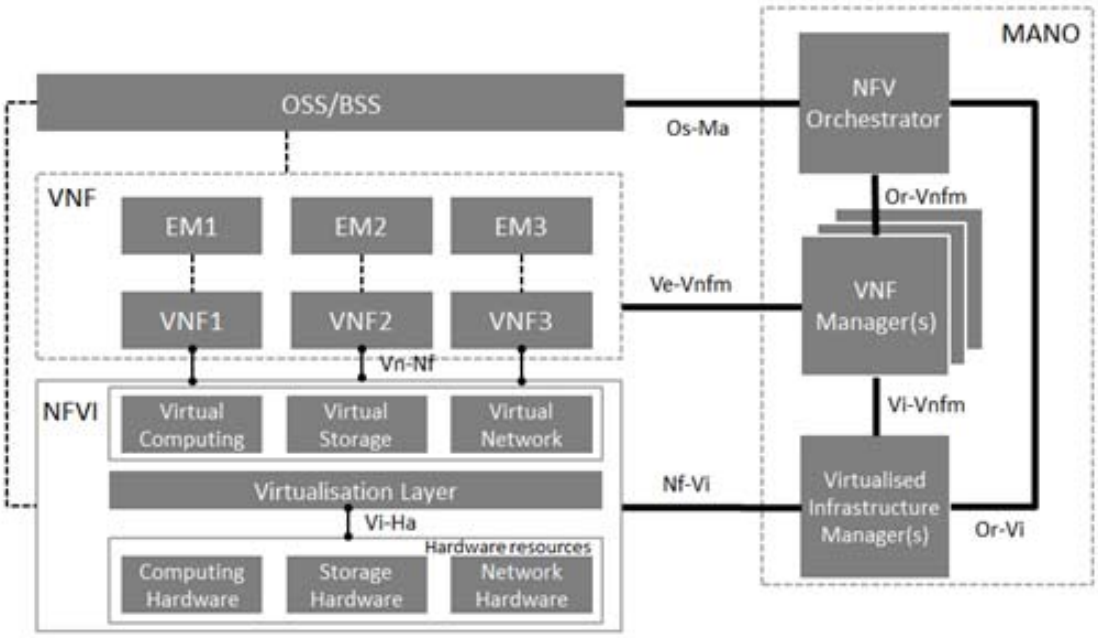

Figure 3. ETSI NFV framework

However, in real world customer environments, because of the differences in underlying technologies and levels of operation, cloud infrastructures may not strictly follow the above NFV framework. To best fit into customers' environments and reduce challenges in deployment and integration, Hillstone provides three types of NFV orchestration solutions, outlined below.

- Orchestration based on cloud platform

In this approach, Hillstone VNF integrates with a cloud platform or cloud management platform. With minor integration efforts, cloud operators can manage and configure Hillstone VNF from existing management frameworks.

Hillstone provides multiple types of VM images to support different types of hypervisors, LSM to support automatic license management, and an embedded agent to support automatic customized configurations. Hillstone also provides a management agent, which can integrate with a cloud management platform and provide an API interface for advanced integration.

Hillstone VNF has been orchestrated by vCenter and OpenStack with this approach, and also integrated with 3rd party cloud platforms through a similar approach. For example, Hillstone VNF has been integrated into HUAWEI cloud orchestration, and allows HUAWEI cloud to manage VNF life cycle and configuration.

Figure 4 shows the block diagram of orchestration based on cloud platform.

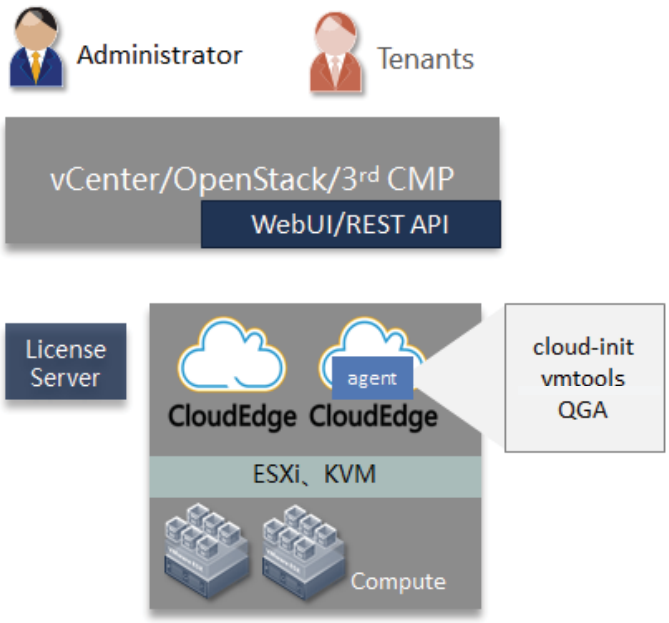

Figure 4. Orchestration based on cloud platform

- Orchestration based on OpenStack FWaaS Plugin

Hillstone VNF module can be integrated with OpenStack Firewall as a Service (FWaaS) plugin and can be managed by FWaaS plugin. In this solution, Hillstone Networks provides a new component, virtual Service Orchestration Module (vSOM). Under an OpenStack deployment, in the process of creating a vrouter or firewall, a vSOM, HillstoneNetworks-L3-agent or HillstoneNetworks-FWaaS-driver can initiate a Hillstone VNF module to act as the vrouter or firewall, to replace the native vrouter or iptables based firewall.

With this approach, the workflows of vrouter and FWaaS creation remain the same, and can be managed from the native OpenStack management portal, Horizon. Hillstone VNF achieves seamless integration with OpenStack through minimum change on the OpenStack management platform. Figure 5 shows the framework for this integration approach.

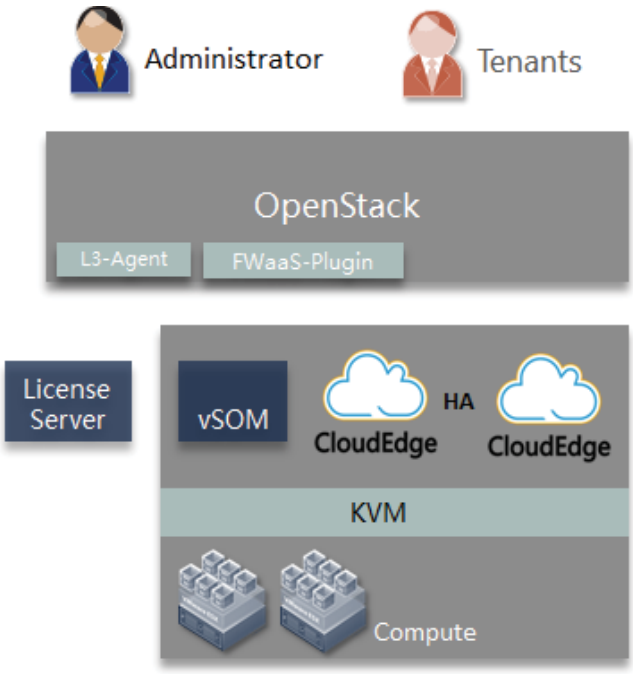

Figure 5. Orchestration based on OpenStack FWaaS

- Orchestration based on open source MANO

Multiple open source MANO solutions (OPEN-O, OSM, Tacker, etc.) are available in the market. By using an open source MANO solution, cloud service providers can implement more flexible orchestration solutions. They also can do further development to meet the needs of their business or customers.

Topology and Orchestration Specification for Cloud Applications (TOSCA), is an OASIS standard language used to describe a topology of cloud based web services, their components, relationships, and the processes that manage them. Many NFV/VNF vendors follow and use TOSCA to describe and specify a Virtual Network Function Descriptor (VNFD). Specified with TOCSA and working with open source MANO, VNFD orchestrates service modules from disparate vendors. This approach ensures NFV services from different vendors are fully decoupled.

Hillstone provides a TOSCA based VNFD template for its VNF module. Through the orchestration of open source MANO, Hillstone VNF can be deployed as a standalone module, a pair with high availability, or one module in Service Function Chaining (SFC). This approach follows ETSI standard and is the ideal solution for NFV orchestration.

Figure 6 shows portions of Hillstone VNFD and VNFFGD.

VNFD Template

```
tosca_definitions_version: tosca_simple_profile_for_nfv_1_0_0

description: waf example

metadata:
  template_name: sample-tosca-vnfd

topology_template:
  node_templates:
    VDU1:
      type: tosca.nodes.nfv.VDU.Tacker
      properties:
        image: vfw
        flavor: vfw
        availability_zone: nova
        mgmt_driver: noop
        config: |
        user_data_format: RAW
        user_data: |
          #cloud-config
          chpasswd:
             list:
                 hillstone: Hillstone@123
          runcmd:
             - ips sigset waf_http template http
             - web-server default
             - sql-injection-check enable sensitive low action log-only
```

VNFFGD Template

```
description: Sample VNFFG template
imports:
- /usr/local/lib/python2.7/dist-packages/tacker/vnfm/tosca/lib/tacker_defs.yaml
- /usr/local/lib/python2.7/dist-packages/tacker/vnfm/tosca/lib/tacker_nfv_defs.yaml
topology_template:
  description: Sample VNFFG template
  groups:
    VNFFG1:
      description: EXT to WEB
      members:
      - forwarding_path1
      properties:
        connection_point:
        - CP11
        - CP21
        constituent_vnfs:
        - waf
        - slb
        dependent_virtual_link:
        - VL11
        - VL21
        number_of_endpoints: 5
        vendor: tacker
        version: 1.0
      type: tosca.groups.nfv.VNFFG
  node_templates:
    forwarding_path1:
      description: creates path (gateway->waf->slb->servers)
      properties:
```

Figure 6. Hillstone VNF VNFD and VNFFGD template samples

Figure 7 shows the block diagram of orchestration based on open source MANO.

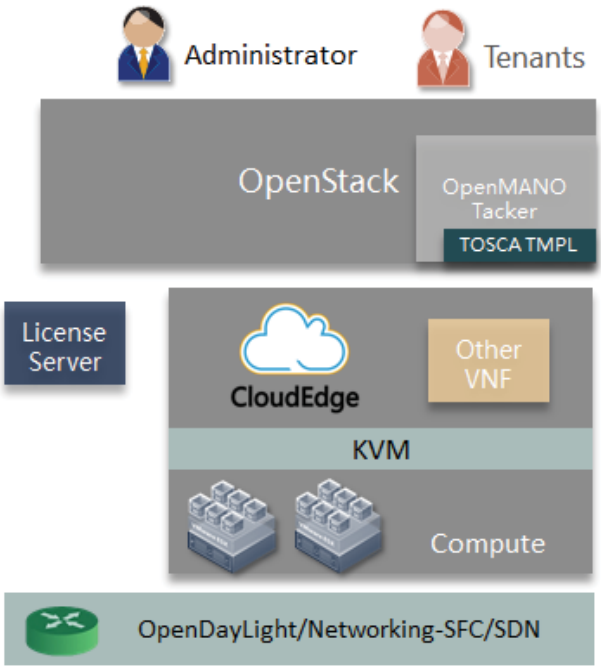

Figure 7. Orchestration based on open source MANO

Customer Success Stories

Hillstone CloudEdge is a virtual firewall VNF solution for NFV deployment. Hillstone Networks has a long-standing and extensive partnership with cloud service providers in developing and enhancing this solution. Real customer deployments and Proof of Concept (PoC) cases of Hillstone CloudEdge are described in the following sections:

Use case 1: Protecting North-South Traffic on Cloud Platform

A major cloud service provider integrates Hillstone CloudEdge with embedded vmtools into its cloud platform. Through CloudEdge REST API, the cloud management platform integrates the CloudEdge security policy configuration into its existing management user interface and provides unified management to its customer. From its management portal, customers can configure and apply NAT rules, security policies, and access control rules to Hillstone CloudEdge .

Use case 2: Orchestration through HEAT

One OpenStack integrator (OpenStack Gold Member) integrates Hilltone CloudEdge with embedded cloud-init into its OpenStack solution. CloudEdge image is initiated through a HEAT template and customized configurations are sent to CloudEdge through REST API.

Use case 3: Replace vrouter in OpenStack Deployment

In a vertical cloud designed for one province in China, the cloud service provider integrates Hillstone CloudEdge through an OpenStack FWaaS plugin. Hillstone Networks-L3-agent converts firewall policies received from the cloud management platform to the Hillstone policy format, and pushes the policies into the CloudEdge module. When a user/tenant creates a new Layer 3 network on the cloud management platform, the Hillstone CloudEdge is automatically created or configured to act as a vrouter for the network.

Use case 4: Replacing OpenStack Native Firewall

A level one Telco in China is designing an internal data center based on an NFV architecture. OpenStack is chosen to be used as the VIM. Their home-grown orchestration software manages both SDN and Hillstone CloudEdge modules. Hillstone CloudEdge is used to replace the OpenStack native firewall. HillstoneNetworks-FWaaS-driver is used to achieve automatic deployment, convert FWaaS policy to the Hillstone policy format, and build service chains along with SDN controller.

Conclusion

NFV is a favorite choice in the path of transforming traditional networks to virtualized networks. Now both traditional network device vendors and traditional network service providers are starting to upgrade or converge to NFV. The complete NFV solution requires deploying multiple different types of, as well as many VNF modules. This type of deployment is typically complex and requires complete automatic orchestration support.

Hillstone Networks has been actively working in the area of cloud computing. Hillstone CloudEdge provides multiple integration solutions for various cloud platforms and has been deployed into multiple test and production cloud environments to serve multiple industries and customer requirements. Hillstone will continue to invest in cloud computing and develop solutions for hybrid-cloud and heterogeneous clouds, to continue to deliver ever more flexible, user-friendly, and robust solutions to the market.

Hillstone™
NETWORKS

How to contact Hillstone Networks

Americas: +1-408-508-6750 | SEA: +65-6678-7660

Europe: +420-721-125-070 | MEA: +971-4557-1493

Email: inquiry@Hillstonenet.com