Orchestrating Advanced Networking and Security Services for OpenStack-Based Clouds

Data centers and clouds are turning to virtualization, software-defined abstractions and orchestration to deliver elastic and responsive infrastructure to business teams. OpenStack provides an innovative infrastructure-as-a-service (IaaS) management and orchestration platform for private and public cloud computing that provides the flexibility of open-source software without proprietary vendor lock-in.

OpenStack goes beyond individual infrastructure elements such as OpenStack Nova for compute, and OpenStack Neutron for networking, instead integrating them together in a holistic view. The need is increasing from carrier and service providers as well as enterprises for tighter integration of network and security within their OpenStack production environments.

Fortinet’s Software-Defined Network Security (SNDS) framework provides the foundation for security automation and integration of not just software-defined networking (SDN) and network virtualization, but also hypervisors for server virtualization and cloud computing in Software-Defined Data Centers. The integration of OpenStack Neutron, the networking-as-a-service framework within the OpenStack architecture, with Fortinet’s leading data center security provides best-in-class advanced networking and security while avoiding performance bottlenecks and limitations.

Delivering Security and Performance at Scale

Neutron is the OpenStack project that provides networking-as-a-service between interface devices (e.g., vNICs) managed by other OpenStack services such as Nova (compute). The FortiGate Connector for OpenStack Neutron enables a FortiGate appliance to operate as an OpenStack Neutron network node and delivers the best of both worlds in advanced security and network performance. The combined solution leverages high-speed hardware ASIC’s in physical appliances to boost the Neutron performance and create security chokepoints to offer the best in class advanced security in one.

Running an external firewall appliance enables higher throughput and lower latency than running virtual firewalls on a Nova compute node (virtualization host). The solution takes the SDNS security approach by integrating the FortiGate appliance via OpenStack Neutron plugins and streamlining OpenStack network security orchestration.

Benefits

- Automated network security with openness and flexibility of leading open and community-driven OpenStack Neutron platform
- Cloud-oriented OpenStack network architecture with Nova compute enables seamless protection of elastic applications and workloads
- Multi-tenant-aware provisioning and delegation to accelerate service delivery and reduce administration costs
- Consolidated platform for advanced networking and security services with ASIC acceleration to eliminate performance bottlenecks
- Single pane-of-glass visibility and control through OpenStack Horizon dashboard and control node orchestration
Auto-Scaling Cloud Workloads
With a tight integration of Neutron network provisioning with workload instances (i.e. virtual machines) spun up in Nova, organizations can easily deploy highly elastic web and SaaS applications to rapidly and more easily connect with end-users, customers, and partners while ensuring confidentiality and compliance. Seamless automated provisioning of Fortinet’s firewall, intrusion prevention, and other Layer-7 enforcement as workloads spin up and down with varying end-user demand ensures user and data privacy, minimizing data breaches and resulting loss of trust.

Multi-Tenant Provisioning
Integration of Fortinet’s patented Virtual Domain (VDOM) technology with OpenStack orchestration enables network isolation and segmentation between business units or tenants. Network security policies can be effectively managed at scale by providing administrative autonomy and delegated authority between segments.

Virtual Segmentation
Enterprises can apply effective security policies by segmenting both by departments or business units and by application type. Administrators can tailor targeted policies by domain to increase security effectiveness while simultaneously improving overall system performance. This unique capability enabled by VDOM integration with OpenStack is unmatched by other security vendors.

Scalable Security-as-a-Service
Cloud providers, service providers, and managed security service providers (MSSP’s) can differentiate their offerings by integrating security-as-a-service capabilities into their cloud or managed services. OpenStack orchestration enables providers to add value and manageably deploy Firewall-as-a-Service (FWaaS), VPNaaS and other Security-as-a-Service as part of an IaaS platform, for Network Function Virtualization, or as a standalone service.

Integrating Security with OpenStack Neutron
The FortiGate Connector for OpenStack Neutron embraces the OpenStack modular architecture to consolidate network and security services using FortiGate firewall appliances, facilitating scalability and elasticity. It makes network services available to OpenStack users by directing Neutron requests to FortiGate physical appliances and leveraging the high performance of ASICs. The FortiGate Connector for OpenStack Neutron delivers Layer 2/3/DHCP/NAT functions on the underlying physical device by transforming these network services through Neutron Network node standardized ML2 and FWaaS integration.

The solution replaces the OpenStack Neutron network node with FortiGate appliances where network and security is combined as one simplified node and supports multi-segment Layer 2 networks in heterogeneous network configurations. The FortiGate appliance behaves as DHCP server, Layer 3 router and Layer 2 switch and becomes the common gateway for the traffic into and out of the cloud instance (north-south bound) and between application tiers. It can also help switch and forward traffic among the Nova compute nodes if needed.

Summary
Security is sometimes referred to as a weak link in the OpenStack architecture, with users having to figure out their own security approaches. Cloud architects deploying OpenStack have the option to integrate and leverage FortiGate’s next-generation firewall to deliver advanced security and control of traffic for private, public and hybrid clouds. The FortiGate Connector for OpenStack Neutron realizes the vision of Fortinet’s Software-Defined Network Security (SDNS) framework (SDNS Framework) by providing management, security orchestration and traffic routing in a seamless package.