Oracle SDN

Virtual Network Services
Oracle’s Virtual Network Services is a new feature of Oracle SDN that virtualizes network functions such as firewall, load balancer, router, virtual private network (VPN), and network address translation (NAT) and makes them available in a single virtual instance. With the capability of Virtual Network Services, Oracle SDN is uniquely able to unify InfiniBand and Ethernet fabrics, allowing end-to-end provisioning of network infrastructure from a single management framework. The network services are daisy chained in a single virtual instance with the flexibility to deploy all or a subset of the services. Furthermore, from the unified management framework, these network services can be provisioned on-demand per tenant.

Frequently Asked Questions

Q: What network services are supported with Virtual Network Services?
A: Firewall, NAT, load balancing, VPN, and routing features are supported. Additionally, the high-availability (HA) feature using virtual router redundancy protocol (VRRP) is supported.

Q: Are there system prerequisites for installing Virtual Network Services?
A: The Virtual Networking Services feature is integrated into the Oracle SDN package with the latest package available on My Oracle Support (MOS). The system requirements are:

i. OS: Oracle Linux 6 (64 bits) Update 5 or Oracle Solaris 11.2.8
ii. Newer x86 processors
iii. Memory: 2 GB minimum
iv. vCPU: 1 to 4

On the virtual instance where Virtual Network Services will be installed, all the virtual network interface cards (vNICs) have to be created and their IP address assignments have to be completed prior to installing Virtual Network Services. After Virtual Network Services is installed, the application starts running and is ready to be managed from Oracle Fabric Manager.

Q: Can new vNICs and vCPUs be added at runtime to the virtual instance in which Virtual Network Services is running?
A: No. The dynamic allocation of vNICs and vCPUs to the virtual instance in which Virtual Network Services is running is not allowed. All the vNIC and vCPU allocations have to be static and completed prior to starting the Virtual Network Services application.

Q: How is Virtual Network Services managed?
A: Virtual Network Services is managed from Oracle Fabric Manager (minimum version is 4.3.1). Oracle Fabric
Manager comes with the Virtual Network Services management plug-in built into it. One Virtual Network Services instance (two in case HA is configured) is created per tenant, and the tenant-specific network services are managed through Oracle Fabric Manager.

Additionally, these services can be provisioned through Oracle Fabric Manager's command-line interface (CLI) as well.

Q: How are the various network services configured and deployed?
A: The network services can be configured and deployed on demand through Oracle Fabric Manager. Connect to the virtual instance on which the Virtual Network Services application is running, from the Oracle Fabric Manager and set up HA (optional) backup Virtual Network Services on another virtual instance. Then the various network services per tenant are enabled/disabled/reconfigured dynamically.

Q: Is there role-based access control (RBAC) support?
A: Yes, role-based access control is supported using the resource domains within Oracle Fabric Manager. In a multitenant deployment, each tenant has visibility only to the tenant’s Virtual Network Services instances. The “admin” role has visibility to all of the tenants’ Virtual Network Services instances.

Q: Is it possible to configure only firewall or load balancer services?
A: Within the tenant’s Virtual Network Services instance, the network services are daisy chained. It is possible to configure all the network services or a subset of them depending on tenant requirements. The services that are not required/not configured are treated as a “no-op” in the daisy chain.

Q: Are dynamic routing protocols supported with Virtual Network Services?
A: The first release does not support dynamic routing protocols. Only static routing is supported.

Q: Is site-to-site VPN supported?
A: Both site-to-site and remote access VPN over IPSec are supported.

Q: What encryption is supported with VPN?
A: Encryption: DES, 3DES, Blowfish, AES128, AES192, AES256
Authentication: MD5, SHA1, SHA256