ORACLE
NETWORKING

Oracle SDN Virtual Network Services Overview

ORACLE WHITE PAPER | AUGUST 2016

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Introduction

An easy-to-access computing utility, with on-demand compute, storage, and network resources, has always been the promise of cloud computing. While server and storage virtualization technologies have been available for some time, network virtualization now adds another dimension of agility and scalability to cloud infrastructures.

By virtualizing the network, the enterprise data center avoids having to configure fixed network silos with specialized service appliances. Instead, the network, subnetworks, and network services can be configured and reconfigured as needed in software. In a cloud-enabled data center, essential network functions, such as firewalls, network address translation (NAT), load balancing, and virtual private network (VPN), must be as virtualized as compute and storage resources. Oracle SDN virtual network services fulfill this requirement.

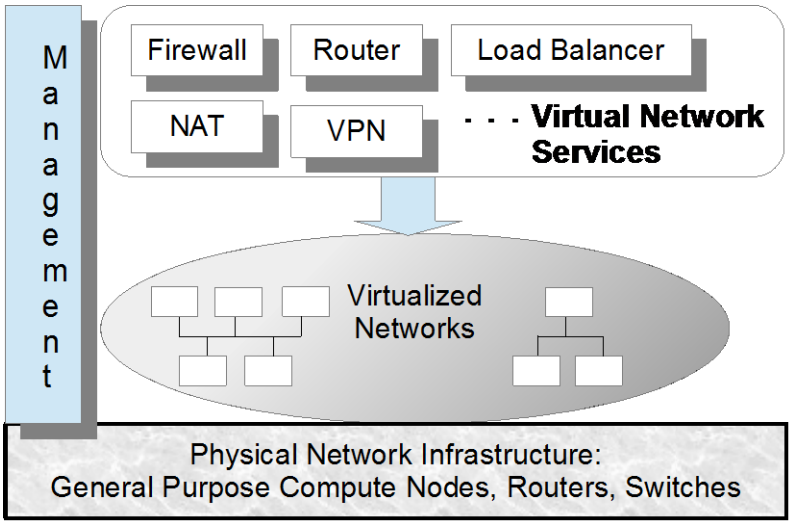

Figure 1. network service virtualization

This document provides an overview of Oracle SDN virtual network services. It highlights key features and describes virtual functions and example use cases.

Oracle SDN Virtual Network Services

Virtual network services (VNS), part of Oracle SDN, are application software that deploys firewall, load balancing, routing, VPN, and other on-demand network functions, from a single virtual machine (VM) compute node. Virtualizing network services in software eliminates the need for costly physical, proprietary, fixed network appliances that lack the flexibility and scalability needed for cloud-enabled data centers. Oracle's VNS provides a set of fundamental fabric network functions independent of the transport media and agnostic to the underlying hypervisor. This enables virtualized network services over any existing hypervisor technology, thereby creating a uniquely agile and elastic network infrastructure for the entire data center.

Oracle SDN virtual network services comprises two software components, the virtual network services application, and Oracle Fabric Manager.

Virtual network services install on a guest VM running Oracle Linux Update 6 or Oracle Solaris 11.3 from a package (.rpm for Linux and .p5p for Oracle Solaris). Once installed into a guest VM, that VM becomes a virtual network services gateway (see the following section for details) that can provide all network functions to all networks and individual hosts that have access to the gateway. A typical configuration of the virtual network gateway has multiple virtual network interfaces (VIFs), with one connected to a public network while one or more are connected to private networks, along with a management VIF connected to the management network running Oracle Fabric Manager.

Oracle Fabric Manager installs as a separate package on either Oracle Linux or Oracle Solaris. The VNS management capability is built into Oracle Fabric Manager 5.0.0 or later. Once installed, user can setup and manage the network functions on their virtual network through the Oracle Fabric Manager graphical user interface (GUI) or command-line interface (CLI).

Virtual Network Services Gateway

Typically, network services, such as firewalls and routers, are deployed using a physical network gateway device. Virtualizing network services on a virtual machine creates a virtual network appliance equipped to provide those essential network functions (see Figure 2). This virtual network appliance can be configured as a network gateway within the virtualized network infrastructure. Each subnet that connects to the network gateway automatically has access to all the network functions provided by virtual network services.

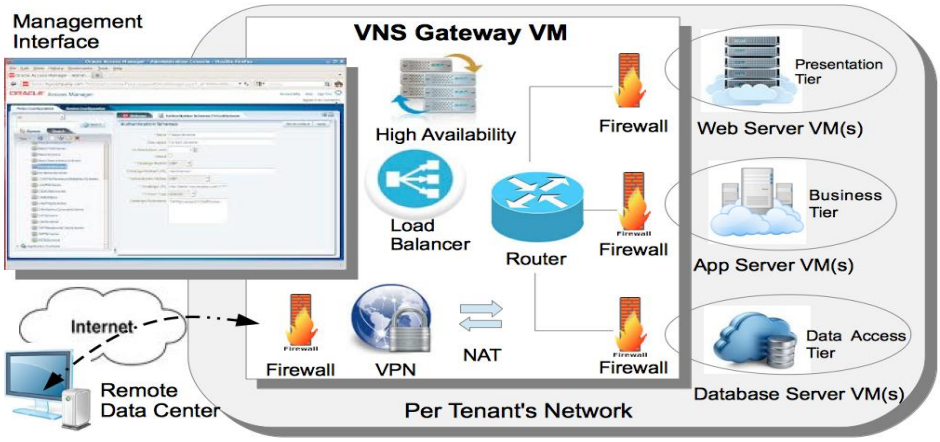

Figure 2. Virtual network services gateway

Multi-Instances for Security and Scalability

A major concern for any enterprise network is the ability to maintain secure isolation between users in an environment where resources are shared among multiple users in a cloud. Individual network data paths need to be separated so that traffic cannot be misdirected or intercepted. Oracle VNS enables secure separation by allowing each user of a tenant resource pool to instantiate one or more of their own virtual network gateways. This gives each tenant complete control over the choice of network functions and how they are used. Since VNS runs in a VM, resources such as virtual CPU and storage dedicated for running VNS are also isolated among tenants—the tenant's entire compute, storage, and network are in a contained and isolated environment. As new tenants are added to the network, more virtual network gateway instances can be added easily, scaling up to an unlimited number of tenants, each with access to its own customized set of network functions, and without rewiring or acquiring additional physical network appliances. Figure 3 shows an example of three tenant domains sharing a pool of compute nodes and network fabric hardware, each with their own unique virtual network gateway configuration. Tenant 1 consists of a single subnet with one dedicated VM hosting a VNS instance. VNS provides network services on north/south traffic between the external network and the private subnet. Each virtual network interface (shown in Figure3 as VIF) is an IP interface to a subnet. Tenant 2 consists of two subnets with one dedicated VM hosting a VNS instance. Here VNS provides network services for both north/south and east/west (between two private subnets) traffic. Tenant 3 has multiple subnets with two VMs dedicated for VNS (one VNS instance on each VM). Tenants' networks span multiple physical servers (not shown in the diagram)

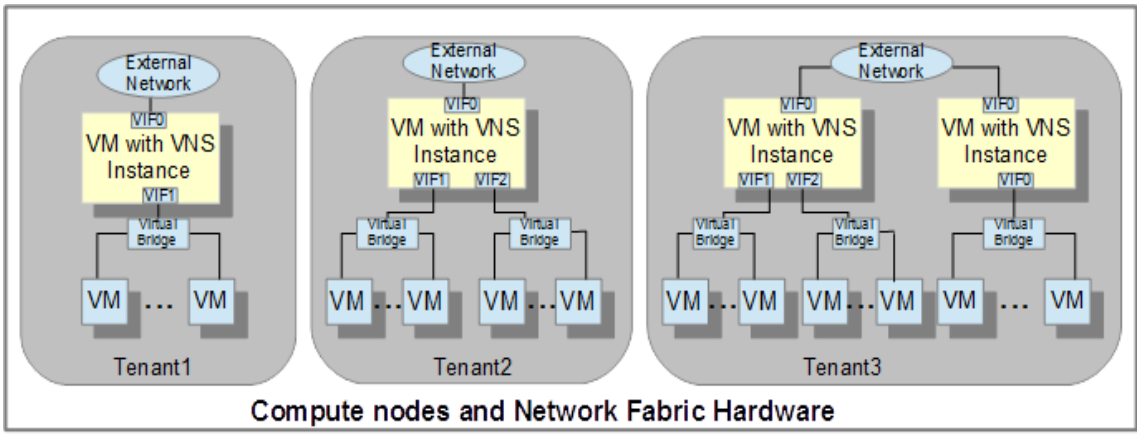

Figure 3. Virtual network services in multitenancy Environment

Architected for Flexibility and Performance

Most virtual network services have dependencies on the hypervisors or the underlying framework that supports them. Also, a network service might require chaining multiple VMs together, providing one service per VM. With multiple network services, traffic needs to traverse multiple VMs and many framework layers.

Oracle SDN virtual network services avoid this complexity. It is designed to be independent of the hypervisor, which means that a guest VM within any VM environment can host VNS, and all network functions are prechained into a service pipeline designed to optimize performance. Packets enter and exit each network function of the pipeline without copying, which greatly improves performance. Each network function in the pipeline is controlled by an "on-off switch" that the user can simply "flip" to enable or disable that particular function. A function that is disabled in the chain bypasses packets without any overhead. Since the pipeline is driven by a single VM, no extra compute node resources are needed for multiple network services. As more services are configured, performance is scaled by increasing the number of CPUs for the VM.

Figure 4 shows two VNS instances with different services on demand. In Instance 1, all services are enabled. All traffic goes through all services for processing. In Instance 2, only firewall service and routing service are enabled. Traffic goes through firewall and routing services and bypasses all others.

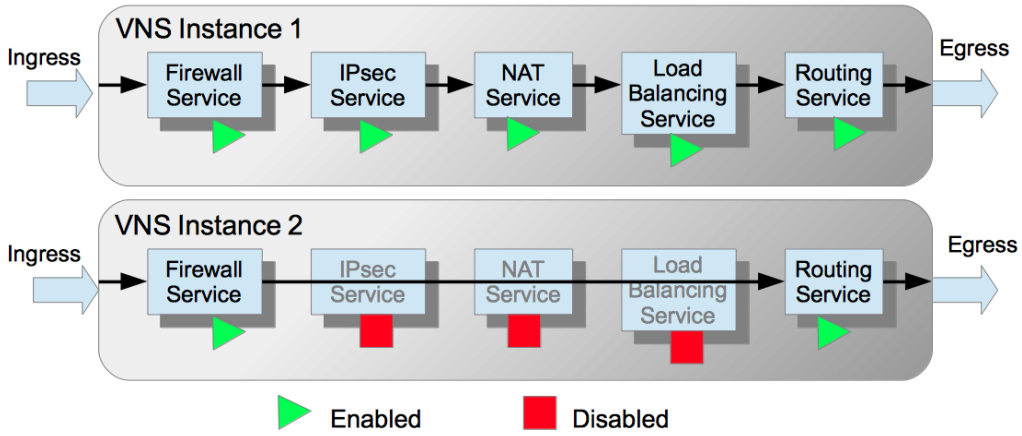

Figure 4. Chaining of network services

Redundancy for High Availability

The VNS high availability (HA) option ensures uninterrupted service by configuring a failover mechanism with redundant network master/backup gateways. A typical HA configuration is shown in Figure 5. The collection of VNS services running on a VNS network gateway with HA redundancy is protected from a single point of failure, as are all the virtual network interfaces of the VNS network gateway.

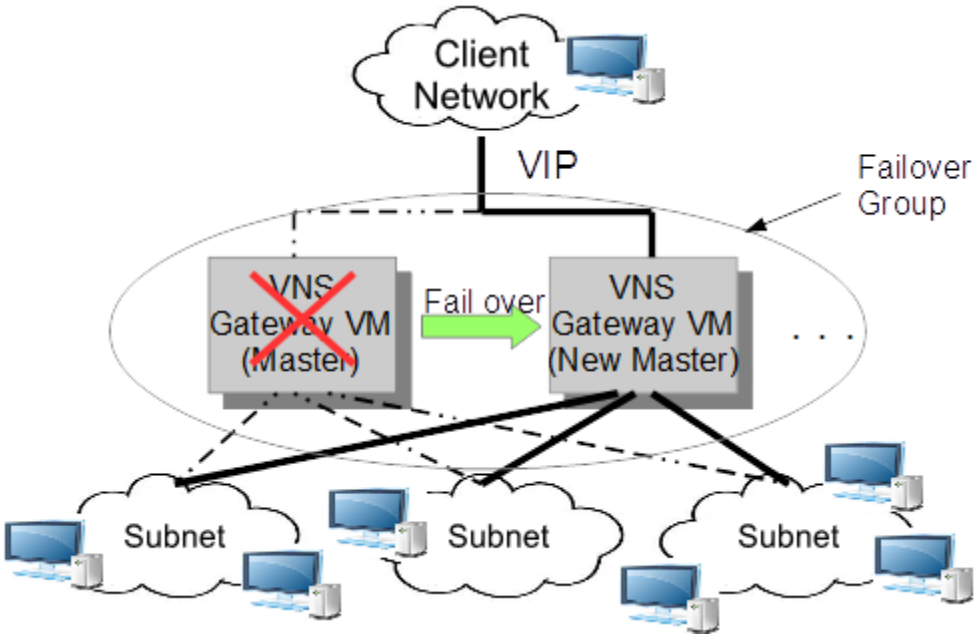

Figure 5. Service failover

A failover group consists of a master VNS network gateway and one or more backup VNS network gateways. To set up an HA configuration, at least two VMs are needed to form a failover group that is presented to the client network as a single virtual IP address (VIP). From a client's perspective, the VIP accesses network services while the Virtual Router Redundancy Protocol (VRRP) provides the HA failover mechanism. The client is never aware of the redundant configuration. Initially, the network services configured on all redundant servers are identical. Subsequent changes to service configurations are synchronized by the HA agent, which is a built-in component of VNS. VRRP provides the mechanism to elect one server from the set of redundant servers in the failover group as master. The master assumes ownership of the virtual IP (VIP) address assigned to the failover group. Clients send their network service requests to the VIP, and are unaware of which VNS server in the redundant failover group is actually providing the service.

Services running on the redundant backup server do not get the packets sent to the VIP, while VRRP drops packets if it is not the master. Hence, at any given time, only those services running on the master in a failover group are active. When configuration commands are received by the master of the failover group, the HA agent synchronizes the command among all VNS network gateways in the group to ensure that configurations are always consistent.

Should the master go down, due to hardware failure, scheduled maintenance, or other reasons, a new master is elected based on its priority (or other decision parameters) and will assume ownership of the failover group's VIP Packets from clients are now routed to the new master. Since the HA agent keeps all network service configurations consistent among the failover group servers, the new master will immediately service clients seamlessly following a failover.

Should a configuration change while a server is offline, that server will be out of sync with rest of the server group. When that server boots, the HA agent will automatically sync with the current master.

Figure 6 shows a high availability configuration within a single physical server. In this configuration, there are two VNS gateway instances (one on each VM). One gateway VM is configured as the master, the other as a backup. Each are connected to multiple subnets. When the master VNS gateway VM goes down, the backup VNS gateway VM continues to provide network services.

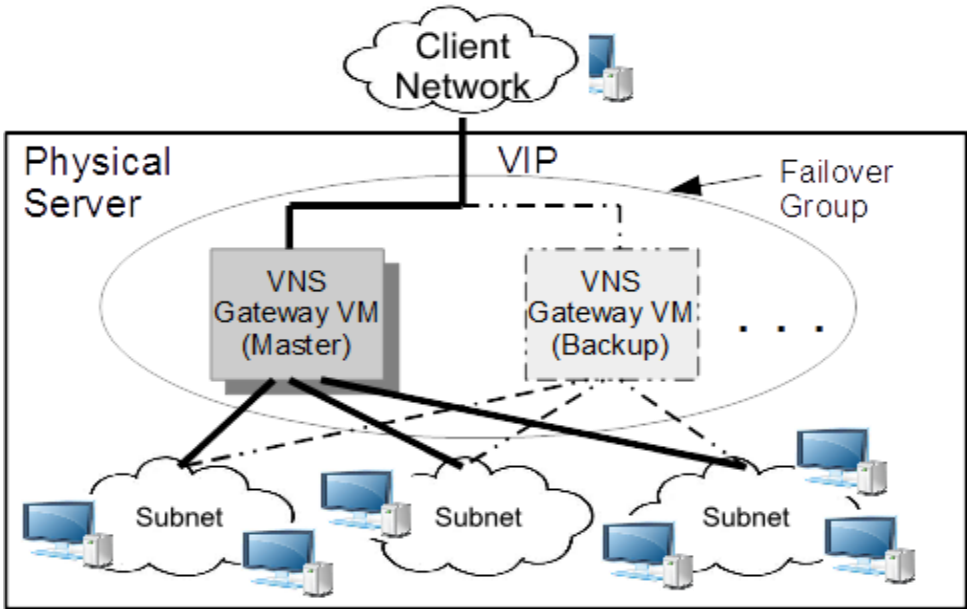

Figure 6. High availability configured within a single physical server

High availability can be configured across two or more physical servers, shown in Figure 7. In this configuration, when the physical server that hosts the master gateway VM goes down, the VNS backup gateway VM hosted by the other physical server continue provide network services.

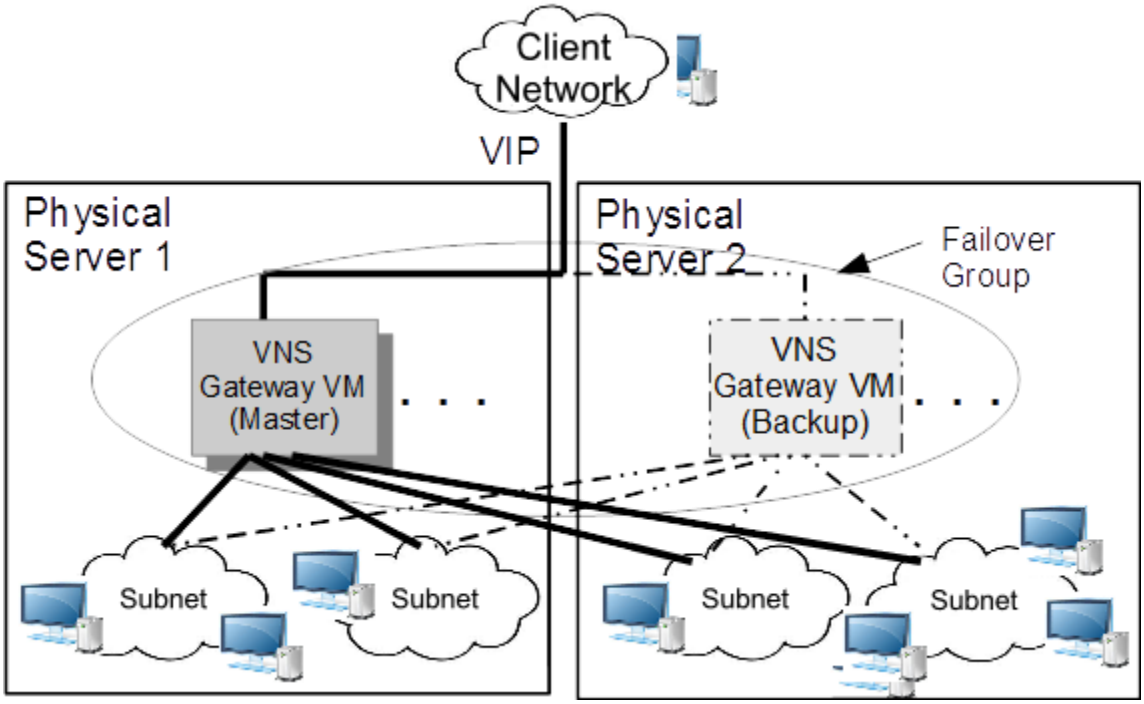

Figure 7. High availability configured across two physical servers

Single-Screen Management for all Network Services

Oracle Fabric Manager, a separate piece of software, manages SDN virtual network services through an intuitive GUI that relies on a set of RESTful APIs. The GUI provides the network administrator the ability to create virtual network functions across the data center network interconnect simply by a point-and-click on the network function tabs. An equivalent CLI provides a scriptable method of configuration that can be run from the console for fast one-step automated operation. The RESTful API can be used for integrating with orchestrating frameworks. Using Oracle Fabric Manager, the administrator can ensure tenant isolation by creating a unique user domain for managing VNS instances belonging to a tenant. With appropriate privileges, a default domain can be created to manage VNS instances of all tenants. Figure 8 shows the Oracle Fabric Manager VNS dashboard.

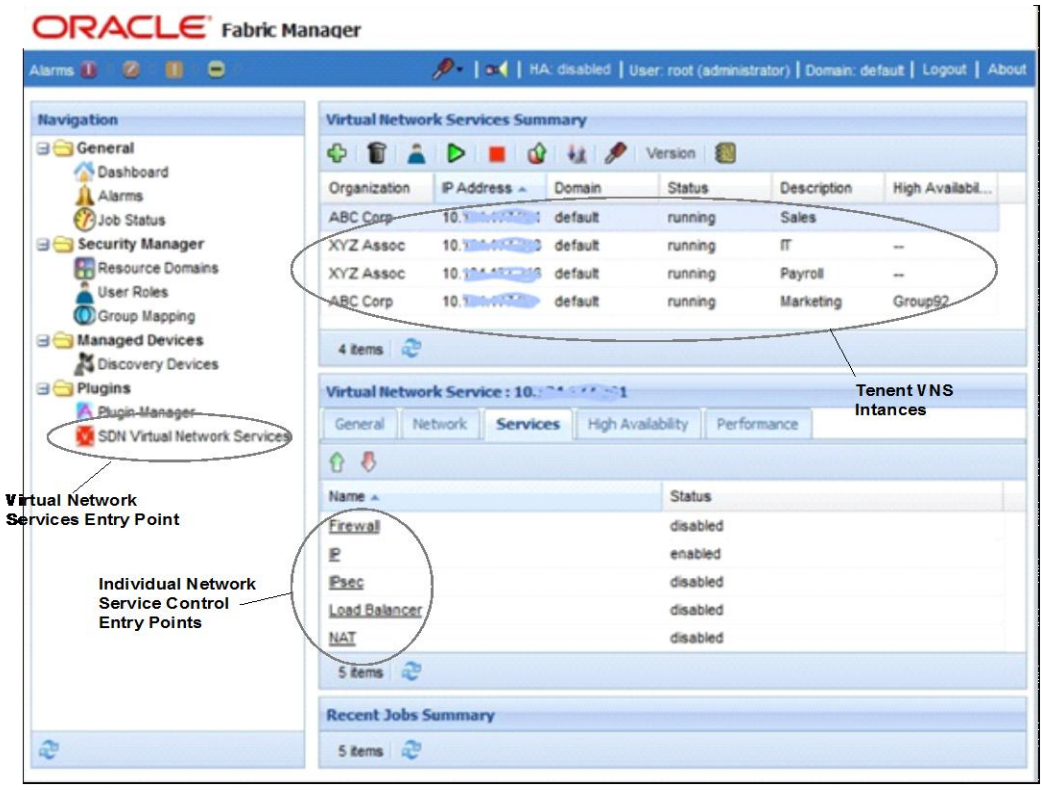

Figure 8. Oracle Fabric Manager VNS dashboard

Network Functions

Oracle SDN virtual network services provides the following standard network functions: static routing, firewall, load Balancing, VPN/IPsec, NAT, and high availability redundancy. Oracle Fabric Manager provides independent management control of each function, along with dashboard monitoring with performance statistics and traffic flow displays.

Firewall

The VNS firewall provides protection for tenants behind a gateway. It enables users to create specific rules that define the packet traffic allowed to pass through the gateway. The firewall has separate ingress and egress rules that can be set independently. The firewall feature is, by default, disabled initially. Users can easily add new rules specific for their individual deployment scenarios and begin testing various configurations. The firewall is multihomed, which enables each rule to be set on a per subnet interface basis to protect cross traffic between subnets. Firewall rules are defined by standard Layer3 and Layer4 attributes, and the firewall is aware of stateful connections, such as TCP. The firewall also provides a quick rule table search, in which action is performed upon the first rule match, overriding the default search method, where the action will not be taken until all rules in the table are searched. Oracle Fabric Manager also displays statistics and logging that tracks blocked and permitted traffic.

Network Address Translation

VNS provides a two-way NAT function for translating destination IP addresses on incoming traffic and/or translating source IP addresses on outgoing traffic. This allows translation between public and private addresses and between public and private networks.

Routing

A VM running virtual network services automatically becomes a network gateway. Implied routing functions are enabled for all the networks connected to the gateway. Users can add static routes for networks that are connected to the gateway through an external next hop router (see Figure 9). The right side of Figure 10 shows VNS virtual router setup to support Equal Cost Multiple Path (ECMP). In this configuration, users enter routes with different next hop addresses to reach the same target. When no ECMP configuration is defined, route selection in VNS virtual router is based on longest prefix match. When an ECMP configuration is defined, the next hop address is chosen based on five-tuple (source IP, destination IP, source port, destination port, protocol type) hashing of the packet header. The algorithm in the virtual network services routing function is designed to minimize the number of memory lookups. With the help of the RESTful API, the VNS routing table may potentially be populated by a SDN-configurable controller to support policy based routing.

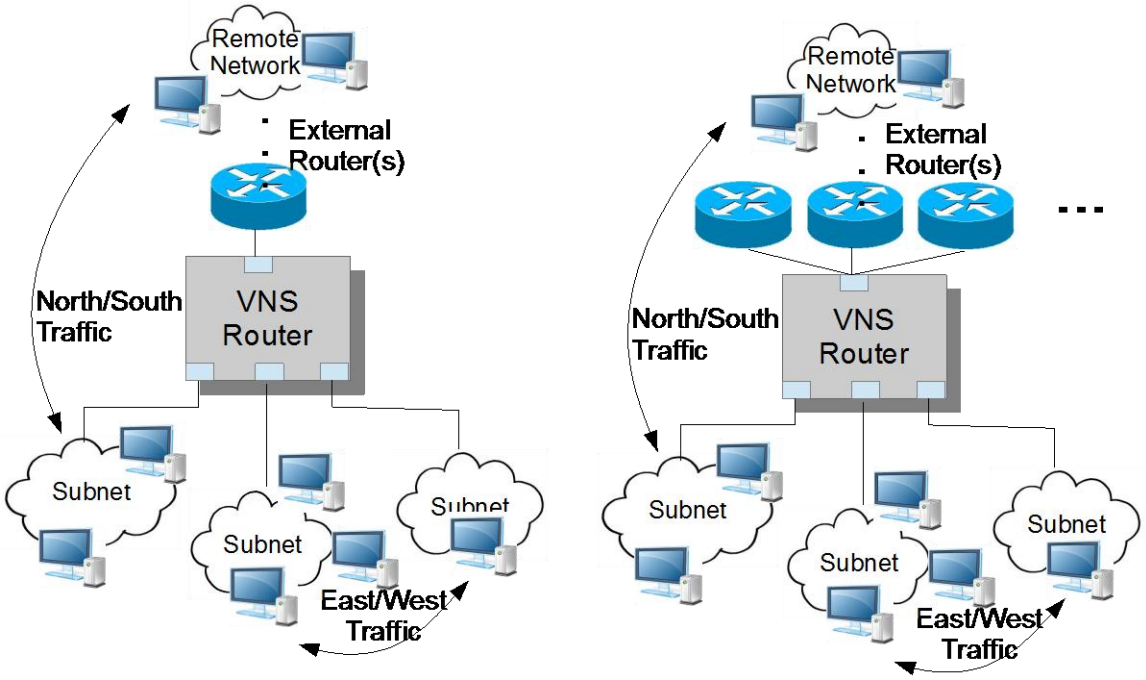

Figure 9. VNS virtual router configurations

Load Balancer

Server load balancing (SLB) is an essential component for maintaining scalability and availability of a network service. It maintains scalability by distributing traffic to a group of server VMs through a single virtual IP address (VIP), resulting in a highly scalable virtual server for hosting applications. It also ensures availability by having multiple instances of the same application replicated by multiple server VMs in a VM server pool, thereby avoiding a single point of failure. Virtual network services load balancer directs a client's traffic to server groups and to an individual server in the group based on the protocol and the algorithm selected. VNS also provides a health check capability that immediately notifies the load balancer of a failed VM so that it can redirect traffic to other available server VMs. It also provides a "stickiness" option that confines a client's traffic to the same server, if needed. Figure 10 shows VNS load balancer configured to distribute traffic to three SLB groups. Each SLB group can be configured with a different application. The client uses different VIPs to address the different groups.

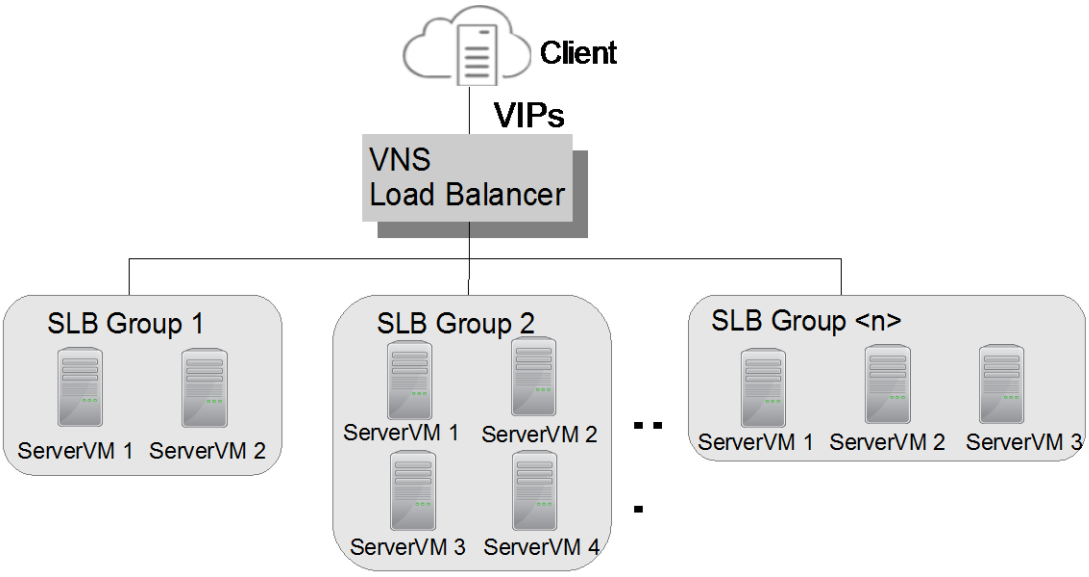

Figure 10. VNS load balancer setup with multiple server groups

Virtual Private Network

When extending a private network to the internet or other external third party networks, establishing a virtual private network (VPN) ensures secure access along with the appropriate levels of encryption and authentication. Virtual network services allow users to configure VPN through an IPsec tunnel, as shown below (Figure 11). Tenants define policies allowing a remote private network or individual remote hosts to access the local network. The remote IPsec gateway can be another VNS instance or a generic IPsec gateway that supports the Internet Key Exchange (IKE) protocol. VNS supports some of the most secure block ciphers, such as AES for encryption and SHA for authentication.

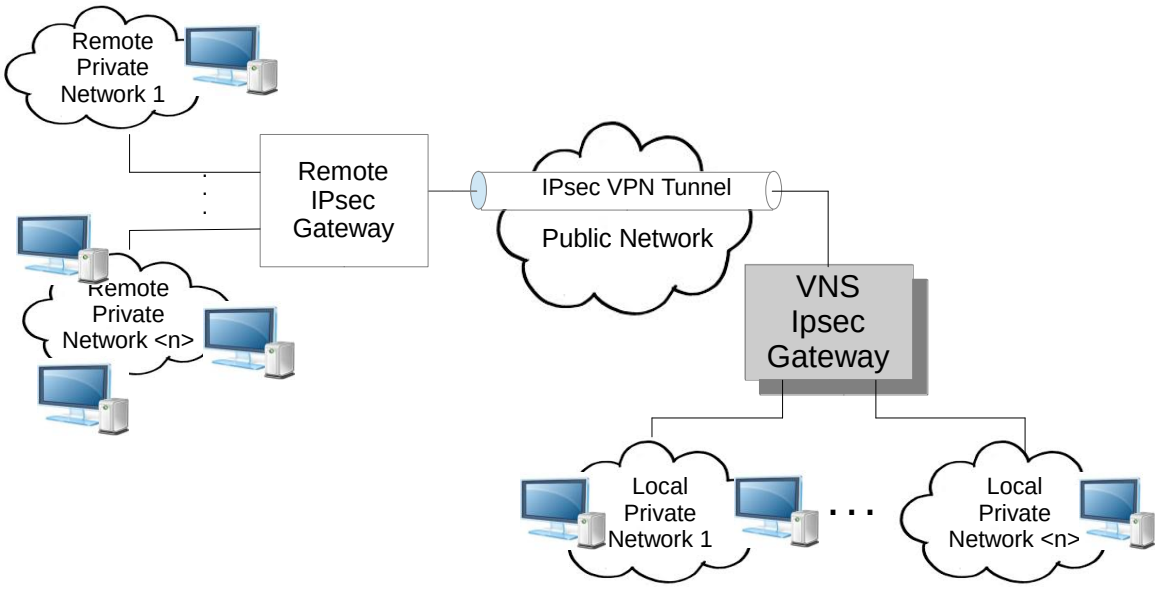

Figure 11. Virtual IPsec gateway

Network Services Use Cases

Use Case 1: Firewall and NAT Services

A common practice is to protect a web server behind a VNS gateway with a firewall (see Figure 12). This involves creating rules that allow ingress traffic to flow to the web server behind the VNS gateway. To provide the required degree of privacy, the firewall service works with the NAT service to translate the private web server's IP address to a globally accessible IP address, as shown in the following diagram:

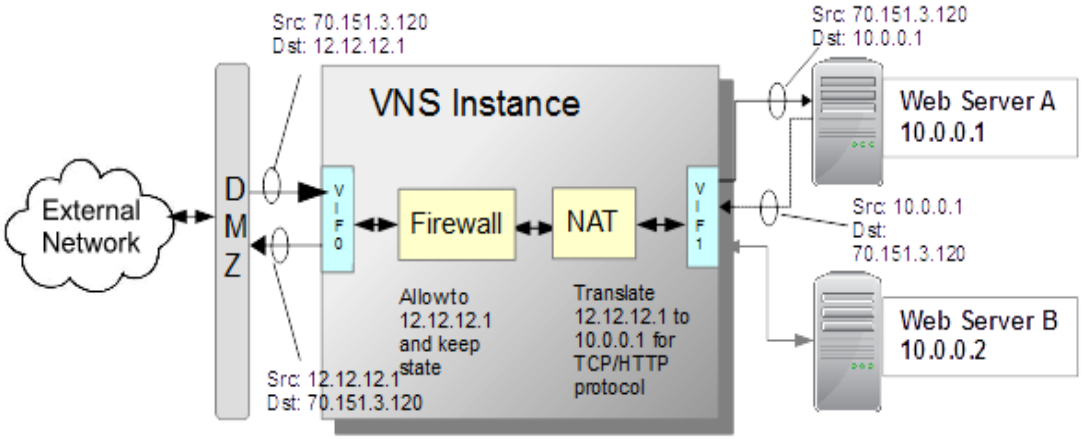

Figure 12. Firewall/NAT use case

In the above diagram, a firewall rule allows incoming traffic to host 12.12.12.1. A NAT rule translates the incoming destination address to 10.0.0.1, which belongs to web server A. This combination of rules effectively hides the web server belonging to the tenant from public view, exposing only the IP address of the public-facing interface of the VNS instance.

Use Case 2: Routing Service

In a multitiered configuration, the user can host all servers within a single subnet. While this configuration provides simplicity, it has a few disadvantages. First, there is no isolation among all the servers; access control (accessing a database server from external network, for example) is solely based on firewall rule settings. Second, all servers are affected if the network goes down.

A more secure approach is to segregate the multitiered servers into multiple subnets to provide an extra level of security by creating further isolation between tiers. For example, a configuration can be created where the web servers do not have direct access to the content of the data servers. Furthermore, when one network goes down, it does not affect access to servers on the other tiers.

Figure 13 below illustrates a three-tier application with each tier on a separate subnet. A VNS Instance provides firewall and routing functions. Note that each firewall block in the diagram depicts a firewall policy. In this configuration, a firewall on each tier allows traffic based on security policies. The web tier allows traffic from clients on the external network. The application tier allows traffic from the web server on the web network only, while the database tier allows traffic from the app server on the app network only. The three-tier networks are directly connected to the VNS instance through their corresponding network interfaces. The client network is multiple hops away from the VNS instance. The server in each tier sets the default gateway for the VNS instance. To route traffic

back to the client network (not directly connected to the VNS instance), a static route drives the client's traffic to the last hop router of the VNS instance.

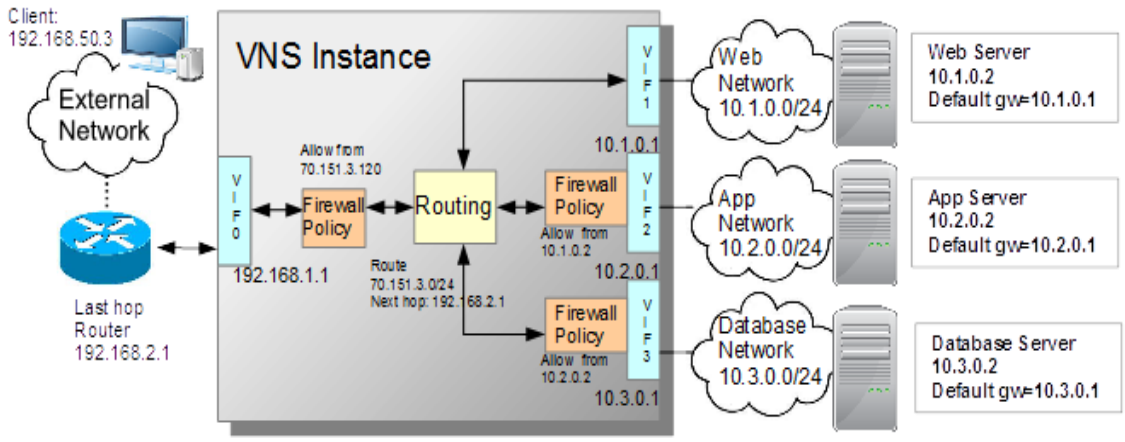

Figure 13. VNS routing use case

Use Case 3: Load Balancing Service

The following example (see Figure 14) demonstrates a typical use case for load balancing. The example shows a load balancing group configured to balance incoming traffic to the web tier. The client accesses the virtual server using a virtual IP address assigned to the load balancing group. The configuration shown in the example uses half-NAT load balancing mode where only the destination address (VIP) is translated into the real server address. With the Round Robin load balancing algorithm selected, each new connection is dispatched to the next server in the group. Also, notice that the health check has detected a failure at web server 1. Responding to the failure, new traffic is steered away from web server 1 and the load balancing algorithm is applied to the remaining servers in the group.

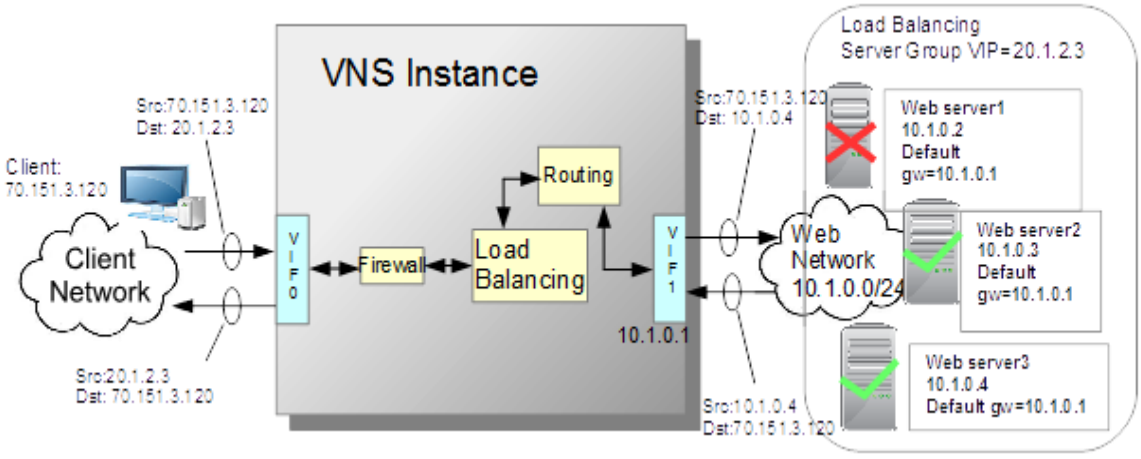

Figure 14. VNS load balancing use case

In another example (Figure 15), the load balancer is configured into a three-tier network with high availability. The configuration encompasses two physical servers. VMs that span both hardware servers form the three-tier server groups. Two VNS instances (with identical services) are configured for high availability (one instance per physical server). The client accesses the virtual web server using the virtual IP address of the high availability group (HA-VIP). When VNS receives the client's request, it further translates the HA-VIP into the virtual IP address of the web server groups (VIP1) to access a virtual web server. Two other load balancing groups are created, one for the application tier and the other for the database tier, represented by VIP 2 and VIP 3. In normal situations, the master VNS instance performs all the operations in the firewall/NAT/load balancing/routing service chain. When the master VNS instance detects a failure or when physical server 1 goes down completely, the backup VNS instance takes over and performs the identical service chain. New web server requests from the client enter this service chain automatically, unaware of the failover.

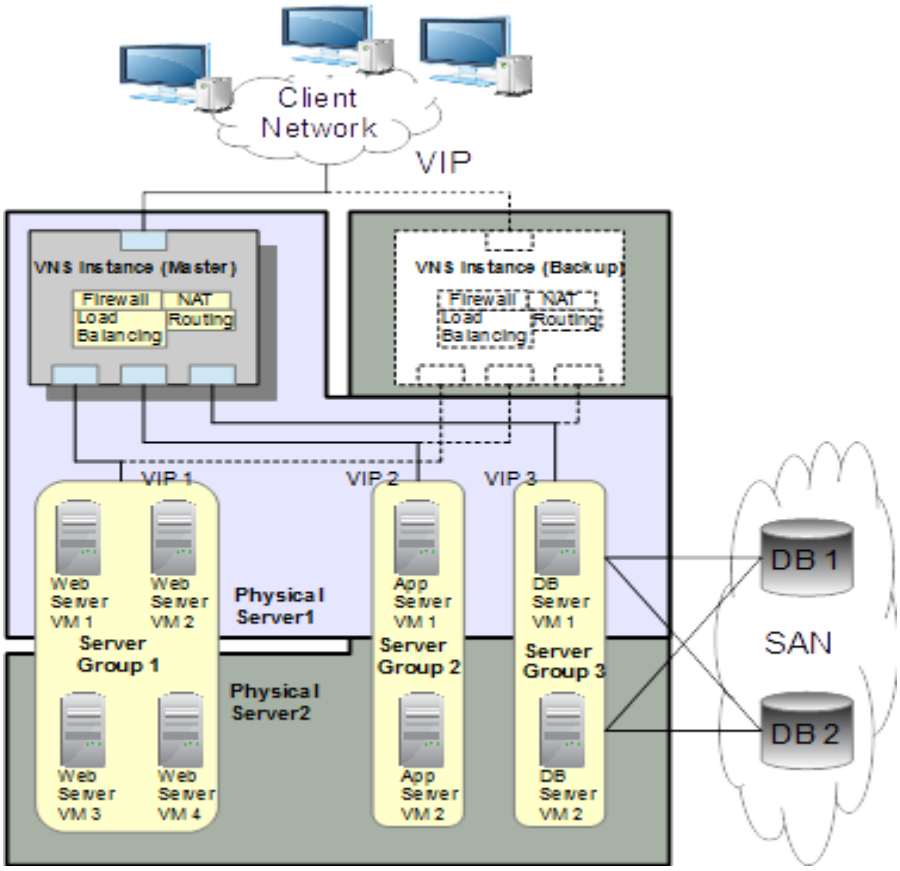

Figure 15. Load balancing in high-availability configurations

Use Case 4: VPN Service

A typical VPN use case is the site-to-site configuration shown below in Figure 16. A user from a remote private network, with given authorization credentials, needs to access data on a local private network that is front-ended by a VNS instance. Enabling a IPsec service on the VNS Instance automatically creates an IPsec gateway, forming an IPsec tunnel between the local IPsec gateway and the remote IPsec gateway. This permits access to the servers in the local private network. The numbers in the diagram indicate the data paths taken inside the VNS instance when packets arrive the VNS instance.

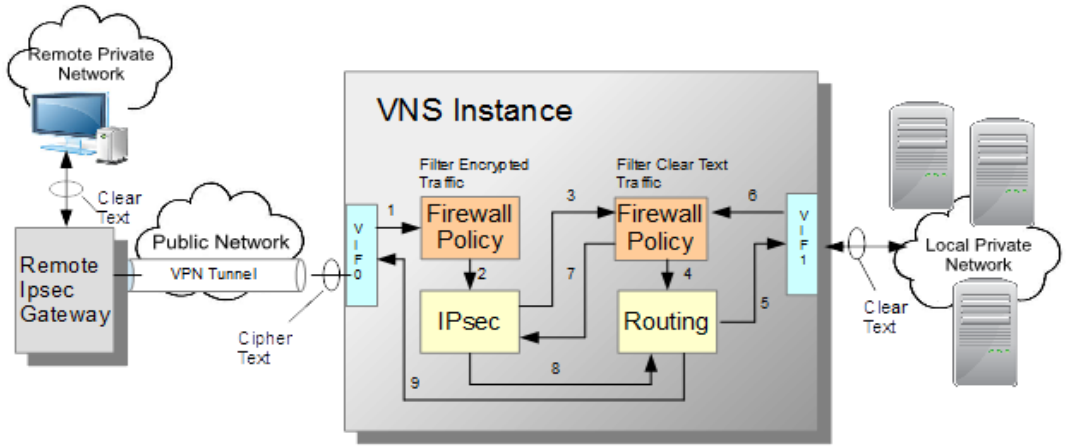

Figure 16. Example VPN/IPsec configuration

The following details the steps taken in the data path:

1: Traffic (cipher text) arrives at the VNS instance local IPsec tunnel endpoint and enters the firewall

2: Filtered traffic enters IPsec module for decryption and authentication

3: Clear text enters firewall for filtering

4: Filtered traffic enters the routing module

5: Routed traffic enters the determined egress port for the target local private network

6: Traffic from local private network enters firewall for filtering

7: Filtered traffic (clear text) enters IPsec module for encryption and authentication

8: Cipher text enters routing module

9: Routed traffic enters the determined egress port for the target remote private network

Analytics

The VNS built-in analytics engine monitors VNS gateway resources and services performance in real time. The analytics engine provides visibility into VNS services and can help in capacity planning. It tracks traffic entering and leaving all VNS gateway network interfaces for each network function. Examples of data collected are:

- Types of packets processed by the IP layer, classified by protocols
- Traffic allowed or blocked by the firewall
- Traffic distribution among servers in a load balancing group
- Amount of packets encrypted and decrypted by IPsec
- Network bandwidth usage for north/south and east/west traffic

Oracle Fabric Manager presents the data collected as infographics in the GUI, or as CLI text output. Figure 17 shows the infographics for the load balancer traffic distribution to servers.

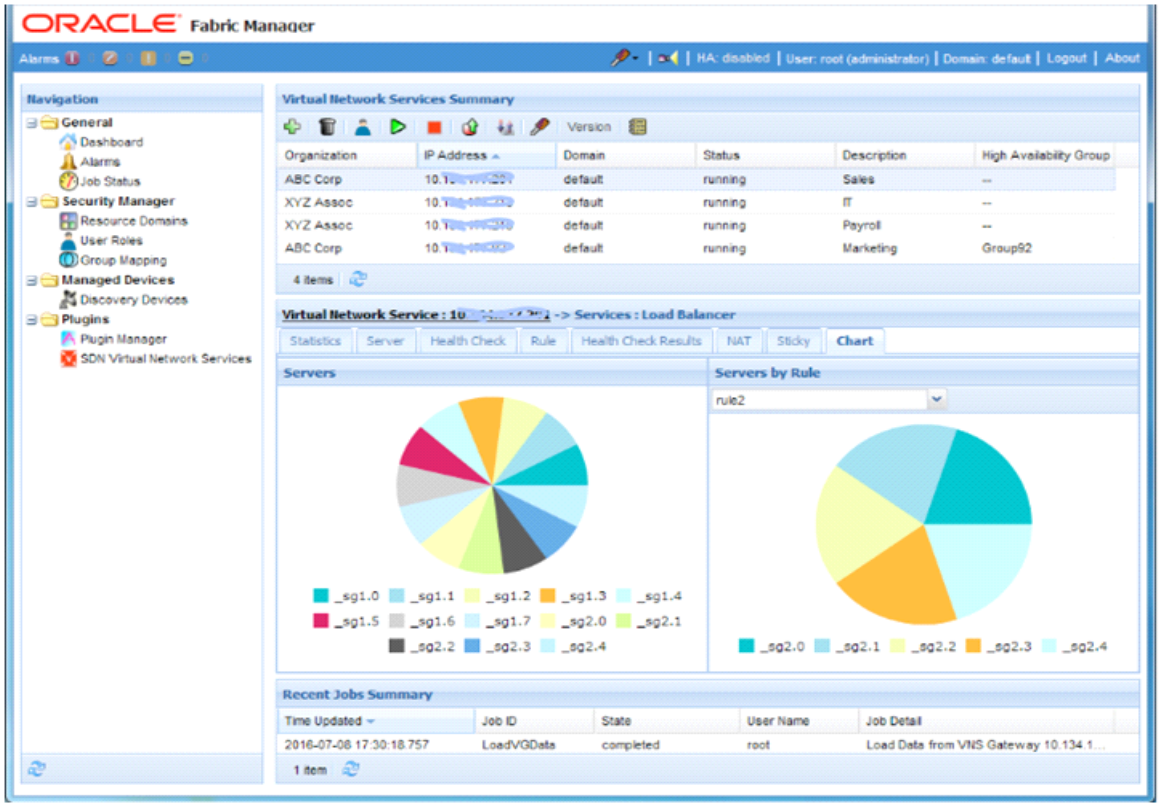

Figure 17. Load Balancer traffic distribution display in Oracle Fabric Manager

Conclusion

Oracle SDN virtual network services fulfill the need for essential network services such as firewalls, NAT, VPN, and load balancing that are virtualized and managed from a single screen. Virtualized network services, implemented in software, eliminate the need for costly, proprietary, fixed network appliances that lack the flexibility and scalability cloud-enabled data centers require. Oracle VNS provides this full set of network functions across both the Oracle InfiniBand and Ethernet fabrics, creating a uniquely agile and elastic network infrastructure for the entire data center.

Learn More...

For more information about Oracle's virtual networking products, visit http://www.oracle.com/us/products/networking/virtual-networking/overview/index.html, call +1.800.ORACLE1 to speak to an Oracle representative, or visit the web resources below.

TABLE 1. RESOURCES

Oracle SDN	http://www.oracle.com/us/products/networking/virtual-networking/sdn/overview/index.html
Oracle Fabric Manager	http://www.oracle.com/us/products/networking/virtual-networking/fabric-manager/overview/index.html
Oracle SDN Virtual Network Services Documents	http://docs.oracle.com/cd/E48586_01/index.html

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US


blogs.oracle.com/oracle


facebook.com/oracle


twitter.com/oracle


oracle.com

Integrated Cloud Applications & Platform Services

Oracle Virtual Network Services
August 2016