VMware vCloud Networking and Security Overview

Networks and Security for Virtualized Compute Environments

vmware®

Overview

Organizations worldwide have gained significant efficiency and flexibility as a direct result of deploying virtualization solutions from VMware. As more business-critical applications are virtualized, administrators are increasingly confronting the challenges of deploying and managing networks and security to keep pace with data center innovation.

VMware vCloud® Networking and Security™ provides essential networking and security functionality for virtualized compute environments built using VMware vCloud® Suite.

Challenges Stifle IT Productivity

Today, a virtual machine can be provisioned in a matter of minutes, but surrounding it with all the necessary network and security services still takes days or weeks. Operational costs rise as manual provisioning, dedicated physical appliances and fragmented management interfaces reduce efficiency and limit IT's ability to support business needs.

Networking and security constructs tied to rigid dedicated hardware increase data center cost and complexity. Underutilized server capacity due to network constraints prevents IT from pooling, moving or scaling across noncontiguous clusters. IT is further constrained by labor-intensive network operations caused by the complexity of VLAN provisioning and management.

Even routine tasks, such as rack maintenance or upgrade, that require workloads to move to different hosts or clusters can take weeks of planning and testing.

The rigidity of physical networks and manual operations inhibits the responsiveness of IT teams, preventing them from adapting to dynamic business needs. Without visibility into how traffic flows in a virtual environment, IT faces the increasing possibility of policy violations, slowing security policy implementation and management.

Businesses now need rapid access to IT resources to support faster time to market. IT needs to deliver this access while ensuring that the data center is fully managed and secured. With vCloud Networking and Security, enterprises can virtualize business-critical applications with confidence, secure VMware Horizon View™ deployments, and build secure and agile private clouds based on VMware vCloud Suite.

VMware vCloud Networking and Security

vCloud Networking and Security provides networking and security capabilities for virtualized compute environments that are built with vCloud Suite technologies. It provides a broad range of services delivered through virtual appliances (see Figure 1), such as a virtual firewall, virtual private network (VPN), load balancing, network address translation (NAT), DHCP and VXLAN-extended networks, while also providing a comprehensive framework to integrate third-party solutions.

These foundational networking and security capabilities of the vCloud Suite enhance operational efficiency, improve agility with control and enable extensibility to partner solutions. Management integration with VMware vCenter Server™ and VMware vCloud Director® reduces the cost and complexity of data center operations.
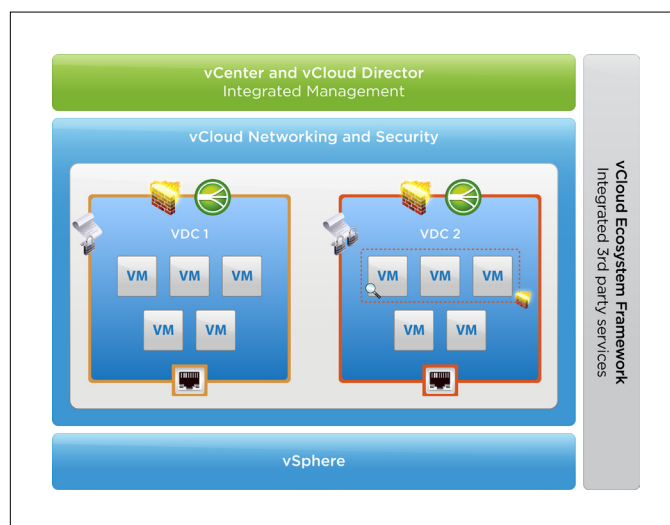

Figure 1. vCloud Networking and Security Solution Overview

Key Capabilities of vCloud Networking and Security

- **Firewall** – Stateful inspection firewall that can be applied either at the perimeter of the virtual data center or at the virtual network interface card (vNIC) level directly in front of specific workloads. The firewall-rule table is designed for ease of use and automation with VMware vCenter™ objects for simple, reliable policy creation. Stateful failover enables high availability for business-critical applications.

- **VPN** – Industry-standard IPsec and SSL VPN capabilities that securely extend the virtual data center. Site-to-site VPN support links virtual data centers and enables hybrid cloud computing at low cost. The SSL VPN capability delivers remote administration into the virtual data center through a bastion host, the method favored by auditors and compliance regulators.

- **Load balancer** – A virtual-appliance–based load balancer to scale application delivery without the need for dedicated hardware. Placed at the edge of the virtual data center, the load balancer supports Web-, SSL- and TCP-based scale-out for high-volume applications.

- **VXLAN** – Technology that, along with VMware vSphere® Distributed Switch™, creates Layer 2 logical networks across noncontiguous clusters or pods without the need for VLANs (multicast required). This enables you to scale your applications across clusters and pods and improve compute utilization.

• **Instrumentation** – Granular network traffic telemetry that enables rapid troubleshooting and incident response. Traffic counters for sessions, packets and bytes provide visibility into the virtual network and streamline firewall-rule creation.

• **Management** – Integrates with vCenter Server and vCloud Director to provide separation of duties with role- based access control (RBAC) while providing a central point of configuration and control for network and security services.

• **vCloud Ecosystem Framework** – Integrates partner services at either the vNIC or the virtual edge using REST APIs.

The complete set of vCloud Networking and Security features (see Table 1) is available in all vCloud Suite editions. vCloud Networking and Security is available only within vCloud Suite editions and is not sold as a standalone product.

FEATURES	VCLOUD SUITE STANDARD	VCLOUD SUITE ADVANCED	VCLOUD SUITE ENTERPRISE
Firewall	●	●	●
VPN	●	●	●
VXLAN	●	●	●
vCloud Ecosystem Framework	●	●	●
NAT	●	●	●
DHCP	●	●	●
High availability (HA)	●	●	●
Load balancing	●	●	●
Data Security	●	●	●
Endpoint	(Bundled in VMware vSphere 5.1 or later)		

Table 1. vCloud Networking and Security Features

Architecture

vCloud Networking and Security is built with virtual appliances. Network traffic from virtual workloads is passed through these appliances, which apply services such as firewalls and load balancing. Third-party services from integration partners also have access to network traffic through these appliances.

There are two vCloud Networking and Security virtual-appliance types. The Edge Gateway appliance establishes a perimeter gateway for network traffic to enter and leave a virtual data center. It provides a wide range of services, including a highly available stateful inspection firewall, IPsec site-to-site VPN, a server-load balancer, NAT, and network services such as static routing, DHCP and domain name system (DNS). A second type of virtual appliance, App Firewall, provides protection directly in front of one or more specific workloads (e.g., virtual machines).

This firewall flexibility is a key advantage of the vCloud Networking and Security architecture (see Figure 1). For example, if IT wants to help protect a specific workload from attack, deploying a firewall immediately in front of that workload may be most

appropriate because IT can then ensure that all traffic directed at the workload is protected by a firewall, regardless of its source. In contrast, if a virtual domain is being created for a lab environment, IT may choose to deploy a firewall at the edge of the domain. In this case, the lab team could do what it wants inside its domain, and IT would simply control access to the corporate network from outside the domain.

vCloud Networking and Security is built on top of vSphere Distributed Switch, available in VMware vSphere Enterprise Plus Edition™. vSphere Distributed Switch provides high-performance virtual networking across clusters. Integrated management with vCenter and vCloud Director provides centralized control and visibility down to the virtual port level.

vCloud Networking and Security Services

vCloud Networking and Security delivers networks and security with a broad range of services in a single solution.

Firewall Services

VMware vCloud Networking and Security Edge™ and VMware vCloud Networking and Security App™ firewalls are tightly integrated into vSphere and rely heavily on vCenter objects in policy creation (see Figure 2). For example, you can use the firewall-rule table to directly select vCenter objects such as workloads, port groups and virtual networks. This integration makes rule creation faster and less error prone than legacy approaches that require administrators to manually create and maintain IP address–based objects. Once defined, rules can be enforced at either the perimeter of the virtual data center with vCloud Networking and Security Edge, or directly in front of a workload at the vNIC level with the vCloud Networking and Security App firewall. Regardless of the enforcement point, vCloud Networking and Security firewall services perform stateful packet inspection at improved performance and low latency.

Figure 2. Intuitive Firewall Rules with vCenter and vCloud Director Objects

vCloud Networking and Security Edge includes multiple virtual network interfaces that give security architects much more flexibility in designing software-defined networks (see Figure 3). These interfaces can segment virtual networks and provide connectivity to multiple VLANs deployed on the physical network.

Figure 3. Multiple Interfaces for Network Segmentation

NAT

vCloud Networking and Security Edge incorporates a flexible NAT engine that can map network and port addresses using a familiar configuration model (see Figure 4). Administrators can deploy protected zones, also known as "demilitarized zones" (DMZs), without needing to manually change addresses for servers and applications. Application-layer gateways for common protocols enable applications to function in NAT environments.

Figure 4. Flexible NAT Engine

VPN

vCloud Networking and Security Edge IPsec VPN provides secure site-to-site connectivity using widely supported standards such as Internet Key Exchange (IKE) with 256-bit Advanced Encryption Standard (AES-256) for strong encryption (see Figure 5). This capability enables you to interconnect virtual data centers securely to physical firewalls from a variety of vendors.

Figure 5. Secure IPsec Site-to-Site VPN Connectivity

SSL

vCloud Networking and Security also incorporates SSL remote access to give administrators access to the virtual data center. SSL is implemented on the Edge Gateway virtual appliance and enables administrators to perform remote configuration, troubleshooting and other routine management tasks. The vCloud Networking and Security implementation resembles administrative remote access through a JumpBox or Bastion host, the method preferred by most security specialists and auditors. This approach minimizes the attack surface of the virtual domain and makes auditing administrative activity easier and more robust.

Load Balancer

vCloud Networking and Security provides powerful server-load–balancing capabilities to increase availability and performance of business-critical applications (see Figure 6). Several load-balancing algorithms are supported, including round-robin, cookie-based and session-based alternatives.

Figure 6. vCloud Networking and Security Server Load Balancing

Edge High Availability

vCloud Networking and Security enables stateful high-availability (HA) firewalls for virtual data centers (see Figure 7). With vCloud Networking and Security Edge HA, active firewall connections can be continuously synchronized between an active/standby pair of Edge virtual appliances. If a failure occurs in the active Edge appliance, sessions are not lost, and the standby unit resumes the passing of traffic in less than 10 seconds. With this level of availability, administrators gain the confidence to virtualize business-critical applications.
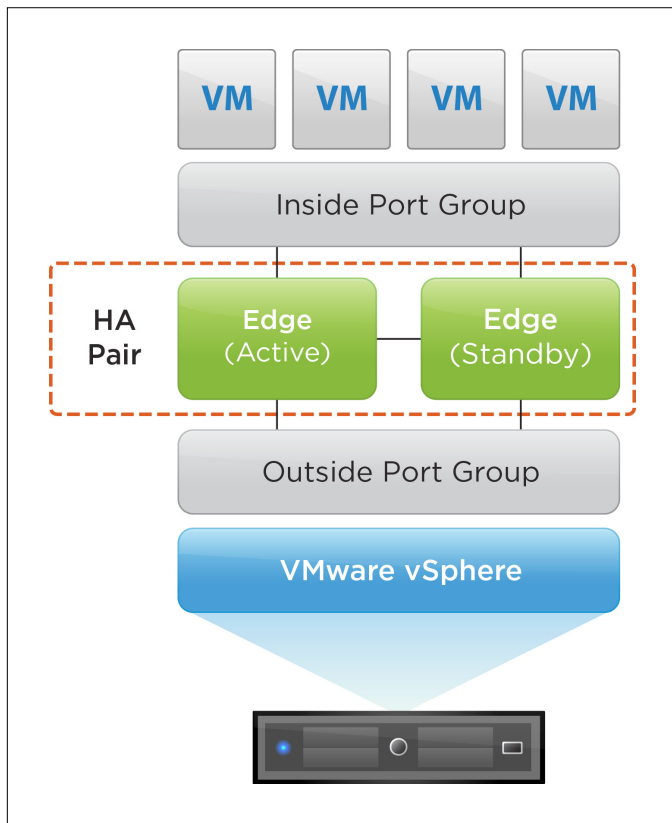
Figure 7. Edge Stateful HA Firewall

Data Security

The solution also includes VMware vCloud Networking and Security Data Security™ for Microsoft Windows. This feature scans Windows (Common Internet File System, or CIFS) file servers for sensitive data that matches predefined templates, such as credit card or social security numbers. The templates provide a wide variety of international sensitive data formats. vCloud Networking and Security Data Security is typically used to locate data that has been stored on file servers without proper access controls or auditing.

VXLAN

The VXLAN protocol leverages user datagram protocol (UDP) encapsulation to enable networks to stretch across multiple clusters and Layer 3 segments of the data center. Moreover, unlike VLANs, which are limited to 4,096 segments, VXLAN scales to 16 million segments without requiring a large upgrade to existing physical switching infrastructure. Administrators use vCenter Server or vCloud Director to define VXLAN segments (see Figure 8), enabling efficiency and "single pane of glass" management of the network. vCloud Networking and Security Edge performs VXLAN-to-VLAN gateway translations to allow simple migration. In addition, VMware has enhanced the vSphere Distributed Switch component of vSphere Enterprise Plus Edition to provide troubleshooting and traffic statistics about VXLAN encapsulated traffic.

Figure 8. VXLAN Software-Defined Networking

vCloud Ecosystem Framework

vCloud Networking and Security includes standards-based APIs that enable third-party solution providers to integrate products into the virtual environment. As part of vCloud Ecosystem Framework (see Figure 9), the APIs allow network-level access to data flows at either the vNIC or the virtual data center edge level. Network traffic can be redirected to flow through a third-party product, or packets can simply be copied. For example, a third-party intrusion prevention system (IPS) should be placed in line with traffic flows, whereas a pure monitoring tool (e.g., a packet capture tool) requires only a copy of the traffic. The framework supports third-party products implemented as either hardware or virtual appliances.
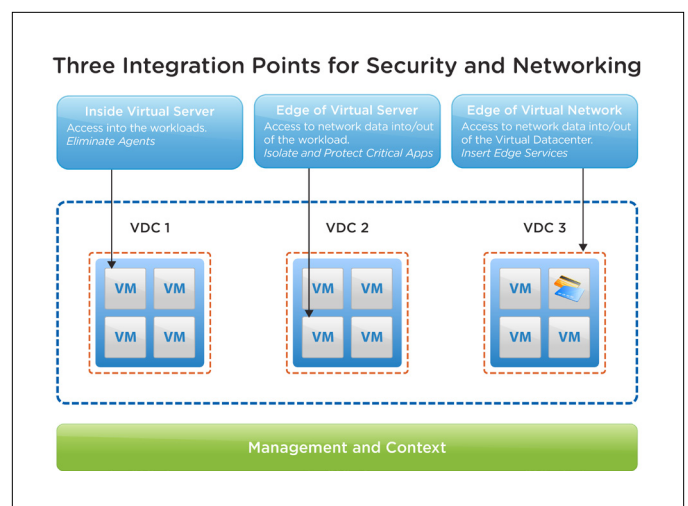
Figure 9. vCloud Ecosystem Framework for Inserting Third-Party Services

This approach means that companies can protect their investments in existing hardware and can easily transition to virtual appliances over time using a consistent operational model.

Key Benefits

vCloud Networking and Security lowers operational costs, increases agility and flexibility, and extends to include third-party services.

Lower Costs by Improving Efficiency and Utilization

Allocate compute resources elastically across clusters and pods with VXLAN-based networks..Simplify provisioning and lower operational costs while reducing the need for specialized devices by using virtual appliances to provide integrated gateway services.

- Manage and allocate compute resources across clusters and pods.
- Reduce dependence specialized devices.
- Take advantage of vCenter or vCloud Director integration.

Adapt to Business Needs with Virtual Workload Agility

Create networks that scale with applications and apply security services exactly where needed without hardware upgrades. vCloud Networking and Security delivers higher application availability and improved network performance.

- Deploy, move or scale virtual workloads across clusters or pods (see Figure 10).
- Automate provisioning and scale-out of networking and security services.
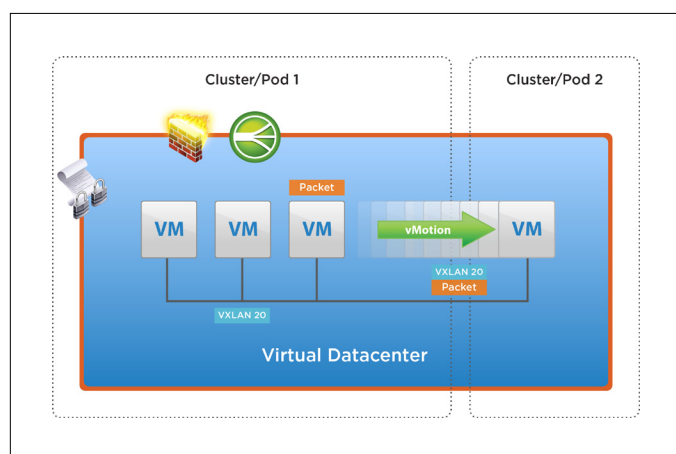- Gain greater visibility into virtual traffic flows.

Figure 10. Workload Mobility Across Clusters and Pods

Use Best-of-Breed Security Solutions Across Your Infrastructure

Take advantage of the latest third-party innovations while leveraging your existing networking and security investments. REST APIs allow service insertion at the vNIC and the virtual edge, with support for both hardware and software solutions.

- Leverage the open architecture and industry-standard APIs.
- Enable consistent support across hardware and software-based solutions.
- Protect your existing networking and security investments.

How to Use vCloud Networking and Security

Using vCloud Networking and Security, enterprises can virtualize business-critical applications with confidence, build secure and agile private clouds, and protect their virtual desktop solutions.

Protect Business-Critical Applications with Lower Cost and Complexity

As organizations virtualize more business-critical applications, they need to protect and isolate them from less secure systems. They need greater visibility into virtual traffic flows so that they can enforce policies and implement compliance controls on in-scope systems.

vCloud Networking and Security provides robust security and isolation for business-critical applications. Isolating these applications used to require physical VLANs and firewalls, but now it requires only logical groupings and virtual firewall rules with vCloud Networking and Security. Not only are the security rules simpler to implement, but they also are easier to manage and do not require dedicated physical appliances. Adaptive security travels with virtual machines as they migrate from host to host in a dynamic cloud environment. vCloud Networking and Security also provides increased visibility and control over inter–virtual-machine communication for faster policy enforcement.

The benefits of using vCloud Networking and Security to protect and isolate business-critical applications include

- Protection and isolation of critical applications with virtualization-aware firewall and adaptive trust zones
- Increased visibility and control over inter–virtual-machine communication
- Optimized resource utilization across clusters and pods
- Identification and protection of sensitive business information

Build Agile and Secure Private Clouds

vCloud Networking and Security delivers an operationally efficient, simple, cost-effective networking and security solution delivered through vCloud Suite. Because VXLAN-based networks can be deployed and scaled across physical boundaries, organizations can optimize management and use of compute resources across clusters and pods.

Integrated firewall and gateway services secure the perimeter of the virtual data center and provide services such as firewalls, NAT, load balancing, VPN and DHCP, reducing the need for dedicated physical appliances. Because vCloud Networking and Security is fully integrated with vCenter Server and vCloud Director, it reduces manual operations and simplifies deployment and management. vCloud Networking and Security is also

designed to work seamlessly with the existing enterprise IT infrastructure and provides APIs for customized integration of third-party services.

With vCloud Networking and Security secure private clouds, IT teams can

• Reduce manual networking provisioning and simplify deployment by eliminating VLANs

• Optimize management and consumption of compute resources across clusters and pods

• Secure the edge of the virtual data center with integrated firewall and gateway services

• Manage inbound Web traffic across virtual-machine clusters with load-balancing capabilities

• Maximize performance by integrating best-of-breed third-party solutions

Secure Virtual Desktop Infrastructure Deployments

vCloud Networking and Security enables granular and efficient access control in virtual desktop infrastructure (VDI) environments, such as Horizon View. vCloud Networking and Security can create logical security perimeters around individual virtual desktops or around the entire virtual desktop infrastructure. This capability ensures that VDI users can access only the applications and data they are authorized to use and also prevents unauthorized access to the broader virtual data center (see Figure 4). Visibility into VDI traffic enables rapid troubleshooting and policy creation.

The benefits of using vCloud Networking and Security to secure virtual desktops include

• Better protection of virtual desktops from neighbor attacks

• More controlled access from virtual desktops to applications

• Improved isolation of the VDI environment from the rest of the virtual data center

• Protection of sensitive data from access by unauthorized staff members or hackers

• Streamlined security management and prevention of performance bottlenecks

Find Out More

For information or to purchase VMware products, call 877-4-VMWARE (outside North America, +1-650-427-5000), visit http://www.vmware.com/products, or search online for an authorized reseller.

vmware®