VMware vCloud® Networking and Security Overview

Efficient, Agile and Extensible Software-Defined Networks and Security

WHITE PAPER

Overview

Organizations worldwide have gained significant efficiency and flexibility as a direct result of deploying virtualization solutions from VMware. However, although compute has been virtualized, network and security continue to be architected based on legacy physical constructs. As more business-critical applications are virtualized, administrators are increasingly confronting the challenges of deploying and managing networking and security to keep pace with datacenter innovation.

To remove the networking and security barrier to datacenter agility, VMware is introducing VMware vCloud® Networking and Security. Just as VMware vSphere® virtualized compute, vCloud Networking and Security virtualizes networking and security to enable greater agility, efficiency and extensibility in the datacenter.

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 rapidly deploy, move, scale and protect applications and data according to business needs.

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

Administrators spend further time and effort on planning and the manual network reconfiguration required for routine tasks, such as rack maintenance or upgrade, that require workloads to move to different hosts and clusters.

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. Furthermore, adding physical capacity becomes a disruptive, time-consuming process that often requires redesigning the entire solution.

Even when organizations want to take advantage of new technology, IT cannot easily insert third-party network and security services into existing environments and procedures while still maintaining an agile operational model. Additionally, technology refreshes or adoption require staff retraining and the costly replacement of existing infrastructure, stifling choice and flexibility.

Although the concept of Software Defined Networking (SDN) and Security emerged a few years ago in response to these challenges, its adoption has stalled. Hardware appliance vendors have made only tentative improvements, because they need to preserve their existing revenue stream. Industry initiatives such as OpenFlow require massive hardware upgrades, significantly increasing costs and disruption. Moreover, because these initiatives are still evolving and support is limited, most organizations are deferring decisions and implementations until the situation has stabilized.

Now the right solution from VMware, with added integrations from partners, is available to overcome these datacenter challenges and enable businesses to achieve their agility goals without disrupting their business models

VMware vCloud Networking and Security

vCloud Networking and Security virtualizes networks and security to create efficient, agile, extensible logical constructs that meet the performance and scale requirements of virtualized datacenters.

vCloud Networking and Security delivers software-defined networks and security with a broad range of services in a single solution (see Figure 1). It includes a virtual firewall, virtual private network (VPN), load balancing and VXLAN-extended networks. Management integration with VMware vCenter Server™ and VMware vCloud Director® reduces the cost and complexity of datacenter operations and unlocks the operational efficiency and agility of private cloud computing.

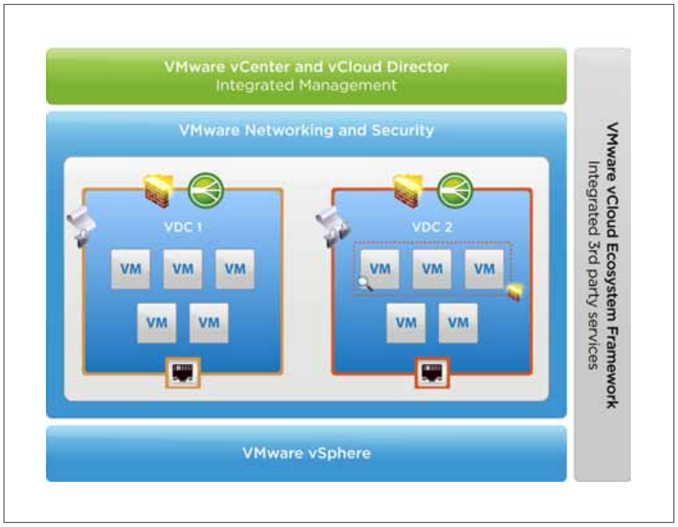

VMware vCenter and vCloud Director
Integrated Management
VMware Networking and Security
VDC 1
VM
VM
VM
VM
VM
VDC 2
VM
VM
VM
VM
VM
VMware vSphere
VMware vCloud Ecosystem Framework
Integrated 3rd party services

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 datacenter 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 and 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 datacenter. Site-to-site VPN support links virtual datacenters and enables hybrid cloud computing at low cost. The SSL VPN capability delivers remote administration into the virtual datacenter through a bastion host, the method favored by auditors and compliance regulators
- **Load Balancer** – A virtual load balancer to scale application delivery without the need for dedicated hardware. Placed at the edge of the virtual datacenter, the load balancer supports Web, SSL and TCP-based scale-out for high-volume applications.
- **VXLAN** – Enabling technology for network virtualization, providing network abstraction, elasticity and scale across the datacenter. VXLAN provides an architecture for organizations to scale applications across clusters and pods without any physical network reconfiguration.
- **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** – Integrated management with vCenter Server and vCloud Director provides 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.

vCloud Networking and Security is available in two editions, Standard Edition and Advanced Edition. Building on Standard Edition, the Advanced Edition adds high availability for Edge firewall, load balancing, and Data Security for Microsoft Windows services to deliver a complete solution (See Figure 2).

	VCLOUD NETWORKING AND SECURITY	
	vCloud Networking and Security Standard	vCloud Networking and Security Advanced
Features		
Firewall	●	●
Virtual Private network (VPN)	●	●
VXLAN	●	●
vCloud Ecosystem Framework	●	●
Network Address Translation (NAT)	●	●
Dynamic Host Config. Protocol	●	●
High Availability (HA)		●
Load Balancing		●
Data Security		●
Endpoint	(Bundled in vSphere 5.1)	

Figure 2. vCloud Networking and Security Editions

Architecture

vCloud Networking and Security is built with virtual security appliances. Network traffic from virtual workloads is passed through these appliances, which apply services such as firewalling 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 datacenter. It provides a wide range of services, including a highly available stateful inspection firewall, IPsec site-to-site VPN, a server-load balancer, network-address translation and network services including static routing, DHCP and domain name system (DNS). The Edge Gateway also acts as a VXLAN gateway, bridging VXLAN networks and traditional VLANs. A second type of virtual appliance, App Firewall, provides protection directly in front of one or more specific workloads (e.g., virtual machines).

This flexibility in firewalling 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 firewalled, regardless of its source. In contrast, if a virtual domain is being created for a lab environment, IT may choose to deploy firewalling 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 into the corporate network from outside the domain.

vCloud Networking and Security is built on top of VMware 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 software-defined networks and security with a broad range of services in a single solution.

Firewalling

vCloud Networking and Security Edge and App Firewalls are tightly integrated into vSphere and rely heavily on vCenter objects in policy creation (see Figure 3). For example, vCenter objects including workloads, port groups and virtual networks can be selected directly in the firewall-rule table. 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 datacenter with Edge, or directly in front of a workload at the vNIC level with App firewall. Regardless of the enforcement point, vCloud Networking and Security firewalling performs stateful packet inspection at high performance and low latency.

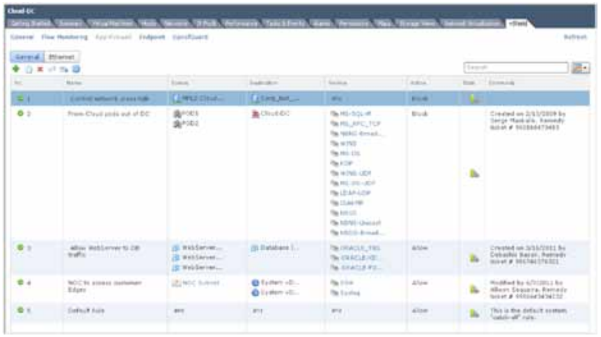


Figure 3. Intuitive Firewall Rules with vCenter and vCloud Director Objects

vCloud Networking and Security Edge includes multiple virtual network interfaces that give security architects much more flexibility in designing software-defined networks (see Figure 4). Edge interfaces can be used to segment virtual networks and provide connectivity to multiple VLANs deployed on the physical network.

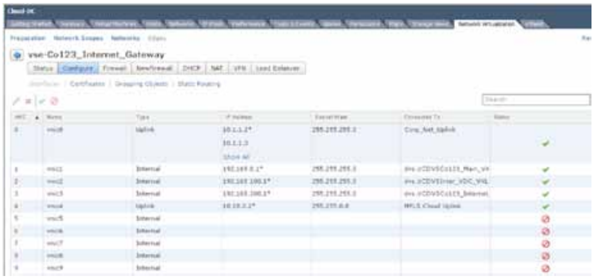


Figure 4. Multiple Interfaces for Network Segmentation

Network Address Translation (NAT)

vCloud Networking and Security Edge incorporates a flexible network address translation (NAT) engine that can map network and port addresses using a familiar original and translated configuration model (see Figure 5). 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.

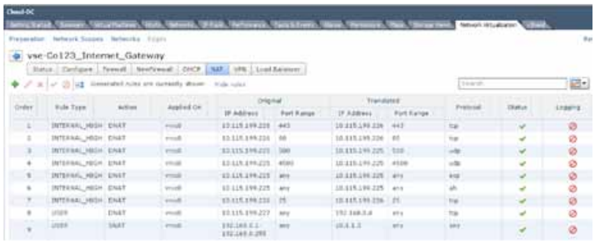
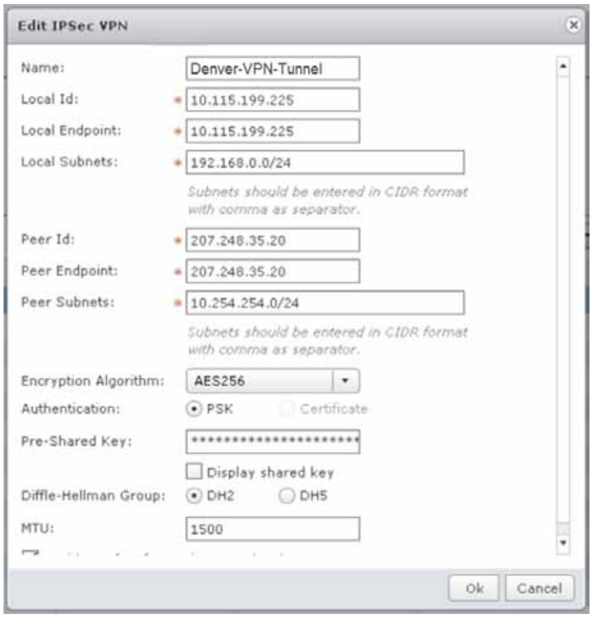


Figure 5. Flexible NAT Engine

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 6). This capability enables customers to interconnect virtual datacenters securely to physical firewalls from a variety of vendors.



Edit IPSec VPN

Name: Denver-VPN-Tunnel

Local Id: * 10.115.199.225

Local Endpoint: * 10.115.199.225

Local Subnets: * 192.168.0.0/24

Subnets should be entered in CIDR format with comma as separator.

Peer Id: * 207.248.35.20

Peer Endpoint: * 207.248.35.20

Peer Subnets: * 10.254.254.0/24

Subnets should be entered in CIDR format with comma as separator.

Encryption Algorithm: AES256

Authentication: ● PSK ○ Certificate

Pre-Shared Key: ********************

□ Display shared key

Diffie-Hellman Group: ● DH2 ○ DH5

MTU: 1500

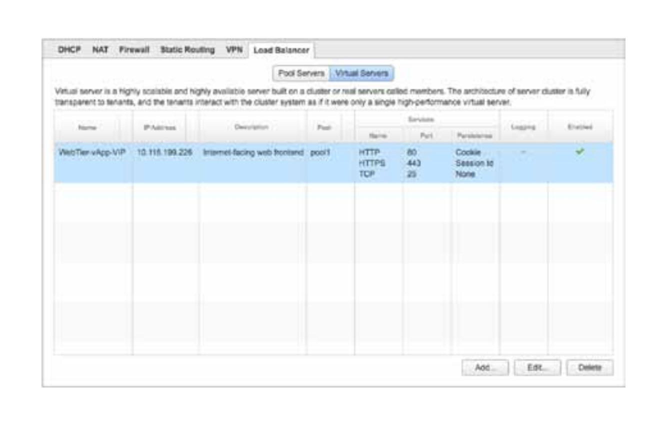
Figure 6. Secure IPsec Site-to-Site VPN Connectivity

SSL

vCloud Networking and Security also incorporates SSL remote access to give administrators access to the virtual datacenter. 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 via a jumpbox or bastion host, the method preferred by most security specialists and auditors. This approach minimizes the attack surface into the virtual domain and makes auditing administrative activity easier and more robust.

Load Balancer

vCloud Networking and Security Advanced Edition adds powerful server load–balancing capabilities to increase availability and performance of business-critical applications (see Figure 7). A variety of load-balancing algorithms are supported, including round-robin, cookie-based and session-based alternatives.



Virtual server is a highly scalable and highly available server built on a cluster or real servers called members. The architecture of server cluster is fully transparent to tenants, and the tenants interact with the cluster system as if it were only a single high-performance virtual server.

Name	IP Address	Description	Pool	Services			Logging	Enabled
				Name	Port	Persistence		
WebTier-vApp-VIP	10.115.199.226	Internet-facing web frontend	pool1	HTTP HTTPS TCP	80 443 25	Cookie Session Id None	-	✓

Figure 7. vCloud Networking and Security Server Load Balancing

Edge High Availability

vCloud Networking and Security Advanced Edition enables stateful high-availability (HA) firewalling for virtual datacenters (see Figure 8). With 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 passing traffic in less than 10 seconds. With this level of availability, administrators gain the confidence to virtualize business-critical applications.

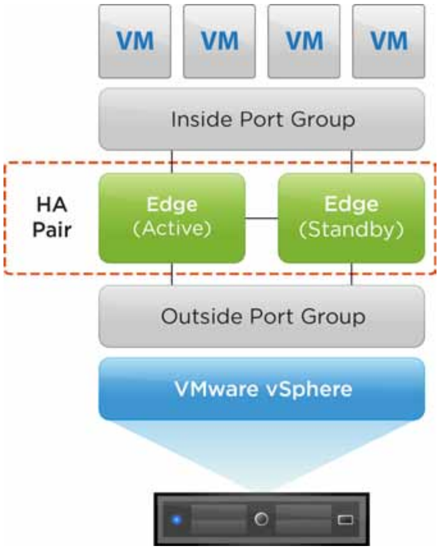


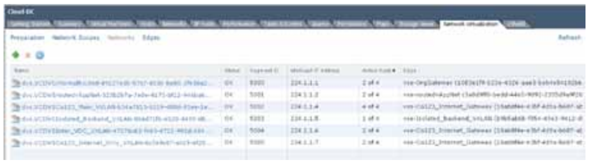
Figure 8. Edge Stateful HA Firewall

Data Security

vCloud Networking and Security Advanced Edition includes Data Security for Microsoft Windows. The solution scans Windows (CIFS) file servers for sensitive data that matches predefined templates, such as credit card or social security numbers. A wide variety of international sensitive data formats are available. Data Security is typically used to locate data that has been stored on file shares without proper access controls or auditing.

VXLAN

vCloud Networking and Security supports software-defined networking with the innovative VXLAN protocol, which provides elastic scale in the datacenter (see Figure 9). VXLAN makes it easy to deploy workloads anywhere in the datacenter without pod or cluster constraint worries. The VXLAN protocol leverages user datagram protocol (UDP) encapsulation to enable the software-defined network to stretch across multiple clusters and Layer 3 segments of the datacenter. 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, enabling efficiency and "single pane of glass" management of the software-defined network. vCloud Networking and Security Edge performs VXLAN-to-VLAN gateway translations to allow simple migration to software-defined networking. In addition, the vSphere Distributed Switch component of vSphere Enterprise Plus Edition has been enhanced to provide troubleshooting and traffic statistics about VXLAN encapsulated traffic.



Preparation Network Scopes Networks Edges Refresh

Name	Status	Segment ID	Multicast IP Address	Active hosts	Edges
[illegible]	OK	5000	224.1.1.1	2 of 4	[illegible]
[illegible]	OK	5001	224.1.1.2	2 of 4	[illegible]
[illegible]	OK	5002	224.1.1.4	4 of 4	[illegible]
[illegible]	OK	5003	224.1.1.5	1 of 4	[illegible]
[illegible]	OK	5004	224.1.1.6	2 of 4	[illegible]
[illegible]	OK	5005	224.1.1.7	2 of 4	[illegible]

Figure 9. 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 the vCloud Ecosystem Framework, the APIs allow network-level access to data flows at either the vNIC or the virtual datacenter 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, while a pure monitoring tool (e.g., a packet capture tool) requires only a copy of the traffic. The framework also supports third-party products implemented as either hardware or virtual appliances.

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. The vCloud Networking and Security APIs work with vCenter Server and vCloud Director APIs to provide not just dataflow access, but true orchestration. Third-party solution providers can include configuration templates in vCloud Director workflows so that vCloud administrators can access the product's rich capabilities in a single interface.

Key Benefits

vCloud Networking and Security lowers operational costs, increases agility and flexibility and extends to include 3rd party services.

Lower Operational Costs

vCloud Networking and Security delivers software-defined networking and security with tightly integrated provisioning and application life-cycle management. The solution abstracts networking and security from the underlying physical network hardware and enables organizations to pool these resources and then consume them on demand. Virtual networks can be programmatically provisioned, attached to workloads, and placed, moved or scaled on demand—without the need for physical network reconfiguration. vCloud Networking and Security simplifies operations by reducing VLAN-related management overhead. Since virtual networks can span physical boundaries, compute resources can be optimally utilized across noncontiguous clusters or pods.

By transforming the networking and security infrastructure from hardware to software constructs that are integrated with provisioning in vCenter Server and vCloud Director, vCloud Networking and Security eliminates the need for dedicated hardware. This approach simplifies operations and reduces datacenter power, cooling and rack space requirements.

Increased Agility and Flexibility

Unlike hardware-based alternatives, vCloud Networking and Security enables organizations to create networks that scale with applications and to position security services exactly where they are needed. VXLAN creates highly scalable virtual networks that support any-to-any connectivity for load balancing, VMware vSphere Fault Tolerance and VMware vSphere vMotion®—in almost any type of application architecture. Organizations can create network architectures that support elastic allocation of compute resources across clusters or pods without physical network reconfiguration (see Figure 10). As networks are virtualized, security, load-balancing and other gateway services are fully aligned and integrated with the new paradigm to ensure maximum agility and utilization. Greater visibility into traffic flows enables easier policy creation. Organizations can segment in-scope workloads for continuous compliance, maintaining trust zones for sensitive data.

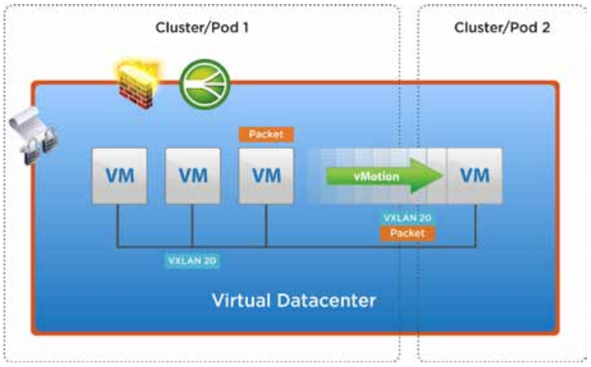


Figure 10. Workload Mobility Across Clusters and Pods

Extensibility and Choice

vCloud Networking and Security provides an open architecture with industry-standard APIs to enable freedom of choice and avoid vendor lock-in. Because the solution allows third-party service insertion (see Figure 11), organizations can easily take advantage of new technology, integrating operational workflows with existing systems and procedures. IT can also deploy consistent best-of-breed solutions across physical and virtual environments. With vCloud Networking and Security, organizations can finally couple existing investments in networking and security solutions with virtualization and cloud efficiency and agility.

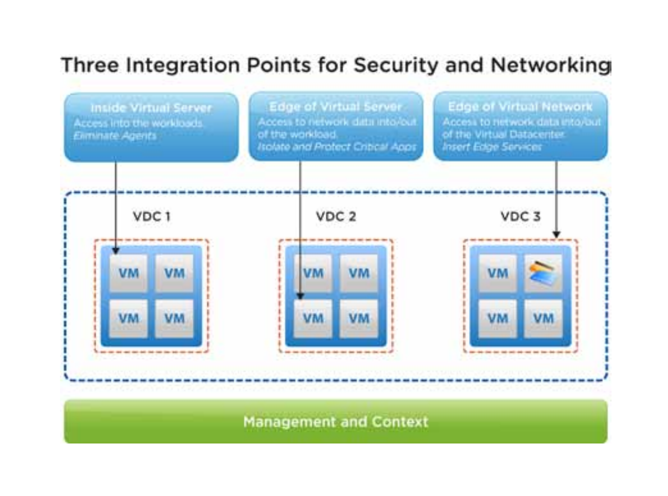

Three Integration Points for Security and Networking
Inside Virtual Server
Access into the workloads.
Eliminate Agents
Edge of Virtual Server
Access to network data into/out of the workload.
Isolate and Protect Critical Apps
Edge of Virtual Network
Access to network data into/out of the Virtual Datacenter.
Insert Edge Services
VDC 1
VDC 2
VDC 3
VM
Management and Context

Figure 11. vCloud Ecosystem Framework for Inserting Third-Party Services

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 (see Figure 12). 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

- Easy segmentation of applications belonging to different trust levels in the same virtual datacenter
- Greater visibility and control over network communications between virtual machines for instrumentation and compliance
- Agile policy enforcement based on logical constructs, and not on infrastructure constructs such as IP addresses or VLANs

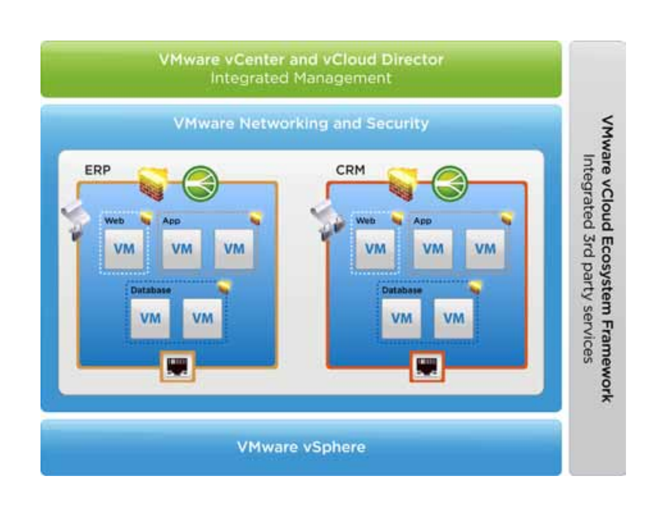

VMware vCenter and vCloud Director
Integrated Management
VMware Networking and Security
ERP
CRM
Web
App
Database
VM
VMware vSphere
VMware vCloud Ecosystem Framework
Integrated 3rd party services

Figure 12. Protected and Isolated Business-Critical Applications

Build Agile and Secure Private Clouds

vCloud Networking and Security delivers an operationally efficient, simple, cost-effective networking and security solution that meets the efficiency and scale requirements of private clouds and virtual datacenters. VXLAN-based logical networks can be deployed and scaled on demand without physical network reconfigurations. Since networks can span physical boundaries, organizations can optimize management and use of compute resources. Simplified deployment through an intuitive user interface and an automation API model enables organizations to set up the infrastructure for a new business unit in minutes (See Figure 13).

Integrated firewall and gateway services secure the perimeter of the virtual datacenter and provide services such as firewalling, 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

- Support multitenant IT environments easily
- Increase use of compute capacity where available, across clusters with VXLAN
- Secure the edge of the virtual datacenter with an integrated firewall, load balancer and VPN
- Promote efficiency by automating security management through vCloud Networking and Security management APIs
- Maximize performance by integrating best-of-breed third-party solutions

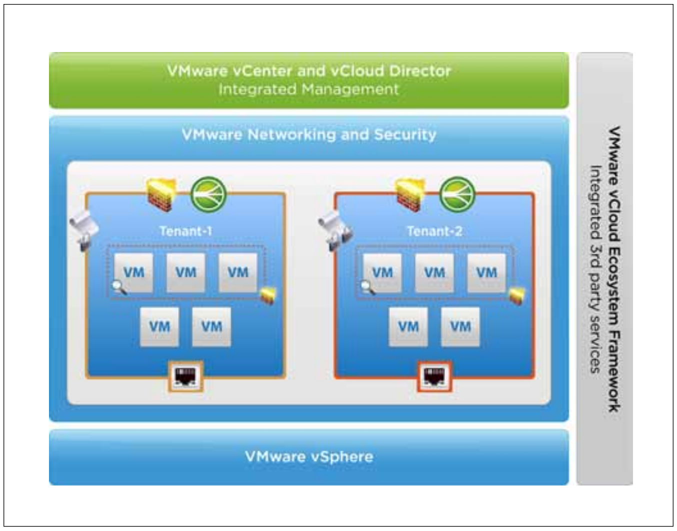

VMware vCenter and vCloud Director
Integrated Management
VMware Networking and Security
Tenant-1
Tenant-2
VM
VMware vSphere
VMware vCloud Ecosystem Framework
Integrated 3rd party services

Figure 13. Agile and Secure Private Cloud

Secure Virtual Desktop Infrastructure Deployments

vCloud Networking and Security enables granular and efficient access control in virtual desktop infrastructure (VDI) environments, such as VMware View™. vCloud Networking and Security can be used to 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 into the broader virtual datacenter (see Figure 14). 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 datacenter

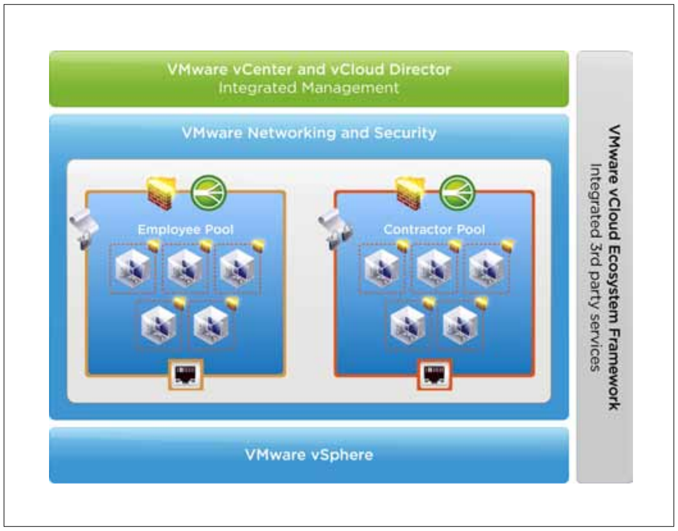

VMware vCenter and vCloud Director
Integrated Management
VMware Networking and Security
Employee Pool
Contractor Pool
VMware vSphere
VMware vCloud Ecosystem Framework
Integrated 3rd party services

Figure 14. Secure VDI Deployments

Gain Agility and Efficiency with vCloud Networking and Security

IT is undergoing rapid transformation, with datacenters moving toward a service-oriented, software-defined model. enables IT to move from rigid networking and security architectures, fragmented management, and manual provisioning to a new model of virtual networks and security, where automation and operations are integrated with the rest of the virtual datacenter. In contrast to other networking and security products, vCloud Networking and Security delivers the levels of efficiency and agility enterprises require to realize the benefits of cloud computing. Only vCloud Networking and Security enables you to build your cloud—the right private, public and hybrid cloud to meet business needs—without compromise.

Using vCloud Networking and Security, organizations can virtualize business-critical applications with confidence, build secure and agile private clouds and protect their virtual desktop infrastructure solutions. They can gain the efficiency and agility of cloud computing while improving flexibility and control. vCloud Networking and Security accelerates IT, so that IT can accelerate the business.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com