# VMware vCloud® Networking and Security

## Efficient, Agile and Extensible Software-Defined Networks and Security

BROCHURE

vmware®

## 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 unlocking datacenter agility, VMware offers 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

Current network and security architectures have not kept pace with the virtualization of the datacenter. They are rigid and complex, and they create a costly barrier to realizing the full agility customers are hoping to achieve with cloud infrastructure. Limitations of physical networks and security tie an increasingly pooled dynamic virtual world back to inflexible, dedicated hardware, creating artificial obstacles to optimizing network architecture and capacity utilization.

Although a virtual machine can be provisioned in a matter of minutes, "surrounding" it with all the necessary network and security services still takes days or weeks because network and security operations remain dependent on manual provisioning. Today's manually constructed VLANs meander through numerous switches, each with its own difficult-to-manage vendor-specific command-line interface. Dedicated physical appliances for security, load balancing and gateway services add to the complexity of the infrastructure. In addition, network and security management is not programmatically integrated with the operations of the virtual datacenter.

As a result, current network and security architectures not only reduce efficiency, but also limit the ability of enterprises to rapidly deploy, move, scale and protect applications and data according to business needs.

*"It takes us four weeks just to provision a VLAN!"*

— IT administrator at a large e-commerce company

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.

| TO OPERATE EFFECTIVELY, A VIRTUAL WORKLOAD NEEDS |
|---|
| • Connectivity |
| • Isolation and security |
| • Monitoring |
| • Performance, including load balancing |
| • Network services |
| • Resiliency and high availability |

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.

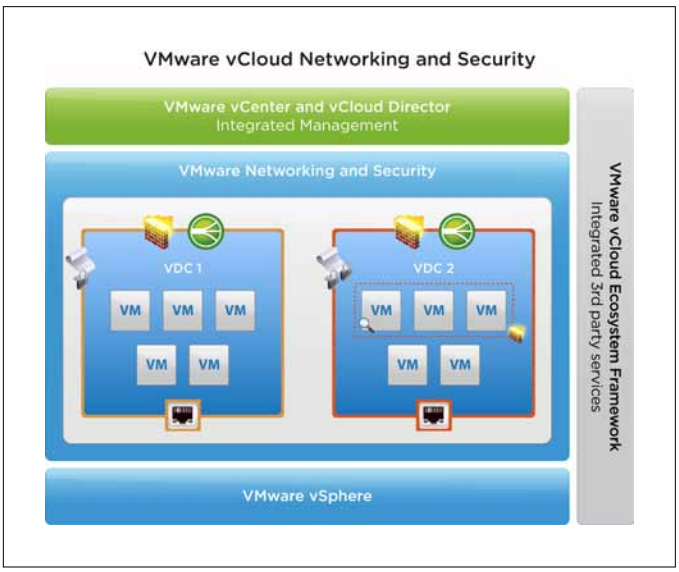


**Figure 1.** vCloud Networking and Security Solution Overview

### 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 to scale applications across clusters and pods without any physical network reconfiguration.
- **Data Security** - Scans Windows (CIFS) file servers for sensitive data and reports violations of regulations (such as PCI-DSS), enabling IT to assess the state of compliance with regulations from around the world.
- **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 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.

| SOFTWARE-DEFINED NETWORKING AND SECURITY CHECKLIST | |
|---|---|
| Distributed Virtual Switch | ✓ |
| 3rd Party Service Insertion | ✓ |
| Extensible Networks | ✓ |
| Integrated Firewall | ✓ |
| Integrated VPN | ✓ |
| Integrated NAT | ✓ |
| Integrated DHCP | ✓ |
| Active / Standby HA | ✓ |
| Integrated Load Balancing | ✓ |
| Workload Isolation and Segmentation | ✓ |

## 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. Just as vSphere virtualizes compute by abstracting and pooling the resources, vCloud Networking and Security virtualizes networking and security. It abstracts networking and security from the underlying physical network hardware and enables organizations to pool these resources and then consume them on demand. VXLAN 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 securityy infrastructure from hardware to software constructs integrated in a single solution, vCloud Networking and Security eliminates the need for dedicated hardware and reduces datacenter power, cooling and rack space requirements. Operations are greatly simplified with provisioning integrated in vCenter Server and vCloud Director (See Figure 2).

*"Our existing provisioning process for new customers requires either configuring a dedicated physical firewall or placing customers on a shared physical firewall with a limited feature set. vCloud Networking and Security Edge will allow us to rapidly provision new firewalls, prevent device sprawl and still provide our customers with the core firewall capabilities that they require."*

— Systems engineer at a datacenter and cloud solutions provider for small and medium businesses

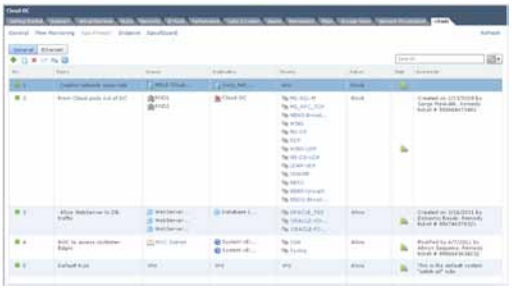

**Figure 2.** Simple, Intuitive Firewall-Rule Table

### 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 3). 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.

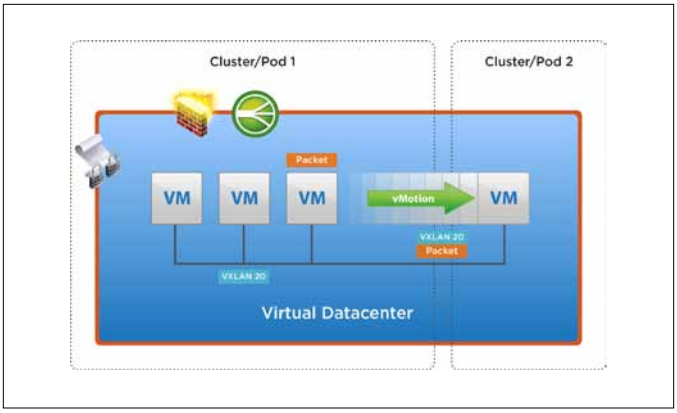


**Figure 3.** Workload Mobility Across Clusters and Pods

*"vCloud Networking and Security enables greater agility. VXLAN helps simplify the physical network, and Edge reduces our dependency on physical gear and provides greater flexibility."*

— Kevin Barrass, SVDC Technical Lead, YHMAN

### 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. The solution provides service insertion at the vNIC and the virtual edge to allow supported third-party products to access both traffic flows and workload context without significant software development (see Figure 4). Now 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.

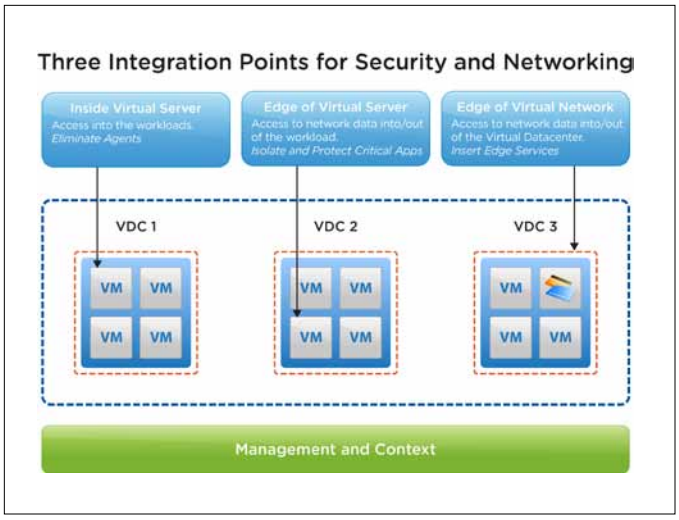


**Figure 4.** vCloud Ecosystem Framework for Inserting Third-Party Services

*"iLand is impressed with the software-defined network constructs that vCloud provides. iLand has been using functionality like vShield Edge since its inception. From critical VPN connectivity in the cloud to protecting 400 virtual machine web farms, the vShield Edge has proven itself as an agile and effective security appliance. With VXLAN, the added new functionality and scale of the Edge gateway in vCloud Networking and Security, we are going to further our operational efficiencies and simplify our physical network bringing greater agility in deploying and scaling new tenants across our large compute farms."*

— Justin Giardina, CTO iLand Internet Solutions Corporation

### 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 secure their virtual desktop solutions.

### Protect and Isolate Business-Critical Applications

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 5). 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

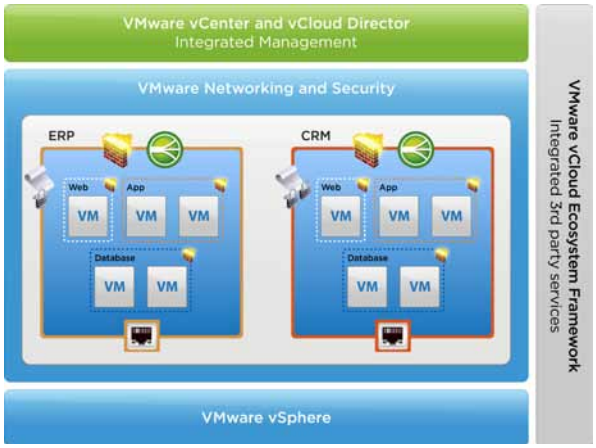


**Figure 5.** Virtualize Business-Critical Applications with Confidence

### 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.

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

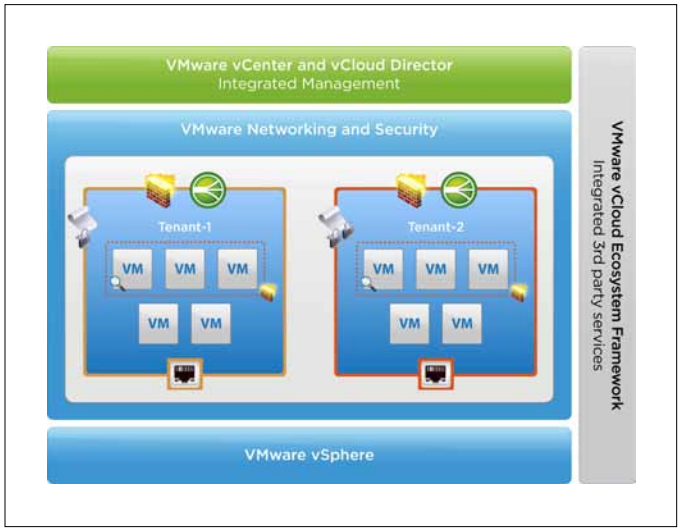


**Figure 6.** Agile and Secure Private Clouds

## 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 7). 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

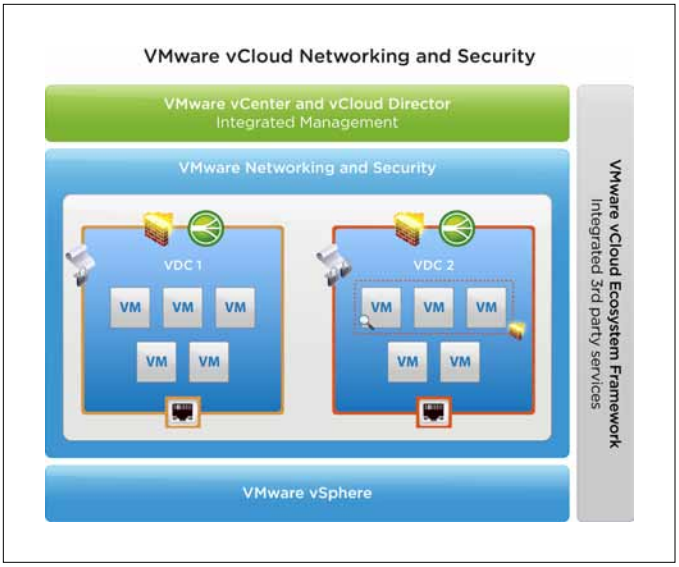


**Figure 7.** Secure VDI Deployments

## Gain Agility and Efficiency with vCloud Networking and Security

IT is undergoing rapid transformation, with datacenters moving toward a service-oriented, software-defined model. vCloud Networking and Security 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 agile and secure 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.

## Compare Editions

Table 1 compares the features included in the vCloud Networking and Security editions.

| | 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 vShpere 5.1) | |

**Table 1.** vCloud Networking and Security Editions

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