SOLUTION BRIEF

Deliver the Most Secure and Agile Cloud with VMware

VMware virtualization has transformed the datacenter by driving both efficiency and flexibility to respond to business needs. However, legacy network and security solutions have not kept pace with this transformation. They are rigid and complex, and they create a costly barrier to realizing the full agility of cloud computing.

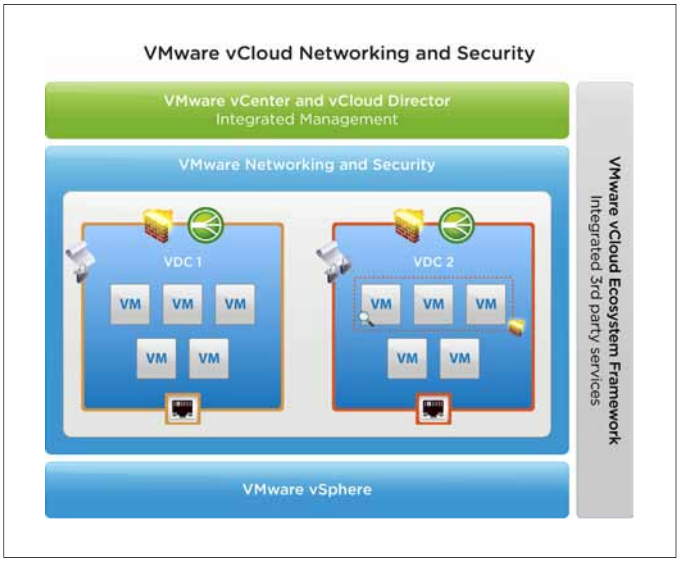
VMware vCloud® Networking and Security solves these datacenter challenges by delivering software-defined networking and security. vCloud Networking and Security enhances operational efficiency, unlocks agility and is extensible to rapidly respond to business needs. It provides a broad range of services in a single solution, including virtual firewall, VPN, load balancing and VXLAN extended networks while also providing a comprehensive framework to integrate third-party solutions.

The VMware networking and security strategy is to focus our solutions and those of our ecosystem partners on supporting specific initiatives critical to accelerating the migration to the cloud. Three initiatives are necessary to realize the benefits of cloud computing, but they must be architected to ensure that data is protected and compliance and audit controls are maintained.

The three initiatives are

- Virtualizing Business Critical Applications
- Creating Virtual Private Clouds and Datacenters
- Virtualizing Desktops

This solution brief describes the security and compliance considerations for each of these initiatives, and how VMware solutions and products address them.


VMware vCloud Networking and Security
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

Solution Overview

Protect Business-Critical Applications

As organizations continue their journey to the cloud they virtualize more of their business-critical applications, and ensuring the security of these applications becomes a crucial step in cloud adoption. In a virtual environment, organizations need to have visibility of traffic between virtual workloads. They need their critical applications and databases protected from threats from less secure or unpatched systems. And they need to implement audit and compliance controls on in-scope hosts. The challenge is to ensure security and compliance while still maintaining flexibility and the ability to scale rapidly.

VMware solutions support compliance objectives and protection of applications in the virtual datacenter, without compromising the benefits of cloud computing. They allow organizations to create business-based security groups and protect critical applications from network-based threats. The hypervisor-level firewall in vCloud Networking and Security provides adaptive security that travels with virtual machines as they migrate from host to host, so that enterprises can securely support their virtual applications in dynamic cloud environments. This approach makes it easy for customers to support applications belonging to different trust levels in the same virtual datacenter and ensures that proper segmentation and trust zones are enforced for all application deployments. Organizations gain visibility into and control over network communications between virtual machines. Policy enforcement is agile, because it is based on logical constructs centered on the workloads to be protected, and not on infrastructure constructs such as IP addresses or VLANs.

Ensuring configuration compliance of the underlying VMware infrastructure and in-scope virtual servers is another critical concern of organizations deploying business-critical applications to the cloud. VMware vCenter™ Configuration Manager™ is a full-featured server-configuration and compliance-management solution. It automates critical configuration and compliance-management tasks including configuration-data collection, change execution and reporting; change auditing; compliance assessment; patch management; OS provisioning; and software package distribution. vCenter Configuration Manager capabilities ensure the infrastructure that underlies your business-critical applications is hardened against security best practices, vendor hardening guidelines, and regulatory mandates such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX).

Finally, a shared virtual infrastructure raises concerns about the ability of an organization to identify and protect sensitive business information. Exposure or leakage of such data—for example, credit card information or personal health information—can cost an enterprise millions of dollars or harm its reputation. The Data Security component of vCloud Networking and Security enables organizations to identify sensitive business information on unstructured file shares and ensure that it is protected. With a large number of predefined templates for country- and industry-specific regulations, it quickly identifies and reports on sensitive data exposures. It also improves performance by offloading data-discovery functions to a virtual appliance.

These capabilities, along with trusted solutions from VMware partners, ensure that VMware based solutions provide the strongest possible protection for your critical applications and data.

Secure Your Private Cloud

Today more and more organizations are leveraging the benefits of private cloud computing to increase flexibility and reduce costs. Yet many have not changed their traditional approach to architecting networks and security. Physical networking and security topologies severely limit flexibility and the ability to scale. They are not virtualization-aware, making it all too easy to become noncompliant as changes occur in a dynamic infrastructure. Also, a heavy reliance on hardware-based solutions leaves organizations with multiple special-purpose appliances, each with its own interface. The lack of a common management interface adds to the cost and complexity of maintaining the security of virtual datacenters.

VMware solutions reduce the complexity of private clouds by enabling organizations to virtualize their networking and security infrastructures and manage them with the same interface used to provision the private cloud itself. VXLAN-based logical networks can be deployed and scaled on demand without physical network reconfigurations. Because VXLAN-based networks can span physical boundaries, organizations can optimize management and utilization of compute resources across physical network boundaries. A simplified deployment model with an intuitive user interface and automation APIs allows organizations to stand up the infrastructure for a new business unit in a matter of minutes.

The Edge component of vCloud Networking and Security delivers an operationally efficient, simple and cost-effective security-services gateway to secure the perimeter of the virtual datacenter. Edge makes it easy for enterprises and cloud service providers to support multitenant IT environments and safely share network resources by creating logical security zones that provide complete network isolation for virtual datacenters. The Edge virtual appliance delivers gateway services such as firewall and network address translation (NAT), load balancer, VPN and DHCP. Fully integrated with VMware vCenter Server™ and VMware vCloud Director®, Edge enables role-based access control and separation of duties as part of a unified framework for managing virtualization security.

Secure Virtual Desktop Deployments

Virtual Desktop (VDI) deployments are growing rapidly, but VDI introduces new security challenges. Since virtual desktop solutions consolidate desktop processing onto centralized servers, resource-intensive tasks like virus scanning can have a significant impact on performance, necessitating additional server hardware and resulting in lower consolidation ratios. Virtual desktops also need proper access controls, to limit third-party extranet users from accessing internal resources that they shouldn't.

VMware enables optimized antivirus and anti-malware security for virtual environments via integration with VMware partners. Endpoint, part of vShpere 5.1, allow security technology partners to offer more efficient antivirus and anti-malware protection for virtual hosts, including VMware View™ desktops. It does so by offloading antivirus and anti-malware functions from individual virtual machines to a centralized secure virtual appliance that protects the host and all virtual machines on it. This approach streamlines security management and provides added protection against antivirus "storms," performance bottlenecks and botnet attacks.

In order to control access within VDI environments, the App component of vCloud Networking and Security is used to create logical security perimeters around virtual desktops. This capability ensures that VDI users can only access applications and data they are authorized to use. It also prevents unauthorized access into the VDI desktops from the rest of the network.

Learn More

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

For detailed information about VMware security and compliance solutions, product specifications and systems requirements, please visit www.vmware.com/go/vcns.

vmware®

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