CHEAT SHEET—INTERNAL USE ONLY

VMware vCloud Networking and Security

Sales and Partner Use Only

What is the VMware vCloud Networking and Security Product?

VMware has combined its security and advanced networking capabilities into a single product: VMware vCloud® Networking and Security. vCloud Networking and Security includes the products originally known as VMware vShield™ App™ and vShield Edge™, and the new networking technology called VXLAN. Note that vCloud Networking and Security does not include VMware vShield Endpoint™ or the Virtual Distributed Switch (VDS). As of vSphere 5.1, Endpoint is now included in vSphere, while the VDS remains in vSphere Enterprise Plus, as before.

What is the vCloud Networking and Security Elevator Pitch?

vCloud Networking and Security is the leading software-defined networking (SDN) and security solution that enhances operational efficiency, unlocks agility and enables extensibility 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. Management integration with VMware vCenter™ and vCloud Director™ reduces the cost and complexity of datacenter operations and unlocks the operational efficiency and agility of private cloud computing.

vCloud Networking and Security Product Family

There are two editions of the vCloud Networking and Security product.

vCloud Networking and Security Standard includes the following features: VXLAN, NAT, DHCP, Edge virtual Firewall, VPN and vCloud Ecosystem Framework for third-party integration.

vCloud Networking and Security Advanced is a superset of the standard edition. Extra features include: Load Balancing, Edge high Available Virtual Firewall, Data Security, and industry certifications.

vCloud Networking and Security is available either stand-alone, or as part of the vCloud Suites. The vCloud Networking and Security editions are licensed on a per virtual machine basis when sold stand-alone, and on a per-processor basis when sold as part of a VMware vCloud Suite.

vCloud Networking and Security

	VCLOUD NETWORKING AND SECURITY STANDARD	VCLOUD NETWORKING AND SECURITY ADVANCED
Pricing and Licensing		
• Price per VM	$150	$250
• List Price (license only)	$3,750	$6,250
• Included Licenses	25 VMs	25 VMs
Products and Features		
• Firewall*	•	•
• Virtual Private Network (VPN)	•	•
• VXLAN	•	•
• vCloud Ecosystem Framework	•	•
• Network Address Translation (NAT)	•	•
• Dynamic Host Configuration Protocol	•	•
• High Availabiity (HA)		•
• Load Balancing		•
• Sensitive Data Discovery		•
• Endpoint	(Bundled in vSphere 5.1)	

* Includes Edge and Application firewall

Relationship to vCloud Suite Packaging and Pricing

The **vCloud Networking and Security Standard** edition is included in **vCloud Standard Suite**, while **vCloud Networking and Security Advanced** is in the **vCloud Advanced and Enterprise suites**.

The vCloud Suites are licensed on a per-processor basis.

What is VXLAN?

As IT organizations to move to a converged infrastructure and service-oriented model, many are finding that current datacenter networking architectures are a limiting factor. VLAN-based switching models have a long history, but suffer from the following challenges in the datacenter:

- Inflexibility: VLAN and switching boundaries are not flexible nor easily extensible. As requirements grow or shrink, compute and storage resources need to be allocated without major operational overhead.
- Fault Tolerance: High-availability technologies such as VMware vSphere® Fault Tolerance work best with “flat” Layer 2 networks, but creating and managing this architecture can be operationally difficult, especially at scale.
- VLAN and IP Address Management: IP address maintenance and VLAN limits become challenges as the datacenter scales, particularly when strong isolation is required or in service provider environments.

VXLAN can solve these challenges. VXLAN is a method for “floating” virtual domains on top of a common networking and virtualization infrastructure. By leveraging industry-standard Ethernet technology, large numbers of virtual domains can be created above an existing network, with complete isolation from each other and the underlying network.

VXLAN offers the following benefits:

- Flexibility: Datacenter server and storage utilization is maximized through the support of “stretched clusters” that cross switching and pod boundaries.
- Streamlined Network Operations: VXLAN runs on standard Layer 3 IP networks, eliminating the need to build and manage a large Layer 2 underlying transport layer.
- Investment Protection: VXLAN runs over standard switching hardware, with no need for software upgrades or special code versions on the switches.

VXLAN should be targeted at large enterprises and service provides. It is implemented using a combination of new software integrated in vSphere 5.1, and requires the VDS in vSphere Enterprise Plus.

Primary Sales Motions

vCloud Networking and Security can be sold as a standalone product or as a component of a vCloud Suite. **In general, try to sell as part of a suite, using the following justifications**:

1. The vCloud suites enable both IT operational efficiency and private cloud computing in a single package.
2. Suite pricing is per-processor. This is easier for the customer to deal with, and also provides increased value and predictable costs the greater their consolidation ratio.
3. The suites provide a lower-cost method to purchase the products in the suite as compared to buying them individually.

As a rule, fall back to selling stand-alone vCloud Networking and Security only if you are unable to close the suite sale.

Example Sales Scenarios and Selling Tips

SALES SCENARIO	KEY BUYERS	SELLING TIPS
Information Security raising concerns about security or audit/compliance of the VMware infrastructure	IT Operations Info Sec	**Carve out $$ from compliance and security budget**: vCloud Networking and Security provides workload isolation, visibility, and insertion of third-party security products such as IPS. vCloud Networking and Security is a better choice than traditional security solutions because of its tight integration with vCenter and vCD management
Public Cloud Threat – IT group concerned about loss of relevance of enterprise data center: Execs and lines of business are debating the benefits of moving to public cloud	CIO, VP of IT Operations, CFO	IT Infrastructure team can justify the enterprise datacenter based on security and compliance that may not be available in public cloud offerings. vCloud Networking and Security enables consistent security and compliance controls
Enterprise customer interested in building a secure private cloud quickly	CIO, VP of IT Operations	Focus on vCloud Suite – provides vCD integration and third- party integration with security and scalable LANs for features such as vMotion and vSphere Fault Tolerance

SALES SCENARIO	KEY BUYERS	SELLING TIPS
Enterprise customer interested in protecting business critical applications deployed on vSphere	CIO, VP of Infrastructure	vCloud Networking and Security provides a virtualization aware firewall to protect business critical applications. Security policies can be applied at a container or VM level
Enterprise customer interested in protecting View deployments on vSphere	CIO, VP of IT Operations	vCloud Networking and Security firewall can protect VMware View™ desktops from internal and external threats, as well as limit access to internal resources by remote View users (e.g. outsource partners)
Enterprise customer interested in scalable Layer 2 datacenter networking within the datacenter or metro cluster	VP of Infrastructure VP/Director of Networking CIO	Discuss VXLAN as an emerging industry standard to build such constructs. Emphasize ease of administration through vCD and vCenter integration, as well as Cisco support for validation

How to Qualify an Opportunity

CUSTOMER CHALLENGE	SALES TRIGGERS	STAKEHOLDERS	QUALIFY IN	QUALIFY OUT
High network and security hardware and operations costs due to VLAN complexity, purpose-built appliances and fragmented management interfaces	• High operational cost • Manual processes • Network boundaries (e.g. between data center pods) cause inefficient allocation of resources	• Infrastructure team • Virtual infrastructure admins	• Target companies that have more than 20% virtualized resources • Datacenter networking under the control of DC infrastructure team, not Networking team	• Requires deep packet inspection firewall
Inability to quickly respond to dynamic business needs due to constraints of networking and security topologies	• Spending a lot of time and money provisioning network and security infrastructure • Planning scale out of the datacenter to accommodate "cloud-bursting" or cyclical demand • Organizations moving to public clouds to improve agility and flexibility	• VI admins	• Companies considering private clouds to improve agility • Companies building trusted private clouds, e.g. banking, online trading, healthcare providers	• Companies unwilling to modify existing networking and security architecture
Lack of choice and flexibility, leading to vendor lock-in and degraded levels of service and performance	• Customer planning a costly rip-and-replace of NW and security infrastructure • Customer wants to maintain physical and virtual infrastructure parity with preferred security or NW partner	• Network and Security Team • Virtual infrastructure team	• Companies considering private clouds with applications that may be accessed by partners or customers • Companies considering building hybrid clouds	* Companies unwilling to modify existing architecture

vCloud Networking and Security Benefits

- Lowers operational cost
  - Optimizes utilization of resources
  - Delivers On-demand adaptive networks without physical network reconfiguration
  - Simplifies provisioning by reducing VLAN related operations and management overhead
- Improves agility and flexibility
  - Ability to deploy and move virtual workloads without physical network re-configuration
  - Ability to scale applications across clusters, pods and metro-clusters
  - Ability to easily add capacity to adapt to business and workload changes and unexpected demands
- Provides extensibility and choice
  - Flexibility to include 3rd party hardware and software services
  - Easily take advantage of latest innovations in technology ecosystem
  - Leverage existing investments

Competitive Landscape Overview

FEATURE	VMWARE VCLOUD NETWORKING AND SECURITY ADVANCED	MICROSOFT HV3	CITRIX XENSERVER	CISCO N1K W/VSG
Switch	✓	✓	✓	✓
Distributed Switch	✓	X	✓	✓
Network Service Insertion	✓	✓	X	✓
VXLAN	✓	X	X	✓
Firewall	✓	X	X	✓
VPN	✓	X	X	X
NAT	✓	X	X	X
DHCP	✓	X	X	X
Active/Standby HA	✓	X	X	X
Traffic Load Balancing	✓	X	X	X
Workload Isolation and Segmentation	✓	X	X	X

Competitive Positioning for Network and Security Virtualization Products

COMPETITOR	STRENGTHS	WEAKNESSES	VMWARE DIFFERENTIATION
Status Quo: Traditional Hardware or Software-based Firewalls			
Cisco, Checkpoint, Juniper, Fortinet	Standard technology in use: Security teams mandate installation of firewalls (typically hardware appliances), connected to virtual infrastructure by VLANs	• Expensive, dedicated hardware/ software solution • High Operational Costs: Expensive and slow to configure to respond to dynamic virtual infrastructure • Poor security if the reality is that the firewalls cannot be applied where they are really needed in the virtual infrastructure ("Doesn't matter how good it is if you can't operationalize it!")	vCloud Networking and Security delivers operationally efficient security for the virtual datacenter or private cloud. It will be much easier to deploy and maintain. It will also result in more effective security because it can easily be configured where security is needed. What used to require physical VLANs and firewalls to isolate critical applications and data, now only requires logical groupings and virtual firewall rules with vCloud Networking and Security. Not only are these security rules simpler to implement, they are easier to manage and do not required dedicated physical appliances. And the vCloud Networking and Security support for security ecosystem partners means that preferred security vendors can be supported where needed
Virtual Security Firewalls/Gateways			
Juniper Virtual Gateway (vGW) (Former Altor virtual firewall)	Juniper is a trusted brand in security	• Juniper vGW is not feature equivalent to their SRX Firewall appliances • Juniper vGW cannot be managed by the security manager which manages the SRX Firewall appliances (so customer will not have consistent firewall management) • Expensive	VMware networking and security delivers robust gateway security services seamlessly integrated with vCenter server and vCloud Director. vCloud Ecosystem Framework for third-party security and networking insertion
Cisco Virtual Services Gateway (VSG)	Cisco is the trusted brand in networking	• N1Kv and VSG require a separate management console (VNMC), vCenter, and CLI configurations in order to operate. • VSG policy model is unique and not user friendly	VMware networking and security delivers robust gateway security services seamlessly integrated with vCenter server and vCloud Director vCloud Ecosystem Framework for third- party security and networking insertion
Cisco ASA 1000v (shipping 2H2012)	Cisco is the trusted brand in networking	• Nexus 1000V virtual switch and ASA 1000v require a separate management console (VNMC), vCenter, and CLI configurations in order to operate • Enterprise security customers manage ASA with Cisco Security Manager (CSM). CSM does not support ASA 1000v	VMware networking and security delivers robust gateway security services seamlessly integrated with vCenter server and vCloud Director. vCloud Ecosystem Framework for third- party security and networking insertion

Comparison of Network Virtualization Protocols

COMPETITOR	BACKERS	STRENGTHS	WEAKNESSES
VXLAN	**VMware,** Cisco, Citrix, Red Hat, Arista, Brcoade, Broadcom, Dell, Emulex, Intel	Supported by Cisco Supported by many hypervisor payers Ability to load balance on standard protocol headers due to use of UDP Plans to support gateway in hardware by major vendors – for cloud scale adoption	Dependency on multicast unattractive to some customers (but objection can be overcome most of the time)
NVGRE (aka Microsoft Network Virtualization)	Microsoft, HP, Dell, Intel, Arista, Emulex	Supported by major server players primarily due to Microsoft relationship	No Cisco support Totally unproven Microsoft has terrible track record for driving networking solutions (e.g. Domain Isolation)

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