VMware NSX Cloud
Hybrid cloud networking and security across private and public clouds

A network built for cloud principles
VMware NSX Cloud delivers networking and security for your applications running natively in public clouds. Together with the VMware NSX family, NSX Cloud enables a virtual cloud network, a software-defined approach to networking that extends across data centers, clouds, endpoints and things.

FIGURE 1: The virtual cloud network.

Use cases
Consistent security across clouds
NSX Cloud enables policy on workloads running across multiple public clouds and on-premises data centers. Policy is defined once and applied to workloads anywhere—across cloud virtual networks, regions, availability zones, and multiple cloud providers. Security policies are dynamically applied to each workload based on application attributes and user-defined tags. Rogue or compromised workloads can even be automatically quarantined if they do not have the right micro-segmentation security policy applied. NSX Cloud supports north-south service insertion, which allows selective traffic to be routed to third-party security appliances for advanced security protection.

Precise control over cloud networking
NSX Cloud is designed for native public cloud environments such as Amazon (AWS) and Microsoft Azure, including AWS GovCloud (US) and Azure Government. NSX Cloud complements the native services available from these public cloud providers. With NSX Cloud, you can continue using the public cloud provider’s infrastructure
and application services for workloads without limitation (e.g., AWS Elastic Load Balancing/Azure Load Balancer, Amazon Route 53/Azure DNS, AWS Direct Connect/ Azure ExpressRoute, and Amazon RDS/Azure Database). Provisioning and configuration management can be automated via REST API requests using your existing automation tools. NSX Cloud also supports gateway consolidation in transit to a VPC/VNet, which allows for simplified operations and the use of built-in services, such as site-to-site VPN as well as third-party edge/transit services.

End-to-end operational control and visibility
NSX Cloud provides standard interfaces and protocols to access the network and security data from cloud networks. Flow, packet and event information is available via IPFIX, Traceflow, port mirroring, and syslog. This data can be consumed by existing on-premises operations tools, and used to enable deep, end-to-end visibility for monitoring, troubleshooting and auditing. This rich operations data helps to dramatically shorten the time it takes to identify and resolve network connectivity, performance and security issues across your entire hybrid cloud deployment, including applications on premises and in the public cloud. NSX Cloud provides granular visibility of public cloud workloads across all VPCs/VNets, a rich search and filter capability for ease of management, and the ability to easily pick and choose workloads to manage with NSX.

Key features
NSX enforced mode – Use NSX tools for consistent security and networking policy enforcement across on-premises and native public cloud workloads.

Cloud enforced mode – Use a public cloud provider’s security and networking constructs for consistent security and networking policy enforcement across on-premises and native public cloud workloads.

Discovery and protection of native public cloud service endpoints – Enable discovery and protection of native public cloud service endpoints in addition to virtual machines (VMs) and Amazon EC2 instances.

Multi-cloud, multi-site networking and security – Bring networking and security capabilities to endpoints across multiple clouds and, by integrating with NSX Data Center, enable networking and security management across clouds and data center sites.

L7 distributed firewall – Gain control over east-west traffic between application workloads running natively in public clouds with stateful firewallsing up to Layer 7 (application identification and distributed FQDN allowlisting). This enables the enforcement of security policies to VMs as well as native services in public clouds.

NSX Cloud also enables micro-segmentation of virtual desktops deployed by VMware Horizon® Cloud Service™ on Azure.

Rich abstraction for security policy definition – Define security groups and rules based on rich policy constructs, such as instance name, OS type, Amazon Machine Image (AMI) ID, and user-defined tags.

Dynamic policy – Automatically apply and enforce security policy based on instance attributes and user-defined tags. Policies automatically follow instances when they are moved within and across clouds.

Quarantine instances – Quarantine rogue and compromised workloads running in the public cloud without micro-segmentation security. Quarantined instances are prevented from communicating on the cloud network, providing multiple layers of security.
FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS
Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit vmware.com/products/nsx-cloud or vmware.com/products, or search online for an authorized reseller.

Service insertion – Selectively route north-south traffic using policy-based routing to a third-party next-generation firewall partner appliance.

Site-to-site VPN – Utilize built-in, high-bandwidth IPsec VPN for secure connectivity to on-premises data centers or between different regions.

Distributed architecture – Eliminate additional network hops and traffic with the NSX Cloud distributed firewalling architecture, which enforces policies at the virtual network interface of each instance rather than routing through an external firewall.

High availability of NSX Cloud components – Deploy all architectural components of NSX Cloud—such as Cloud Service Manager (in case of public cloud deployment) and Public Cloud Gateway appliances—in a high availability configuration.

Shared gateway in transit to a VPC/VNet – Gain support for gateway consolidation in transit to VPCs/VNets, which results in simpler administration, faster onboarding of compute VPCs/VNets, and the ability to insert third-party services.

Edge firewalling – Use stateful firewalling to filter north-south traffic flowing between instances in virtual networks and the public internet.

RESTful API – Programmatically provision and configure networking and security infrastructure on demand via RESTful API and automation tools.

Templating – Use existing automation and orchestration tools to create standardized application templates, and simplify provisioning and management of networking and security services across public clouds.

East-west traffic visibility – Use existing Day 2 operations tools to gain visibility into east-west traffic within and across VPCs.

Security logging – Gain real-time visibility and auditing of security events such as allows/denies and quarantine incidents. Send security event information to a syslog or SIEM server.

Support for AWS GovCloud (US) and Azure Government – Extend NSX networking and security capabilities to AWS GovCloud (US) regions, and have a central management and control point across workloads hosted on premises, in an AWS Cloud, and in AWS GovCloud (US) regions. Similarly, NSX Cloud also supports Azure Government.