VMWARE NSX CLOUD

Consistent Networking and Security for Applications Running Natively in Public Clouds

AT A GLANCE

VMware NSX® Cloud delivers consistent networking and security for applications running natively in the public cloud. NSX Cloud uses the same management plane and control plane as NSX Data Center, enabling a single networking and security solution from the private data center to the public cloud.

KEY BENEFITS

Common networking and security, across public clouds such as AWS and Azure, significantly improves scalability, control, and visibility—with lower OpEx

- Simple scalability across virtual networks, availability zones, regions, and public clouds.
- Precise control of security and networking services brings protection and standardization to applications.
- End-to-end visibility of networking and security ensures the health and compliance of applications in public clouds.

PRICING

- Subscription based pricing, available in 1-year and 3-year term licenses
- Based on vCPUs consumed by powered–on workloads within the public cloud, independent of the number of virtual networks (e.g. AWS VPCs, Azure VNets)
- NSX Data Center license not required for cloud-only use-cases

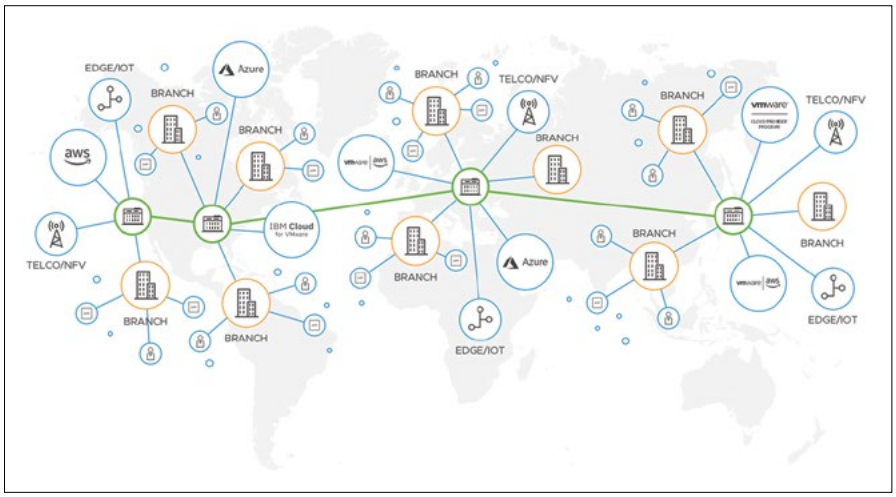

Figure 1: The Virtual Cloud Network

A Network Built for the Cloud Principles

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

Use Cases

Consistent Security Across Clouds

NSX Cloud enables policy across workloads running across multiple public clouds. NSX Cloud leverages the same control plane and data plane as NSX Data Center, enabling end-to-end policy management across data centers and clouds. 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.

Precise Control over Cloud Networking

VMware NSX Cloud is designed for native public cloud environments such as Amazon (AWS) and Microsoft Azure. 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 ELB/Azure Load Balancer, AWS Route53/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.

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

CALL

877-4-VMware (outside North America, +1-650-427-5000),

VISIT

www.vmware.com/products/nsx-cloud.html or http://www.vmware.com/products to search online for an authorized reseller.

End-to-end Operational Control and Visibility

VMware 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-premise 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-premise and in the public cloud.

Key Features

Multi-cloud, Multi-site Networking and Security: NSX Cloud brings networking and security capabilities to endpoints across multiple clouds, and by integrating with NSX Data Center, enables networking and security management across clouds and data center sites.

Micro-segmentation: Control over East-West traffic between application workloads running natively in public clouds.

Security Groups: Security groups and rules can be defined based on rich policy constructs, such as instance name, OS type, AMI ID, and user-defined tags.

Dynamic Policy: Security policy is automatically applied and enforced 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 that are running in the public cloud without micro segmentation security. Quarantined instances are prevented from communicating on the cloud network.

Distributed Architecture: NSX Cloud's distributed firewalling architecture eliminates additional network hops and traffic because policies are enforced at the virtual network interface of each instance, rather than routing through an external firewall.

Edge Firewalling: NSX Cloud provides stateful firewalling that filters North-South traffic flowing between instances in virtual networks and the public Internet.

RESTful API: RESTful API and automation tools to programmatically provision and configure networking and security infrastructure on-demand.

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: 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.

vmware®

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