VMware NSX Cloud and AWS

Hybrid cloud networking and security across private and public cloud native workloads

AT A GLANCE

VMware NSX® Cloud provides single-pane-of-glass visibility, rich networking capabilities, consistent security policy, and granular and operationally scalable micro-segmentation across on-premises and native public cloud environments such as AWS cloud.

KEY BENEFITS

- Define a security policy once and apply to workloads across private data centers and public clouds.
- Enable end-to-end operational control and visibility for monitoring, troubleshooting, and auditing across data centers and clouds.
- Get a complete inventory view across all accounts, regions, subscriptions, VPCs, and VNets, as well as the operational status of every VM, to enable quicker troubleshooting.

VMware and AWS have partnered to provide solutions that help customers adopt hybrid cloud to increase flexibility and reduce cost, while leveraging their existing IT investments and expertise. As global workloads rapidly increase, the need for greater agility drives customers to adopt public clouds. It's critical for enterprises to have the ability to centrally manage their public cloud environments and on-premises enterprise networks. VMware NSX Cloud enables a common and consistent way to secure and manage cloud native workloads across the public cloud as well as on-premises workloads from a single pane of glass.

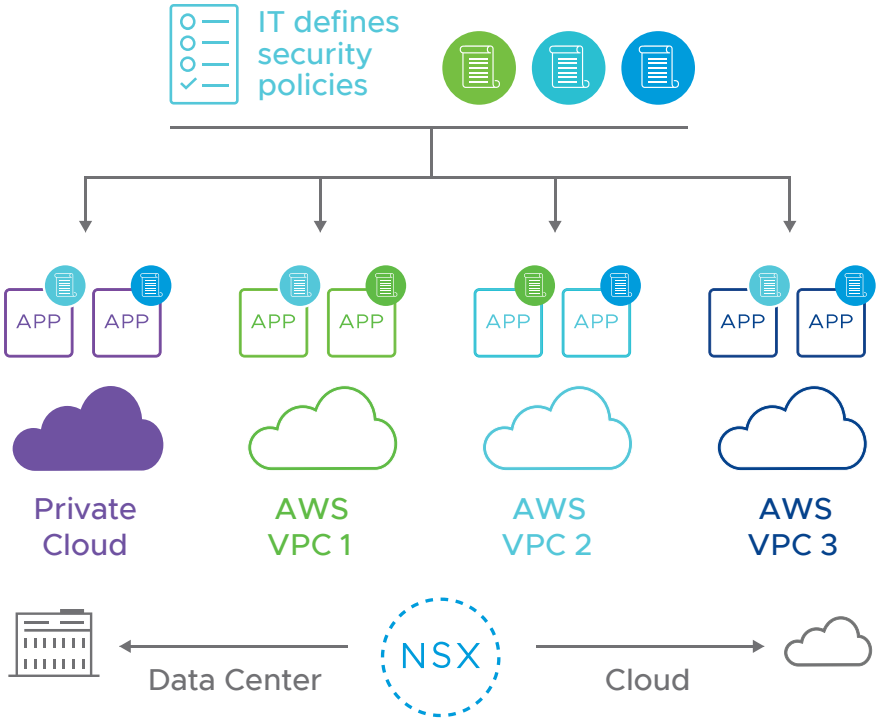


FIGURE 1: Hybrid cloud networking and security across private and public cloud native workloads

vmware® | aws

aws partner network
Advanced Technology Partner

"With NSX Cloud, we got a very compact firewall policy—easy to review and easy to manage. The power, administratively, is that we go to one place to update our policy and when we publish it, it automatically deploys it to every cloud server instance. This was a big win for a small team like ours."

BRIAN JEMES
NETWORK MANAGER
UNIVERSITY OF IDAHO

NSX CLOUD ON AWS SOLUTION SPACE

The AWS Solution Space showcases featured use cases by AWS and AWS Competency Partners for NSX Cloud on AWS. Learn more at *https://aws.amazon.com/solutionspace/solutions/vmware-nsx-hybrid-network-on-aws/*.

Key benefits

Consistent security policy across clouds

Define a security policy once and apply to workloads anywhere—across virtual private clouds (VPCs), regions, availability zones, and multiple private data centers.

Single-pane-of-glass visibility

NSX Cloud provides a complete inventory view across all accounts, regions, subscriptions, and VPCs, as well as the operational status of every virtual machine (VM), to enable quicker troubleshooting.

Operational control

NSX Cloud provides standard interfaces and APIs to plug in to your existing operations tools to enable deep, end-to-end visibility for monitoring, troubleshooting, and auditing across data centers and clouds.

Key features

Micro-segmentation and edge firewalling

NSX Cloud provides granular control over east-west traffic between application workloads running natively in public clouds and on-premises data centers. Stateful firewalling filters north-south traffic flowing between instances in virtual networks (VNets) and the public Internet.

Shared gateway in transit VPCs/VNets

Gateway consolidation in transit VPCs/VNets results in simpler administration and faster onboarding of compute for VPCs/VNets, as well as enables selective routing of traffic for service insertion via third-party appliances.

Traffic visibility with any SIEM tool

NSX Cloud supports standard protocols such as Syslog, IPFIX, and L3SPAN, as well as troubleshooting tools such as Traceflow. Use any existing Day 2 operations tools to gain real-time visibility into traffic flows and firewall logs within and across VPCs.

Site-to-site VPN

The built-in IPsec virtual private network (VPN) support encrypts traffic between on-premises and public clouds, as well as between public clouds, eliminating costs of VPN connectivity.

Service insertion

Service insertion allows for selective routing of north-south traffic to third-party next-generation firewall partner service appliances by programming the NSX Cloud gateway in the transit VPC/VNet. This can significantly reduce virtual L7 firewall charges that are billed based on traffic.

vmware® | aws

NSX Cloud on AWS—under the hood

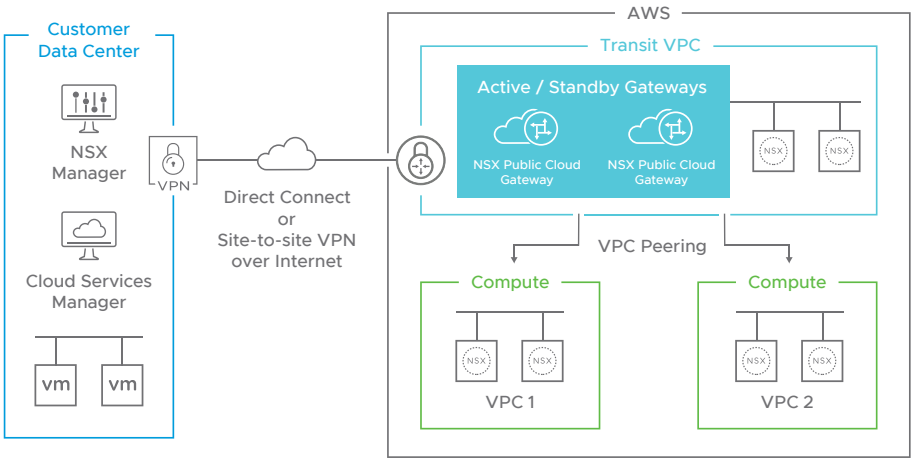


FIGURE 2: NSX Cloud architecture.

Core components

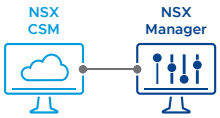
The core NSX Cloud components are:

- **NSX Manager™** for the management plane with policy-based routing, role-based access control (RBAC), control plane, and runtime states defined. This is a core NSX-T™ Data Center component in the customer data center.
- **Cloud Service Manager (CSM)** for integration with NSX Manager to provide public cloud-specific information to the management plane.
- **NSX Public Cloud Gateway (PCG)** for connectivity to the NSX management and control planes and NSX Edge™ gateway services, and for API-based communications with public cloud entities. The NSX Public Cloud Gateway can either be a standalone gateway appliance or shared across public cloud VPCs to achieve a hub-and-spoke topology.
- **NSX Agent** functionality, which provides a datapath managed by NSX for workload VMs.

How it works

1. Install the CSM appliance and connect with NSX Manager

   The CSM appliance is a core component of NSX Cloud and needs to be connected with NSX Manager to allow these components to communicate with each other.



2. Connect one or more AWS accounts in CSM

   There may be one or more AWS accounts with VPCs and workload VMs that need to be brought under NSX-T Data Center management.

NOTE THE DIFFERENCE

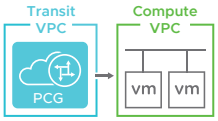
VMware Cloud™ on AWS is another hybrid cloud offering from VMware and addresses a different set of use cases and customer requirements. VMware Cloud on AWS brings VMware's enterprise-class software-defined data center (SDDC) software—VMware vSphere®, VMware vSAN™, and VMware NSX—to the AWS cloud with optimized access to AWS services. It is a service used by organizations looking to modernize, protect, and scale applications based on vSphere in AWS. Learn more at *https://cloud.vmware.com/vmc-aws*.

DID YOU KNOW?

NSX Cloud is based on NSX-T, the same platform that underpins the NSX Data Center product offering. NSX Cloud can be used in conjunction with NSX Data Center to offer end-to-end security, visibility, and networking across on-premises data center and native public cloud environments. Learn more at *https://www.vmware.com/products/nsx.html*.

3. Deploy the PCG in your transit VPC and link to compute VPCs

   The PCG provides north-south connectivity between the public cloud and the on-premises management components of NSX-T Data Center. The PCG deployed in a VPC can optionally be used to onboard VMs hosted in other VPCs or VNets.



4. Onboard workload VMs

   Onboard workload VMs to be managed by NSX by tagging in AWS and installing NSX Agents on them. After the workload VMs have been successfully onboarded, you can use NSX-T Data Center to manage them by assigning tags and applying distributed firewalling rules.

Ready to secure and centrally manage your public cloud workloads?

Check out these resources to learn more about NSX Cloud, and reach out to your VMware sales representative for further details.

NSX Cloud:
https://www.vmware.com/products/nsx-cloud.html

NSX Cloud blog:
https://blogs.vmware.com/networkvirtualization/tag/nsx-cloud/

NSX Cloud Hands-on Lab:
https://my.vmware.com/en/web/vmware/evalcenter?p=nsx-cloud-18-hol

NSX-T Data Center documentation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html