VMware NSX Cloud

跨私有云和公有云环境的混合云网络连接和安全性

概览

VMware NSX® Cloud 为公有云中原生运行的应用提供始终如一的网络和安全性。NSX Cloud 与 NSX Data Center 使用相同的管理平面和控制平面，因而支持从专有数据中心到公有云采用一致的网络和安全性解决方案。

主要优势

跨 AWS 和 Azure 等公有云提供通用网络和安全性，从而显著提高可扩展性、控制力和可见性，同时降低 OPEX：

- 使用 NSX 结构或原生公有云结构，可灵活部署
- 可跨虚拟网络、可用区、区域和公有云轻松扩展
- 精确控制安全性和网络连接服务，实现应用标准化并为其提供保护
- 端到端深入了解网络和安全性，确保公有云中的应用正常运行并且合规

定价

- 基于订阅的定价，提供一年期或三年期许可证
- 基于公有云中处于开启状态的工作负载所使用的 vCPU，与虚拟网络的数量无关；例如，AWS 虚拟私有云 (VPC) 和 Azure 虚拟网络 (VNet)
- 仅限云的应用场景无需 NSX Data Center 许可证

专为云计算原则构建的网络

VMware NSX Cloud 为公有云中原生运行的应用提供网络和安全性。与 VMware NSX 系列结合使用时，VMware NSX Cloud 支持虚拟云网络，能够以软件定义的方式实现可跨数据中心、云、端点以及物联网终端延展的网络。

图 1：虚拟云网络。

应用场景

跨多个云的一致安全性

NSX Cloud 可对跨多个公有云和本地部署数据中心运行的工作负载实施策略。只需定义一次策略，即可将其应用于任意位置的工作负载，包括跨云虚拟网络、区域、可用区和多个云服务提供商的工作负载。安全策略将根据应用属性和用户定义的标记以动态方式应用于每个工作负载。对于未应用适当的微分段安全策略的恶意工作负载或遭到入侵的工作负载，甚至可以实现自动隔离。NSX Cloud 支持南北向服务注入，允许选择性流量路由到第三方安全设备，以实现高级安全保护。

精确控制云网络

VMware NSX Cloud 专为 Amazon (AWS) 和 Microsoft Azure 等原生公有云环境而设计。NSX Cloud 是对这些公有云提供商提供的原生服务的补充。借助 NSX Cloud，您可以继续针对工作负载无限制地使用公有云提供商的基础架构和应用服务（例如 AWS ELB/Azure Load Balancer、AWS Route 53/Azure DNS、AWS Direct Connect/Azure ExpressRoute 和 Amazon RDS/Azure Database）。您还可以使用现有的自动化工具提出 REST API 请求，以自动执行调配和配置管理。NSX Cloud 还支持执行网关整合以便向 VPC/VNet 过渡，这样一来，不仅可以简化运维，还可以使用内置服务，如站点间 VPN 以及第三方边缘/传输服务。

端到端运维控制和可见性

VMware NSX Cloud 提供标准的接口和协议，支持从云计算网络访问网络和安全性数据。您可以通过 IPFIX、Traceflow、端口镜像和 Syslog 获取流、数据包和事件信息。这些数据可供现有的本地部署运维工具使用，实现端到端深入了解监控、故障排除和审核。这些丰富的运维数据有助于大幅缩短确定和解决整个混合云部署（包括本地部署应用和公有云中的应用）中的网络连接、性能和安全性问题所花的时间。NSX Cloud 使您可以精确了解跨所有 VPC/VNet 的公有云工作负载以及轻松选择要使用 NSX 管理的工作负载，并且提供了丰富的搜索和筛选功能，让您能够轻松进行管理。

主要功能特性

NSX 强制模式 – 使用 NSX 工具跨本地部署和原生公有云工作负载实施一致的安全性和网络策略。

原生云强制模式 – 使用公有云提供商的安全性和网络结构，跨本地部署和原生公有云工作负载实施一致的安全性和网络策略。

原生公有云服务端点的发现和保护 – 除了虚拟机 (VM) 和 EC2 实例之外，还可以发现和保护原生公有云服务端点。

多云、多站点网络和安全性 – 可跨多种云环境为端点提供网络和安全性功能，并通过与 NSX Data Center 集成，跨云环境和数据中心站点实现网络和安全性管理。

微分段 – 控制在公有云中原生运行的应用工作负载之间的东西向流量。NSX Cloud 还支持对 VMware Horizon® Cloud on Azure 部署的虚拟桌面进行微分段。

用于安全策略定义的丰富抽象功能 – 基于丰富的策略结构（例如实例名称、操作系统类型、AMI ID 和用户定义的标记）定义安全组和规则。

动态策略 – 根据实例属性和用户定义的标记自动应用和实施安全策略。当实例在云环境内或跨云环境移动时，策略会自动随之移动。

隔离实例 – 隔离在未实施微分段安全保护的公有云中运行的恶意和遭入侵的工作负载。阻止被隔离的实例在云网络上进行通信，从而提供多层安全性。

服务注入 – 有选择地使用基于策略的路由将南北向流量路由到第三方提供的新一代防火墙合作伙伴设备。

站点间 VPN – 利用内置 VPN 支持将流量回程传输到本地部署数据中心。

分布式体系架构 – 使用 NSX Cloud 分布式防火墙保护体系架构消除了额外的网络跃点和流量，该体系架构在每个实例的虚拟网络接口上实施策略，而不是通过外部防火墙进行路由。

向 VPC/VNet 过渡的共享网关 – 支持执行网关整合以便向 VPC/VNet 过渡，这将可以简化管理，加快对计算 VPC/VNet 的纳管速度，并且能够注入第三方服务。

边缘防火墙保护 – 使用有状态防火墙保护对在虚拟网络中的实例和公共 Internet 之间传输的南北向流量进行过滤。

RESTful API – 通过 RESTful API 和自动化工具按需以编程方式调配和配置网络和安全性基础架构。

要获取更多信息或购买 VMWARE 产品

请拨打 400-816-0688、访问 vmware.com/cn/products/nsx-cloud 或 vmware.com/cn/products，或者在线搜索授权代理商。

模板创建 – 使用现有的自动化和编排工具来创建标准化应用模板，并简化跨公有云调配和管理网络和安全性服务的流程。

东西向流量可见性 – 使用现有的后续运维工具来了解 VPC 内部和跨多个 VPC 的东西向流量。

安全性日志记录 – 实时了解和审核安全事件，例如，允许/拒绝和隔离突发事件。将安全事件信息发送到 Syslog 或 SIEM 服务器。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com 威睿信息技术（中国）有限公司
北京朝阳区新源南路 8 号启皓北京东塔 8 层 801 邮编：100027 电话：+86-10-5976-6300
中国上海办公室 上海市淮海中路 333 号瑞安大厦 805B-809 室 邮编：200021 电话：+86-21-8024-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真 852-3696 6101 www.vmware.com/cn