VMWARE NSX CLOUD

为公有云中原生运行的应用提供始终如一的网络连接和安全保护

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连接和安全保护。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连接和安全性解决方案。

主要优势

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

- 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连接和安全性，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 1 年期或 3 年期许可证
- 基于公有云中处于开启状态的工作负载使用的虚拟 CPU，与虚拟网络（如 AWS VPC、Azure VNet）的数量无关
- 仅限云的使用情形无需 NSX Data Center 许可证

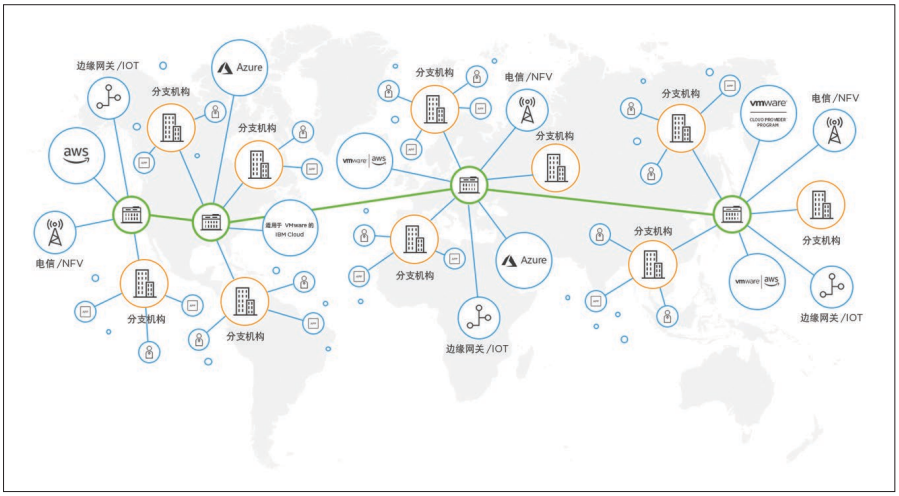

图 1：虚拟云网络

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连接和安全保护。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连接。

使用情形

一致的跨云安全保护

NSX Cloud 可在跨多个公有云运行的工作负载中实施策略。NSX Cloud 与 NSX Data Center 使用相同的控制平面和数据平面，因而支持跨数据中心和云环境实现端到端策略管理。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。

对云计算网络连接的精确控制

VMware NSX Cloud 专为 Amazon (AWS) 和 Microsoft Azure 等原生公有云环境设计。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 Route53/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。

要获取更多信息或购买 VMWARE 产品
请拨打
010-59934306

访问
https://www.vmware.com/cn/products/nsx-cloud.html 或 http://www.vmware.com/cn/products 在线搜索授权代理商。

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（包括本地和公有云中的应用）中的网络连接、性能和安全性问题的时间。

主要功能特性

多种云环境、多站点网络连接和安全性： NSX Cloud 可跨多种云环境为端点提供网络连接和安全保护，并通过与 NSX Data Center 集成，跨云环境和数据中心站点实现网络连接和安全性管理。

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。

安全组： 可根据丰富的策略结构（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： 系统会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，策略会自动随之迁移。

隔离实例： 隔离公有云（未实施微分段安全保护）中运行的恶意工作负载和遭到入侵的工作负载。隔离的实例将无法在云计算网络上进行通信。

分布式体系结构： NSX Cloud 的分布式防火墙体系结构可消除额外的网络跃点和流量，因为它会在每个实例的虚拟网络接口处实施策略，而不是通过外部防火墙进行路由。

边缘网关防火墙保护： NSX Cloud 提供有状态防火墙保护，可过滤虚拟网络和公共 Internet 中实例之间的南北向流量。

RESTful API： RESTful API 和自动化工具能够以编程方式按需调配和配置网络连接和安全基础架构。

创建模板： 使用现有的自动化和编排工具来创建标准化应用模板，并跨公有云简化网络连接和安全服务的调配和管理。

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 VPC 之间的东西向流量。

安全日志记录： 实时了解和审核安全事件，例如允许/拒绝和隔离事件。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 www.vmware.com
威睿信息技术（中国）有限公司
中国北京办公室 北京市朝阳区新源南路 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

项目号：149451wf-vmw-q2fy19-sddc-launch-ds-nsx-cld-a4 6/18