VMware NSX Data Center

主要优势

- 利用工作负载级微分段和精细安全机制保护应用。
- 通过自动化将网络调配时间从数天缩短至数秒并提高运维效率。
- 在数据中心和原生公有云内以及跨多个数据中心和原生公有云以独立于物理网络拓扑的方式实现对网络和安全性策略的一致管理。
- 获得详细的应用拓扑可视化、自动化的安全策略建议以及持续的流监控。

VMware NSX® Data Center 是一个支持虚拟云网络的网络虚拟化和安全性平台，能够以软件定义的方式实现可跨数据中心、云环境和应用框架进行延展的网络。借助 NSX Data Center，可以使网络和安全性更贴近应用，而无论应用在何处（包括虚拟机 [VM]、容器和裸机）运行。与虚拟机的运维模式类似，可独立于底层硬件对网络进行调配和管理。NSX Data Center 通过软件方式重现整个网络模型，从而实现在几秒钟内创建和调配从简单网络到复杂多层网络的任何网络拓扑。用户可以创建多个具有不同要求的虚拟网络，利用由 NSX 或范围广泛的第三方集成（从新一代防火墙到高性能管理解决方案）生态系统提供的服务组合构建本质上更敏捷、更安全的环境。然后，可以将这些服务延展至同一云环境内部或跨多个云环境的各种端点。

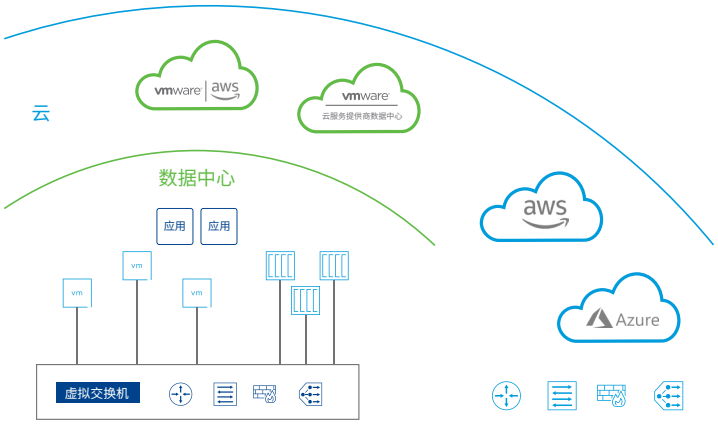

图 1：NSX DATA CENTER 网络虚拟化和安全性平台。

软件形式的网络

VMware NSX Data Center 提供了一种通过软件定义的全新网络运维模式，构成了软件定义数据中心 (SDDC) 的基础并延展到了虚拟云网络。数据中心操作员现在可获得的敏捷性、安全性和经济性，在以前数据中心网络仅与物理硬件组件紧密关联时，是无法实现的。NSX Data Center 提供了一组完整的逻辑网络和安全性功能及服务，其中包括逻辑交换、路由、防火墙保护、负载均衡、虚拟专用网络 (VPN)、服务质量 (QoS) 和监控。可以通过利用 NSX Data Center API 的任何云计算管理平台在虚拟网络中对这些服务进行调配。虚拟网络可以无中断地部署到任何现有网络硬件上，并且可以跨数据中心、公有云和私有云、容器平台和裸机服务器进行延展。

主要功能特性

交换	支持逻辑第 2 层叠加网络在数据中心内部以及跨数据中心边界在路由（第 3 层）结构中进行延展。支持基于 VXLAN 和 GENEVE 的网络叠加。
路由	在 hypervisor 内核中，采用分布式方式在虚拟网络之间执行动态路由；借助物理路由器的双活故障转移功能横向扩展路由。支持静态路由和动态路由协议（包括 IPv6）。
网关防火墙	最高可运用到第 7 层的有状态防火墙保护（包括应用识别和 URL 白名单），嵌入在 NSX 网关中，跨整个环境而分布并且采用集中式策略和管理。
分布式防火墙	最高可运用到第 7 层的有状态防火墙保护（包括应用识别和 URL 白名单），嵌入在 hypervisor 内核中，跨整个环境而分布并且采用集中式策略和管理。此外，NSX 分布式防火墙直接集成到云原生平台（如 Kubernetes 和 Pivotal Cloud Foundry）、原生公有云（如 AWS 和 Azure）以及裸机服务器中。
负载均衡	L4–L7 负载均衡器，具备 SSL 负载分流和直通、服务器运行状况检查功能（和被动运行状况检查），以及关于可编程性及通过 GUI 或 API 控制流量的应用规则。
VPN	站点间和远程访问 VPN 功能，通过非代管 VPN 提供云计算网关服务。
NSX 网关	支持将在物理网络和 NSX 叠加网络上配置的 VLAN 桥接起来，以便在虚拟工作负载和物理工作负载之间建立无缝连接。
NSX Intelligence™	NSX Intelligence 提供自动化安全策略建议，以及针对每个网络流量的持续监控和可视化功能，以便提高可见性，实现极易审核的安全状况。作为与 NSX-T™ Data Center 相同的 UI 的一部分，NSX Intelligence 为网络团队和安全性团队均提供了单一窗口。
NSX Data Center API	基于 JSON 的 RESTful API，用于实现与云计算管理平台、DevOps 自动化工具和自定义自动化功能的集成。
运维	中央 CLI、跟踪流、叠加逻辑 SPAN 和 IPFIX 等原生运维功能，可以主动监控虚拟网络基础架构并进行故障排除。与 VMware vRealize® Network Insight™ 等工具集成，可执行高级分析和故障排除。
环境感知微分段	可以基于属性（不只是 IP 地址、端口和协议）动态创建并自动更新安全组和策略，将虚拟机名称和标记、操作系统类型以及第 7 层应用信息等元素包括在内，以启用自适应微分段策略。以来自 Active Directory 和其他来源的身份信息为基础的策略可在远程桌面服务和虚拟桌面基础架构 (VDI) 环境中实现下至单个用户会话级别的用户级安全性。
自动化和云计算管理	与 vRealize Automation™/VMware Cloud™ Automation Services、OpenStack 等原生集成。完全受支持的 Ansible 模块、完全受支持的 Terraform 提供商和 PowerShell 集成。
第三方合作伙伴集成	支持在大量不同领域（例如，新一代防火墙、入侵检测系统 (IDS)/入侵防御系统 (IPS)、无代理防病毒、交换、运维和可见性、高级安全性等）与第三方合作伙伴进行管理平面、控制平面和数据平面的集成。
多云网络和安全性	无论底层物理拓扑或云计算平台是怎样的，均可跨数据中心站点以及私有云和公有云边界实现一致的网络和安全性。
容器网络和安全性	支持在以 Kubernetes 和 Cloud Foundry 为基础而构建并在虚拟机或裸机主机上运行的平台上对容器执行负载均衡、微分段（分布式防火墙保护）、路由和交换。提供对容器网络流量（逻辑端口、SPAN/Mi、IPFIX 和跟踪流）的可见性。

应用场景

安全性

NSX Data Center 可帮助在私有云和公有云环境中高效实现对应用的零信任安全保护。无论目标是锁定关键应用、以软件方式创建逻辑隔离区 (DMZ)，还是减小虚拟桌面环境的受攻击面，NSX Data Center 都可以通过微分段在单个工作负载级别定义和强制实施网络安全策略。

多云环境网络

NSX Data Center 提供了网络虚拟化解决方案，能够跨异构站点以一致的方式实现网络和安全性，从而精简多云环境的运维。因此，NSX Data Center 可实现多种多云应用场景，从无缝数据中心延展到多数据中心池化，再到工作负载快速移动。

自动化

通过将网络和安全性服务虚拟化，NSX Data Center 可以消除手动管理的网络连接和安全性服务及策略的瓶颈，从而可以更快速地调配和部署全体系应用。NSX Data Center 与云计算管理平台和其他自动化工具（例如 vRealize Automation/VMware Cloud Automation Services、OpenStack、Terraform、Ansible 等）原生集成，使开发人员和 IT 团队能够按照业务要求的速度调配、部署和管理应用。

云原生应用的网络和安全性

NSX Data Center 为容器化应用和微服务提供集成式全体系网络和安全性，从而在开发新应用时针对每个容器提供精细策略。这可为微服务实现原生的容器间 L3 网络和微分段功能，并跨新旧应用提供网络连接和安全性策略的端到端可见性。

VMware NSX Data Center 的版本

Standard

适用于需要敏捷的自动化网络连接功能的企业。

Professional

适用于需要 Standard 版本功能及微分段功能，并且可能具有公有云端点的企业。

Advanced

适用于需要 Professional 版本功能及高级网络连接和安全性服务，并与范围广泛的生态系统集成且可能拥有多个站点的企业。

Enterprise Plus

适用于具有以下需求的企业：NSX Data Center 提供的最先进的功能、使用 vRealize Network Insight 执行网络运维、使用 VMware HCX® 实现混合云移动性，以及使用 NSX Intelligence 实现流量可见性和安全运维。

Remote Office Branch Office (ROBO)

适用于需要为远程办公室或分支机构中的应用将网络和安全性虚拟化的企业。

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX DATA CENTER[1]					
分布式交换和路由	•	•	•	•	•[5]
NSX 网关防火墙（有状态）	•	•	•	•	•
NSX 网关 NAT	•	•	•	•	•
软件 L2 桥接到物理环境	•	•	•	•	
通过 ECMP 进行动态路由（双活）	•	•	•	•	•
与 Cloud Management Platform 集成[3]	•	•	•	•	•
针对裸机上运行的虚拟机和工作负载的分布式防火墙保护		•	•	•	•
VPN（L2 和 L3）		•	•	•	•
与 NSX Cloud[4] 集成以便为 AWS 和 Azure 提供支持		•	•	•	•
负载均衡			•	•	•
与分布式防火墙（Active Directory、VMware AirWatch®、Endpoint Protection 和第三方服务注入）集成			•	•	•
容器网络和安全性			•	•	
多站点网络和安全性			•	•	
IPv6			•	•	
环境感知微分段（应用识别、RDSH、协议分析器）				•	
高级 NSX 网关防火墙（应用识别、协议分析器）				•	
URL 筛选				•	
+NSX INTELLIGENCE					
虚拟机之间流量分析				•	
防火墙可见性				•	
自动安全策略				•	
规则和组建议分析				•	
+vREALIZE NETWORK INSIGHT ADVANCED[2]					
流量 (IPFIX) 可见性和网络监控				•	
防火墙规划和管理				•	
NSX 运维和故障排除				•	
+VMWARE HCX ADVANCED[2]					
大规模工作负载迁移				•	
优化 WAN 以便迁移工作负载				•	
跨多个链路的流量和负载管理				•	

1.如需了解详细的功能特性，请参阅关于 NSX Data Center for vSphere® 功能特性和 NSX-T Data Center 功能特性的知识库文章，获取最新信息。
2.NSX Data Center Enterprise Plus 包括所有版本的 vRealize Network Insight Advanced 和 VMware HCX Advanced。
3.仅限 L2、L3 和 NSX 网关集成。不使用安全组。
4.对于公有云工作负载，需要订购 NSX Cloud。
5.仅限交换，支持 VLAN。

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