通过 VMware NSX 实现网络虚拟化和安全性

改变传统网络连接的现状，并释放软件定义的数据中心的全部价值。

业务案例白皮书

vmware®

目录

内容提要 4
软件定义的数据中心的高价值 IT 成效 4
现状概述 4
关键趋势：IT 越来越像云服务提供商 4
软件定义的数据中心 (SDDC) 5
混合云计算 5
网络虚拟化 6
开放网络连接 6
IT 面临的挑战：用更少的资源获得更高的速度、敏捷性和安全性 6
高级持续性威胁 6
硬件局限性和束缚 7
容易出错的手动配置 7
VMware 解决方案 8
NSX：SDDC 的网络虚拟化与安全性 8
开创性使用情形 8
微分段 8
灾难恢复 9
自助研发云计算 9
云应用移动性和数据中心迁移 9
IT 自动化和编排 10
基础架构优化和更新 10
业务价值 11
功能性优势：速度、敏捷性、安全性和可靠性 11
最大限度降低数据泄漏的风险和影响 11
加快 IT 服务交付和上市速度 11
简化网络流量 11
提高服务可用性 11
提高协商和购买能力 11
更高效地使用网络工程师 12

经济优势：节省大量 CAPEX 和 OPEX 12
高效微分段带来 CAPEX 节省 12
IT 自动化降低了 OPEX 13
高效利用服务器资产节省 CAPEX 14
高性价比带来 CAPEX 节省 15
硬件生命周期延长节省 CAPEX 16
总结 17
变革性优势和无中断部署 17
开始体验 17
参考资源 17

内容提要

软件定义的数据中心的高价值 IT 成效

此 VMware 业务案例面向业务和 IT 高管、IT 运维、IT 基础架构和 IT 安全专家。您将了解领先的企业如何从面向其软件定义的数据中心 (SDDC) 的网络虚拟化和安全解决方案中获得前所未有的价值。

领先的企业知道 SDDC 对于现代 IT 至关重要。他们借助 SDDC 推动创新、加快业务发展速度、打造竞争优势和降低总 IT 成本。他们已转向借助 VMware 来寻求其 SDDC 平台和方法的重要支柱。这些企业在为其 SDDC 提供支持的统一平台中使用 VMware NSX™ 网络虚拟化和安全解决方案，以及 VMware 存储和服务器虚拟化技术。

借助 NSX，企业将获得前所未有的速度、敏捷性和安全性，将经济性、灵活性和选择的自由度提高若干数量级。下面是使用 NSX 的企业实现的一些主要使用情形和 IT 成效：

- 微分段 - 借助防火墙控制和保护数据中心内的东西向流量。最大限度降低数据泄漏的风险和影响。可节约大约 68% 的 CAPEX。
- IT 自动化和编排 - 减少网络调配和管理的手动任务和周期时间。缩短新应用的 IT 服务交付和上市时间。节约 56-86% 的 OPEX。
- IT 优化和更新 – 现代分支 / 主干网络结构、裸机交换机、开放网络连接以及其他数据中心优化的催化剂。节约 66-88% 的 CAPEX。
- 灾难恢复 - 云级服务可用性。降低计划外停机的风险和影响。每次事故节约的 OPEX 从 690,000 到数千万美元不等。

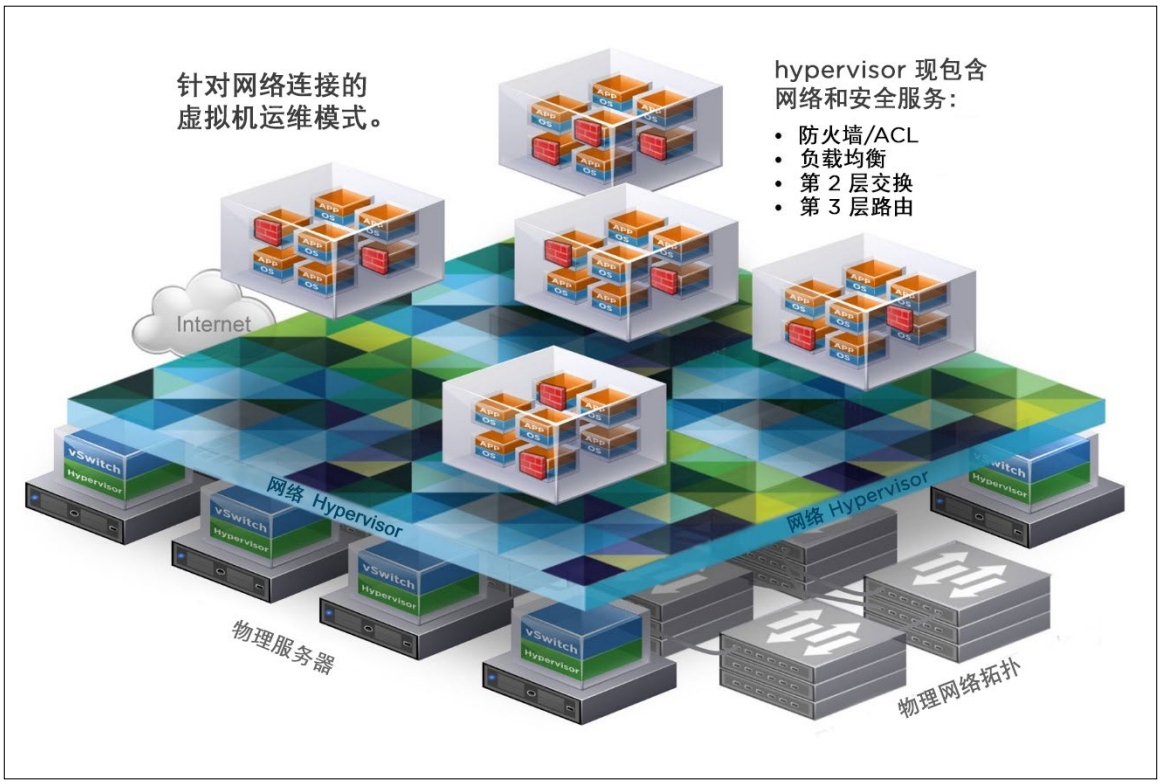
现状概述

关键趋势：IT 越来越像云服务提供商

企业希望 IT 的速度、敏捷性和安全性能与 Amazon、Facebook 和 Google 等大型云服务提供商一样。虽然大多数企业级数据中心的大小和规模与这些网络巨头相差甚远，但它们仍需要实现类似的速度、敏捷性和经济效益。Amazon、Facebook 和 Google 通过在其基础架构中融入抽象层设计实现了这些优势。这些网络元素和服务与硬件分离，并集成到其软件应用中。

从历史角度看，抽象化一直都是计算机科学和软件工程领域的基础支持要素之一。每次我们添加一个重要的抽象层时，我们都会推动其上方和下方抽象层的创新。例如，考虑操作系统、编程语言、API 和服务器虚拟化如何革新信息技术。

借助服务器虚拟化，服务器 hypervisor（一个抽象层）会在软件中重现 x86 物理服务器的属性（如 CPU、RAM、磁盘、NIC）。将网络虚拟化视为与网络 hypervisor 对等的功能。NSX 可在软件中重现第 2 至 7 层的网络连接服务（如交换、路由、防火墙、负载均衡、VPN、访问控制和 QoS）。企业使用 NSX 可在短短几秒内调配唯一、隔离的虚拟网络，就像调配虚拟机一样。



软件定义的数据中心

在 SDDC 体系结构中，所有基础架构（包括计算、存储和网络连接）都是按需虚拟化、池化和交付的。数据中心的运维和控制已实现高度自动化和标准化。业务线 (LOB)、应用和 Web 团队通过自助服务即时部署基础架构。

根据最近的一项调查，SDDC 每年可节省 56% 的调配和管理运维开销。[1] 调配新应用的生产网络所需的天数（包括任务完成时间和周期）从 3-4 周缩短至几分钟。SDDC 还通过更好的生态系统功能、重要创新和缩短上市时间为企业提供价值。

混合云计算

企业日益采用混合云来以更低的成本加快 IT 服务交付速度。根据最近的一项调查显示，82% 的企业制定了混合云战略。[2] 混合云涵盖 On Premise（本地部署）私有云和 Off Premise（远程部署）公有云或私有云。企业将混合云用于数据存储、自动扩展和云爆发、高可用性和灾难恢复、数据驻留法合规性、开发和测试以及其他使用情形。

传统数据中心受到供应商特定的硬件和物理拓扑的限制。一直以来，这些限制让 IT 很难实施混合云。现在，企业可以使用 NSX 桥接和构建混合云，而不管基础硬件如何。借助 NSX，他们无需担心网络互操作性或服务提供商束缚。最终的混合云可提供无与伦比的业务敏捷性，显著简化运维并降低成本。

网络虚拟化

我们最近经历的一场结构性转型彻底改变了网络连接方式。企业将在速度、敏捷性和安全性方面实现突飞猛进。将经济性、灵活性和选择的自由度提高若干数量级。和虚拟机一样，可以编程方式创建、移动、复制、删除和还原虚拟网络，而无需重新配置底层物理硬件或拓扑。

NSX 可在虚拟化层中创建一个完整的网络架构。虚拟网络可以包含第 2 层交换、第 3 层路由、负载均衡、防火墙、VPN、ACL、QoS 等。正如 x86 服务器成为计算容量池一样，物理网络也已成为可根据需要使用和改变用途的运输容量池。

开放网络连接

IT 组织将利用开放网络连接的强大性价比优势。网络硬件和软件的分离推动了这种转变。企业将用商用裸机交换机和开源 Linux 网络操作系统取代昂贵的专有设备。将网络服务抽象到虚拟化层中也推动了裸机交换机的采用。

除了引入注目的 CAPEX 节约之外，企业还使用开放网络连接实现了 OPEX 节约。借助开放操作系统提供的访问功能、工具和社区服务，企业可以更加经济高效地自动运行、配置和监控网络，向其中添加新功能或排查其故障。

IT 面临的挑战：用更少的资源获得更高的速度、敏捷性和安全性

IT 正面临两难境地：企业总希望投入少，收益多。一方面，IT 需要适应不断变化的市场需求和技术使用模式，提高生产力、业务发展速度以及服务质量。另一方面，还需要整合并降低成本。就像使用服务器虚拟化一样，IT 组织正使用网络虚拟化成功化解这两种压力。

像 Google、Facebook 和 Amazon 这样的云服务提供商已证实应用和服务可以按需调配，并且会对业务产生立竿见影的影响。高级领导层坚信其 IT 能够取得和这些大型云服务提供商类似的运维成效和性能。他们需要同级别的速度和敏捷性来满足业务需求。

如果 IT 组织无法像云服务提供商那样思考和行动，它们将失去业务主管的信任。所以，企业有时会绕过 IT 组织以获得其所需的基础架构、应用和服务，而这会导致不必要的需求分散，从而降低企业其他 IT 服务的总体价值。

高级持续性威胁

尽管最近 Target、Anthem、Home Depot、Sony 以及其他企业遭受的攻击各不相同，但它们存在一个共性。一旦进入数据中心边界，攻击者就能够在服务器之间横向扩展威胁，从而收集并向外部泄漏敏感数据。这些案例凸显出现代数据中心的一个重大漏洞。它们的安全控制措施有限，无法遏制高级持续性威胁 (APT) 从边界内部蔓延。

边界防火墙在阻止 APT 方面至关重要且富有成效。但最近的攻击表明，威胁仍可以通过合法接入点进入数据中心。一旦进入，它们就会在服务器中蔓延，并增加它们造成危害的几率。从运维层面解决此问题是不可行的。所需的物理防火墙数量庞大，并需要使用一系列复杂的规则，因此不仅负担极大，成本也极为高昂。

根据最近的一项调查，2013 年确认有 63,437 例安全事件，其中 1,367 例确认是由敏感数据泄漏引起的。[3] 数据泄漏事件给美国公司造成的平均总损失达 585 万美元。[4] 全球最低平均损失为 137 万美元，是在印度。所有其他国家 / 地区的损失介于此范围内。

从广泛报道的数据泄漏事件中，我们了解到实际损失可能是个天文数字。举例来说，Sony Pictures Entertainment 在近几年发生了两次数据泄漏事件。据报道，一次发生在 2011 年 6 月，另一次发生在 2014 年 11 月。[5] 2011 年的数据泄漏给 Sony Pictures 造成了 1.71 亿美元的损失。根据我们对 2014 年数据泄漏事件的了解，分析师认为损失可能达到 1 亿美元。[6] Sony Pictures 在 2014 年遭受的攻击导致其整个网络停运数天，不仅如此，还引发了成本极其高昂的灾难恢复事件。调查表明，出现涉及至少 10,000 条记录的重大数据泄漏的可能性约为 22%。鉴于损失可能会超过 1 亿美元，确实应该规避此风险。

硬件局限性和束缚

传统网络基础架构限制了 IT 适应不断发展变化的数字世界的能力，也阻碍了其创新步伐。工作负载（甚至是虚拟机中虚拟化的工作负载）受限于物理硬件和拓扑，从而限制了它们的移动性。封闭式黑盒网络连接方法（使用自定义操作系统、ASIC、CLI 和管理）使企业进一步受限于现有的硬件。

传统的网络硬件显著减慢了调配流程，并且限制了工作负载的安置和移动性。一项研究发现，90% 的企业表示因为其网络的复杂性而无法充分发挥优势，影响可以部署应用和服务的时机、场所，以及可部署的应用和服务种类。平均而言，IT 在 12 个月内会对企业网络进行 10 次变更，而这些变更都需要花时间维护。维护时段的平均等待时间是每个时段 27 天。所以，企业一年之中总共需要花费 270 天（9.6 个月）的时间来等待 IT 部门提供新服务或改进的服务。大型企业需要进行更多此类变更，因此等待维护的时段更长。在接受调查的公司中，有 45% 报告员工的工作效率受到不利影响，有 42% 报告业务分析受到不利影响。[7]

容易出错的手动配置

物理网络迫使网络管理员每天执行大量重复的手动任务。例如，如果业务线或部门请求新应用或服务，管理员需要创建 VLAN、跨交换机和上行链路映射 VLAN、创建端口组、更新服务配置文件以及执行许多其他任务。并且需要通过笨拙的 CLI 在此基础上完成相关配置。

手动配置网络基础架构容易出错。实际上，人为错误是造成停机的主要原因。研究一致发现，占百分比最大的网络事件（介于 20%[8] 到 32%[9] 之间）是由人为 / 配置错误造成的。即使是一个错误也会导致出现关键连接问题或停机，从而对业务造成影响。计划外数据中心停机在财务上造成的影响巨大。所报道事件的平均持续时间为 86 分钟，每分钟的损失是 7,900 美元。每个事件的总平均成本约为 690,200 美元。[10]

就影响范围而言，82% 的公司遇到的网络停机是由进行错误配置的 IT 人员造成的。其中，94% 的受访者报告业务遭受了一些损失。80% 报告出现收入损失，49% 报告出现员工生产力损失。[11]

VMware 解决方案

NSX：SDDC 的网络虚拟化与安全性

领先的企业将 VMware NSX 作为其 SDDC 的重要支柱。这些组织将 NSX 视为一个可解决大量 IT 问题并帮助实施业务计划的战略平台。

NSX 可交付适用于网络的虚拟机运维模式。与服务器虚拟机类似，可在软件中独立于底层硬件和拓扑，以编程方式对网络服务进行调配和管理。NSX 让企业摆脱了传统网络基础架构的束缚。

NSX 可在数秒内创建和调配具有一致的配置和安全性的复杂多层网络。所有网络连接要素和服务（逻辑交换机、路由器、防火墙、负载均衡器、VPN 和工作负载安全性）都位于 hypervisor 内。

虚拟网络将底层物理网络用作简单的 IP 转发底板。可考虑使用带有底板和插槽的传统网络机箱。线路卡直接连接到底板。没有人对机箱背板进行配置更改；它只是在线路卡之间转发数据包。在虚拟化网络中，hypervisor 就好比线路卡，物理网络好比底板。

开创性使用情形

企业使用 NSX 提供大量新使用情形和高价值 IT 成效，这是传统网络基础架构不可能实现的。IT 执行现有操作的速度要快得多，成本也更低。企业通常可以通过一种使用情形来证明 NSX 成本的合理性。同时，他们可以建立一个战略平台，该平台能自动化 IT 运维并支持他们逐渐利用其他一些使用情形。下面讨论了 VMware 客户当前在生产部署中最常见的使用情形。

微分段

当今 NSX 平台的主要用途是微分段，该功能可以大幅提高数据中心边界内部的网络安全性。如果威胁进入网络内部，NSX 将对其进行遏制并阻止它横向移动到其他服务器，从而可以大幅减小企业受攻击的范围和面临的风险。客户可使用微分段来解决传统防火墙在运维层面无法解决的重大问题，并且报告的成本为原来的三分之一。

利用微分段可以在虚拟化网络中了解和控制工作负载。每个工作负载都获得了安全保护。在每个虚拟机的 vNIC 级别实施防火墙规则。事实上，这会为每个工作负载创建一个单独的“微信任分区”。

NSX 会根据虚拟化相关上下文（而不仅仅是物理拓扑）自动分配相应的安全组和策略。NSX 还可以根据不断变化的环境（包括第三方提供的环境）动态更改安全组和策略，例如恶意软件或漏洞评估解决方案。

NSX 提供了分组 VM 和应用安全策略的新方法。例如，它可以根据应用类型、网络结构和 // 或基础架构拓扑保护工作负载。安全策略不再局限于单个分布式虚拟交换机或端口组。

NSX 对安全策略进行集中编排，这不仅可以减缓规则剧增的情况，还能确保准确、一致地实施安全策略。而且，当您调配、移动或删除虚拟机时，它的防火墙规则也会随之被添加、移动或删除。这些更改是自动进行的，无需人为干预。此全新级别的自动化可以大幅降低跨工作负载管理安全策略的操作复杂性和费用支出。

借助 NSX，将通过内核虚拟机管理程序提供微分段。每个虚拟机管理程序提供 20 Gbps 的防火墙吞吐量。防火墙的分布式特征可提供快速的横向扩展体系结构。向数据中心添加额外主机后，防火墙容量会自动增加。

通过与 Palo Alto Networks、Intel Security、Trend Micro 和数十家其他 VMware NSX 合作伙伴实现 API 级集成，可提供威胁防御和恶意软件防护等高级安全功能。

灾难恢复

企业可使用 NSX 作为其现有灾难恢复 (DR) 解决方案的补充。NSX 将帮助他们将其恢复时间目标 (RTO) 减少 80% 以上，并最大限度减少停机和业务成本。

企业可使用 NSX 复制整个网络及其安全环境。他们可以定期为网络结构及其应用和服务拍摄快照，并在恢复站点对其进行维护。IT 无需更改 IP 地址，因为虚拟网络结构与底层硬件和拓扑是分离的。灾难恢复站点与主站点相同，不必对功能或性能进行权衡取舍。处于备用模式中的恢复站点中部署有副本，发生灾难时可一键激活。对源网络所做的所有更改都会自动复制到恢复站点上的副本。

自助研发云计算

企业可使用 NSX 作为其首选平台，以交付自助研发云计算计划及其他“基础架构即服务”(IaaS) 计划。借助 NSX，调配网络基础架构不再是影响业务发展速度和上市时间的瓶颈。

NSX 可调配位于同一物理基础架构上的开发、测试和生产前测试环境的成千上万个隔离网络。NSX 消除了与采购、安装和配置传统网络基础架构相关的手动任务，并且不再需要花费周期时间。网络将与其工作负载同步部署，这是经过全面审核的自助服务事务。应用将快速通过开发、测试、生产前调试和生产阶段，无需更改其 IP 地址。

云应用移动性和数据中心迁移

NSX 使应用和服务能够摆脱物理网络基础架构的束缚，使网络能够像虚拟机一样可移动。使用 NSX，将在与虚拟机相连的同一软件交换机中虚拟化网络。如果移动了某个工作负载（例如，VMware vSphere® vMotion®），则该工作负载的网络和安全服务会自动随之移动。

企业可使用 NSX 在主机或数据中心之间无缝迁移应用。实际使用情形包括移动应用以利用其他位置的容量，遵守数据驻留法律，迁移到新数据中心，或执行物理基础架构的维护 / 更新。

过去，物理网络拓扑和地址空间要求 IT 在移动应用时更改 IP 地址。有时，IP 地址被硬编码到应用中，由于需要更改代码和进行回归测试，成本变得更加高昂。借助 NSX，企业可以随意快速移动应用而不用重新为其分配 IP。这些便利可大幅降低运维成本，并提高 IT 敏捷性和响应能力。

IT 自动化和编排

NSX 可提供适用于网络的虚拟机运维模式。IT 使用 NSX 将网络服务调配时间从数周缩短为数秒。这消除了与采购、安装和配置传统网络硬件相关的手动任务，并且不再需要花费周期时间。

NSX 功能强大的编排功能可以编程方式将网络服务与虚拟机同步分发。企业可使用 NSX 标准化和维护包含网络拓扑及服务的预定义模板。例如，网络工程师可为多层应用创建用于开发的模板。通过自助服务，只需数秒即可将环境调配给应用开发者。可跨多种应用和服务针对采用一致的配置和安全策略的 QA、生产前测试和生产环境完成相同的操作。NSX 的自动化功能可减少运维开支，加快上市速度和 IT 服务交付速度。

NSX 还可整合所有虚拟和物理网络连接的配置状态及测量数据，从而简化运维。管理员可以从运维角度全面了解整个网络基础架构中发生的情况。这可简化流量管理、监控、故障排除和修复。

基础架构优化和更新

企业可使用 NSX 桥接和简化数据中心，而无需中断运行。NSX 使用传统的多层树形体系结构和更扁平的新一代结构化架构。从而构建了一个采用相同逻辑网络连接、安全和管理模式的公共平台。企业可以将 NSX 用于各种优化和整合场景。例如，在完成并购之后集成信息系统，跨多租户云环境中的各个租户最大限度实现硬件共享，以及访问未用计算容量孤岛。

如果由现有的网络供应商决定，企业将继续每隔几年淘汰和更换一次他们的设备，改用更加昂贵的硬件。幸好，这不再是您的唯一选择。NSX 会提供更有吸引力的经济优势和选择性。企业现在可以灵活地选择他们如何及何时更新自己的网络基础架构。借助 NSX，只需您现有的物理网络基础架构即可部署 SDDC。

业务价值

功能性优势：速度、敏捷性、安全性和可靠性

最大限度降低数据泄漏的风险和影响

领先的企业可使用 NSX 支持的微分段功能显著减少泄漏事件的攻击范围和成本。他们可以使用微分段将每个工作负载与自己的安全策略相隔离，从而遏制威胁并阻止横向移动。借助微分段，威胁将无法潜入其他应用并将数据泄漏到外部。

微分段可帮助规避或最大限度降低数据泄漏成本，相关开销包括与司法专家接洽、内部调查、改组导致的客户流失、客户赢得率降低、提供免费的信用或身份监控订阅、客户通信和外包热线支持以及许多其他成本。如前所述，每一次数据泄漏事件造成的损失从几百万美元到上亿美元不等。

加快 IT 服务交付和上市速度

正如 VMware 服务器虚拟化转变计算的运维模式一样，VMware NSX 也改变了网络连接方式。企业可使用 NSX 调配网络连接，并实现与用于计算的虚拟机相同的敏捷性、速度和控制能力。

借助 VMware 产品，企业可在数秒内调配云环境原生或传统应用，以及全套计算、存储和网络服务。借助 NSX，应用团队可完全实现自助服务调配。他们无需再等待数天或数周来购买硬件和设置网络。而且，NSX 的自动化和编排功能消除了手动配置错误的风险。

NSX 大大缩短了工程设计团队将新的创收应用和服务投向市场所需的时间。这一全新级别的速度和敏捷性加快了创新，提升了竞争优势。

简化网络流量

数据中心内的现代应用所产生的服务器间流量在持续增长。借助 NSX，客户可减轻过度使用的核心中的东西向流量负载。借助虚拟网络，虚拟机可通过虚拟交换机或聚合结构实现相互通信。这将大大减少东西向流量跃点，避免复杂的流量模式造成的“发夹式”和核心链路过度使用。
借助 NSX，企业省去了使用更多硬件增加核心容量的开支。

提高服务可用性

云级数据中心很少停机。这并不是因为它们可以实现昂贵、冗余的高可用性。而是因为它们采用更扁平的结构，这种结构支持在网络上的所有点（而不是分层硬件集群集合）之间进行等价多路径 (ECMP) 路由。简化的“分支 - 主干”型结构使得单个链路或设备变得微不足道。网络可以在无需停机的情况下承受多次同时发生的设备故障。

企业可在这些结构化架构的基础上使用 NSX，并获得与云级服务提供商（如 Facebook、Google 和 Amazon）相同的高可用性。

提高协商和购买能力

许多 NSX 企业客户一直在使用他们现有的网络硬件。但在更新之后，他们现在提高了协商和购买能力。部署 NSX 之后，可以在虚拟化层内提供更高价值的网络功能和特性。物理基础架构已逐渐商品化。企业在借助现有供应商更新其网络硬件时，可利用这种市场动态压低价格。

更高效地使用网络工程师

就像虚拟化转变和简化了服务器管理员的工作一样，它现在也正在转变和简化网络工程师的工作。网络工程师很看重 NSX，因为他们可以将更多时间集中在能给企业带来利润的战略计划上。已部署 NSX 的团队现在将他们的更多时间花在网络设计级注意事项上。网络管理员可以设计新一代网络结构并实施软件定义的数据中心，而不用执行单调的策略变更管理。他们将集中精力寻求让网络更具弹性和可扩展性且更易于管理的方法。

要培养 SDDC 和网络虚拟化领域的专业知识，网络管理员和架构师必须具备在现阶段和未来实现成功所需的专业技能和知识。

经济优势：节省大量 CAPEX 和 OPEX

高效微分段带来 CAPEX 节省

许多企业通常都会在数据中心内部署防火墙来控制日益增长的东西向流量，这种方法所耗费的成本已变得过于高昂。此外，该方法所需的设备之多以及设置和管理复杂的防火墙规则组合所需的精力都使其在运维上变得不可行。

除了能让微分段变得更为简单和安全，VMware NSX 还极大降低了该特定使用情形的 CAPEX 和 OPEX。仅从资金开销的角度衡量，NSX 可让企业在采购用于微分段的物理防火墙方面节省高达 70% 的开销。下图分析了一家想要通过微分段改善数据中心内部各服务器之间流量控制的企业所能节省的 CAPEX。

环境和容量	
VM 数量	2,500
每 CPU VM 数量	5
每服务器 CPU 数	2
服务器	250
需要 FW 控制的 VM 的百分比	40%
Gbps - 平均每台主机的应用吞吐量	7
Gbps - 所有 VM 需要的防火墙吞吐量（以 Gbps 为单位）	1,750
Gbps - 需要的有效防火墙吞吐量	700
防火墙数（每针对 HA 实现 20Gbps 吞吐量即增加 2 倍）	70
硬件成本	
每 20 Gbps FW 清单计价	135,000 美元
硬件防火墙总成本（但在操作上不可行）	9,450,000 美元
NSX 成本	
每 CPU 的 NSX 清单计价	*5,995 美元*
NSX 总成本	*2,997,500 美元*
借助 NSX 节省的 CAPEX	**6,452,500 美元**
	68%

IT 自动化降低了运维成本

我们来了解一下企业如何使用 NSX 来显著降低运维开销。NSX 显著减少了网络连接任务（包括调配、更改 / 调整、扩展和故障排除 / 修复）的手动工作量和周期时间。（周期时间会将由于请求、审批、协调、交接、后勤工作、停机时段等造成的延迟考虑在内。）

网络虚拟化和简化的分支 / 主干型结构可显著减少完成网络任务所需的工作量和时间。通常，NSX 可将工作量从数小时减少到数分钟，将周期用时从数天缩短到数分钟。如果您考虑跨开发、测试、生产前调试和生产环境来调配和管理物理网络所需执行的所有手动任务，以及 NSX 可以自动执行这些任务的事实，就可以开始看到降低运维开销的所有机会。

正如以下的 OPEX 分析显示，NSX 大大加快了将网络初次调配到生产环境的速度。如果使用传统硬件，与为新应用调配网络关联的周期时间将迫使企业等待 23 天。NSX 可将该时间缩短至数分钟，以尽可能缩短销售就绪时间。同样，为新应用调配网络需要 14 个工时或将近两天的工作量。NSX 将工时缩短到不到 2 小时，减少幅度高达 87%。

	任务量（小时）		周期用时（天）	
	手动	自动化 - NSX	手动	自动化 - NSX
请求和审查网络和安全性资源	1.00	0.00	1	0
定义网络和安全性环境	4.50	1.00	3	0
确定所需更改（容量可用性）	4.50	0.00	3	0
审查和批准流程（更改审批委员会）	0.50	0.50	5	0
更改命令调度	0.50	0.00	5	0
配置网络（VLAN、路由）	1.00	0.00	2	0
安全性配置（防火墙）	1.00	0.00	2	0
配置负载均衡器	1.00	0.00	2	0
调配环境	0.30	0.30	0	0
总计	14.30	1.80	23	0
借助 NSX 节省的 OPEX	**12.50 小时**		**23 天**	
	87%		**100%**	

高效利用服务器资产节省 CAPEX

企业还可使用 NSX 访问数据中心内未用计算容量的孤岛。在传统拓扑中，每个网络集群都有自己的计算容量。由于访问其他集群中的可用容量所需的网络重配置工作十分耗时且容易出错，因此 IT 往往过度调配计算资源。根据众多衡量结果，网络的总计算容量中有 60% 或以上处于闲置状态，从而浪费了资源。企业可使用 NSX 桥接两个或更多个网络集群，并将工作负载部署到这些未用的容量中。因此，通过使用现有的服务器容量而不是购买新的物理服务器，他们可以节省超过 88% 的成本。以下 CAPEX 分析显示了企业通过利用 NSX 来使用其更多现有计算容量，每年节省的服务器开销：

环境	
服务器	250
运维 VM	1,000
当前高效的服务器整合比	4:1
设计整合比/每台主机的 VM 数（由应用性能要求确定）	10:1
年 VM 增长率	30%
每年的 VM 数	300
计算资产使用率	
当前计算资产使用率	40%
有效利用的服务器容量	100
有效的隐秘服务器容量（60% 超额配置）	150
目标计算资产利用率	85%
目标资产利用率下具有当前主机容量的运维 VM	2,125
高效的目标服务器整合比	8.5:1
目标资产利用率下有效利用的服务器容量	213
目标资产利用率下有效的隐秘服务器容量（15% 超额配置）	37
未采用 NSX 的成本	
平均主机成本	12,000 美元
当前计算资产利用率下用于支持增长的年度服务器成本（每年 75 台服务器）	900,000 美元
当前计算资产利用率下用于支持增长的 5 年服务器成本	4,500,000 美元
采用 NSX 的成本	
不增加主机容量的情况下实现计划内年度增长的年度数	3.75
目标资产利用率下用于支持增长的 5 年服务器成本（共 45 台服务器）	**540,000 美元**
借助 NSX 实现的 5 年 CAPEX 节约	**3,960,000 美元**
	88%
5 年 NSX 成本 每台服务器 2 个 CPU，每个 CPU 的产品标价为 3,995 美元 + 4 年产品升级和技术支持服务（提供 25% 的折扣）	**3,995,000 美元**
5 年投资回报	**99%**

高性价比带来 CAPEX 节省

某些使用 NSX 的企业已经从采用固定第 2 层框架的传统三层设计（访问 / 聚合 / 核心），改为基于针对东西向流量进行优化的第 3 层结构的双层（分支 / 主干）设计。在这些结构中，第 2 层邻接关系、逻辑交换和路由均由 NSX 进行处理。许多企业都在逐渐弃用其专有硬件，而使用可从多个来源购买、具有更好性价比的成本更低的基础架构。与现有设备相比，那些使用安装有 Linux OS 的裸机交换机的企业将实现 66% 的 CAPEX 节约。

	每台交换机的成本	新交换机数量	总计
传统交换机	18,400 美元	25	460,000 美元
裸机交换机	6,300 美元	25	157,500 美元
	借助 NSX 节省的 CAPEX		302,500 美元 66%

建议：首先进行虚拟化

VMware 建议企业在需要增加网络容量时先进行虚拟化。企业发现，通过虚拟化他们的工作负载，他们可以将所需的物理端口数减少 60% 以上，从而实现可观的 CAPEX 节省。

硬件生命周期延长节省 CAPEX

企业使用 NSX 可从其现有的网络基础架构中获得更多价值。NSX 可对来自网络核心的日益增加的东西向流量进行负载分流，并延长其寿命，而不用增加成本高昂的容量。而且，借助 NSX，底层网络硬件会转变为简单的 IP 转发底板。企业可以选择将其现有的网络连接设备使用更长一段时间，而不用在会计折旧周期结束时对其进行更新。使用此方法，他们只在添加更多容量或在单个设备出现故障时更换设备的情况下，才需要操作硬件。

企业在省去硬件 CAPEX 的同时，也省去了“淘汰更换”迁移所需的 OPEX。企业借助该战略可节省数百万美元的预算开支，节省比例通常在 80% 以上。以下是针对将其现有网络连接设备使用更长一段时间的企业的 CAPEX 节约分析：

传统更新周期
5 年摊销，但在 3 年后更新。

	第 1 年	第 2 年	第 3 年	第 4 年 - 更新	第 5 年	第 6 年	第 7 年	第 8 年 - 更新	8 年的总成本
网络交换机									
新	10	1.50	1.73	11.98	2.28	2.62	3.02	14.97	48
成本	180,000 美元	27,000 美元	31,050 美元	215,708 美元	41,064 美元	47,223 美元	54,307 美元	269,453 美元	865,804 美元
负载均衡器									
新	15	2.25	2.29	17.98	3.42	3.94	4.53	22.45	74
成本	450,000 美元	67,500 美元	77,625 美元	539,269 美元	102,659 美元	118,058 美元	135,767 美元	673,632 美元	2,164,509 美元
防火墙									
新	30	4.50	5.18	35.95	6.84	7.87	9.05	44.91	144
成本	4,050,000 美元	607,500 美元	698,625 美元	4,853,419 美元	923,932 美元	1062,521 美元	1,221,899 美元	6,062,684 美元	19,480,581 美元
总计	4,680,000 美元	702,000 美元	807,300 美元	**5,608,395 美元**	1,067,654 美元	1,227,802 美元	1,411,973 美元	**7,005,769 美元**	**22,510,893 美元**

应用 NSX 延长的生命周期

	第 1 年	第 2 年	第 3 年	第 4 年	第 5 年	第 6 年	第 7 年	第 8 年	8 年的总成本
网络交换机									
新	10	1.50	1.73	1.98	2.28	2.62	3.02	3.47	27
成本	180,000 美元	27,000 美元	31,050 美元	35,708 美元	41,064 美元	47,223 美元	54,307 美元	62,453 美元	478,804 美元
负载均衡器									
新	15	2.25	2.29	2.98	3.42	3.94	4.53	5.20	40
成本	450,000 美元	67,500 美元	77,625 美元	89,269 美元	102,659 美元	118,058 美元	135,767 美元	156,132 美元	1,197,009 美元
防火墙									
新	30	4.50	5.18	5.95	6.84	7.87	9.05	10.41	80
成本	4,050,000 美元	607,500 美元	698,625 美元	803,419 美元	923,932 美元	1,062,521 美元	1,221,899 美元	1,405,184 美元	10,773,081 美元
总计	4,680,000 美元	702,000 美元	807,300 美元	**928,395 美元**	1,067,654 美元	1,227,802 美元	1,411,973 美元	**1,623,769 美元**	**12,448,893 美元**
借助 NSX 节省的 CAPEX				**4,680,000 美元**				**5,382,000 美元**	**10,062,000 美元**
				83%				**77%**	**45%**

假设前提

年增长率	10%	网络交换机	18,000 美元
年故障率	5%	负载均衡器	30,000 美元
		防火墙	135,000 美元

总结

变革性优势和无中断部署

VMware NSX 在网络连接领域引发的大规模结构转型前所未有，就像 VMware 在计算虚拟化领域引发的转型一样。NSX 会改变传统网络连接的现状，并释放 SDDC 的全部潜在价值。

各个行业的企业无论规模大小，都可使用 NSX 摆脱基于硬件的数据中心的限制和束缚，并实现大量高价值 IT 成效。他们将获得大量好处，包括更高的安全性、按需 IT 服务交付、更快的上市速度、全新的竞争优势以及显著的 CAPEX 和 OPEX 节约。

企业可将 NSX 用于多种此前无法通过传统数据中心基础架构实现的使用情形。随着他们部署更多使用情形并利用更多平台功能，获得的价值也显著增加。

开始体验

加入将 NSX 作为其 SDDC 的战略支柱的 VMware 领先企业客户之列。如您所见，企业正使用 NSX 提供多个高价值使用情形。许多企业客户都已开始使用微分段来保护处理 PCI 或 PII 数据的敏感工作负载。在看到成效后，他们会将微分段扩展到其数据中心的所有工作负载中。在完全部署微分段后，企业可使用 NSX 平台处理另一种使用情形，例如 IT 自动化、自助服务研发云计算，或者我们讨论过的许多其他情形之一。

让您的 VMware 代表或合作伙伴演示 NSX 的强大功能。让他们知道您想要了解的使用情形和功能。

参考资源

[1] Transforming the Datacenter with VMware's Software-Defined Data Center vCloud Suite。Taneja Group。

[2] Cloud Computing Trends: 2015 State of the Cloud Survey。RightScale。

[3] 2014 Data Breach Investigation Report。Verizon。

[4] 2014 Cost of Data Breach Study: Global Analysis。Ponemon Institute。

[5] 隐私权信息交流中心。

[6] Sony Breach Could Cost $100 million。《华尔街日报》。

[7] Network Agility Research 2014。Dynamic Markets。

[8] Network Agility Research 2014。Dynamic Markets。

[9] 2014 Network Barometer Report。Dimension Data。

[10] 2013 Cost of Data Center Outages。Ponemon Institute。

[11] Network Agility Research 2014。Dynamic Markets。

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
中国北京海淀区科学院南路 2 号融科资讯中心 C 座南楼 1 层 邮编：100190 电话：+86-10-5993-4200
中国上海办公室 上海市淮海中路 333 号瑞安广场 15 楼 1501 室 邮编：200021 电话：+86-21-6034-9200
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