# 数据中心微分段

## 针对“零信任”安全策略的软件定义数据中心方法

白皮书

vmware®

目录

**内容提要** ..... **3**

**软件定义的数据中心就是未来** ..... **4**

**SDDC 更敏捷、更灵活且更安全** ..... **5**

**SDDC – 武器，而非目标** ..... **5**

**真正微分段数据中心网络的曙光** ..... **6**

性能 ..... 6

自动化 ..... 6

**由 NSX 提供支持的 SDDC 中的原生安全功能 隔离和分段** ..... **7**

隔离 ..... 7

分段 ..... 7

通过高级安全服务插入、串联和流向引导实现的分段 ..... 7

**成本** ..... **8**

**更加安全的数据中心 – 软件定义的新常态** ..... **8**

## 内容提要

虽然软件定义的数据中心 (SDDC) 的体系结构已得到充分了解，但随着组织逐渐部署并发现其他需要改进的方面，它正开始显露出其敏捷性、速度和效率以外的一些优势。组织正在推进 SDDC 部署的一个关键领域是安全性。

当企业和公共部门 IT 组织采用 SDDC 并虚拟化计算、网络和存储后，他们可以自动执行调配，并大幅缩短 IT 应用和服务的销售就绪时间。他们还可以简化基础架构的迁移、添加和变更过程，同时消除相应风险。这种全新的运营模式可提供一些额外的优势。在客户利用 VMware NSX 平台的自动化和“嵌入式”安全功能来构建其 SDDC 的过程中，他们意外发现了一些显著的安全优势。随着黑客在组织数据中心边界内自由移动日益频繁，为了解决这一问题，许多企业在尝试针对数据中心网络采用一种越来越精细的分段方法（如 Forrester Research 的“零信任”网络体系结构）。这些方法能够将安全控制功能打包成小得多的资源组，通常可以小到一小组虚拟化资源或单个虚拟机。尽管从安全角度来看，微分段这种方法是一种最佳实践，但它却很难应用到传统环境中。凭借 NSX 平台固有的安全和自动化功能，微分段第一次在企业数据中心范围内在操作上变得可行。

VMware NSX 可针对数据中心网络部署三种安全模式：完全隔离的虚拟网络、分段的虚拟网络（通过 NSX 平台自带的高性能、全自动防火墙），以及我们的安全合作伙伴提供的高级安全服务实现的分段。合作伙伴集成的示例包括 Palo Alto Networks 通过新一代防火墙提供的网络分段或 Rapid7 提供的漏洞扫描。

在业务案例方面，使用 VMware NSX 提供的网络微分段不仅在操作上可行，而且经济高效，只需硬件成本的一小部分即可在数据中心网络内部部署安全控制功能。

许多大型数据中心都将安全性视为软件定义数据中心的首要优势之一。在不久的将来，安全性更高的数据中心将成为新常态。

## 软件定义的数据中心就是未来

软件定义的数据中心 (SDDC) 是数据中心设计的一种体系结构方法，它利用了计算机科学的一个基本原理：抽象化。操作系统、更高级别的编程语言、网络连接协议以及最近的服务器虚拟化都是抽象化的示例，在过去 25 年中，抽象化的引入导致了主要行业创新周期的产生。通过引入抽象层，抽象层上方和下方的系统和服务能够独立地运行和实施创新，同时通过完善的接口在各层之间维持商定的通信路径并推出服务。SDDC 方法采用了抽象化原则，以软件形式交付整个数据中心架构，从而将服务交付与底层物理基础架构分离开来。这样一来，用户就可以将底层硬件作为一般化的计算、网络和存储容量池使用，并能够以编程方式对其进行组合、使用并重新调整其用途，而无需修改硬件。

SDDC 方法已经过全球众多最大型、最敏捷且最高效的数据中心的验证，包括 Google、Facebook 和 Amazon。在过去 10 年中，这些“巨型数据中心”运营商已通过设计将 SDDC 抽象层整合到其自定义应用和平台中，这使他们能够实现数据中心运营几乎每个方面的自动化，同时与底层计算、网络和存储硬件完全分离。这种分离可显著降低其物理基础架构的资金和运营开销，并使他们能够以比大多数企业 IT 组织快出许多的速度来交付客户订购的服务。

如今，企业 IT 部门可在其数据中心内实现与“巨型数据中心”相同级别的敏捷性和效率，而无需修改其现有硬件基础架构。

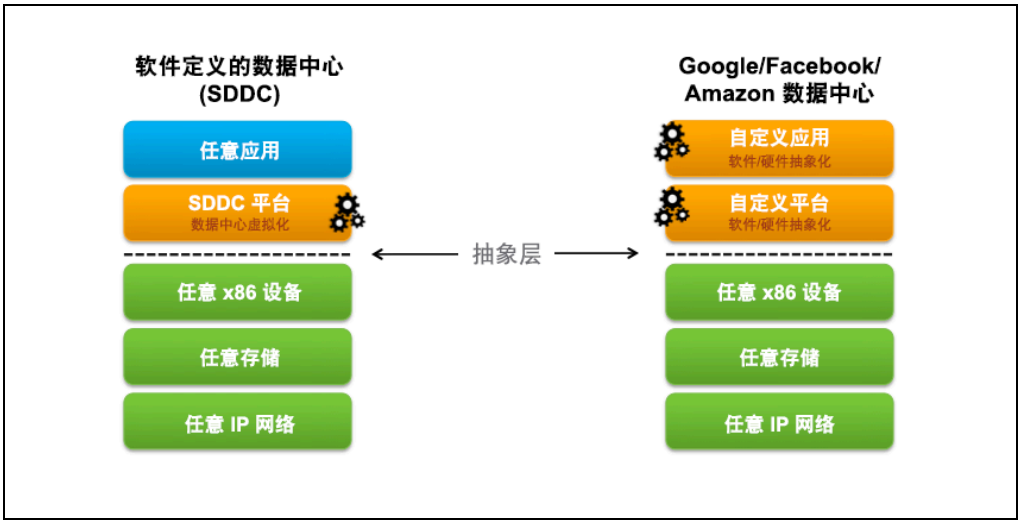


图 1 - 将智能转移到软件中，以便在软件和底层物理基础架构之间创建抽象层。通过将智能应用到其自定义应用或平台软件中，大型数据中心十年以来一直采用这种方法。如今，企业数据中心可通过利用数据中心虚拟层中的软件来实现相同的分离。

VMware 已将数据中心抽象层内置到其 NSX 网络虚拟化平台中。该平台基于传统虚拟化管理程序和虚拟交换机相结合的分布式系统控制器，可使整个数据中心架构忠实地无中断重现在软件中，且独立于现有的物理基础架构。VMware NSX 平台已在大量生产部署中得到验证，其中一些部署已超过三年，目前正在部署的单位包括全球三大服务提供商中的两家、全球五大金融服务公司中的四家以及几乎每个行业（包括医疗保健业、制造业、零售业、消费类产品业、银行业、保险业、交通运输业、联邦政府、州政府和地方政府以及高科技业）中超过 100 个企业级数据中心。

## SDDC 更敏捷、更灵活且更安全

SDDC 方法充分利用了虚拟化和自动化的优势，并将这些优势延展到整个数据中心架构内。在软件中以编程方式针对虚拟机执行创建、快照拍摄、移动、删除和还原操作的能力转变了 IT 计算的运维模式。现在，借助 SDDC 方法，IT 能够以编程方式在软件中对计算、存储和网络方面的整个数据中心架构执行创建、快照拍摄、移动、删除和还原操作。数据中心自动实施的自助式 IT 以及网络运维模式的全面转型均已成为 SDDC 方法公认的巨大优势。在部署中，业务与 IT 领导均同意，SDDC 方法可在 IT 速度、敏捷性和竞争优势方面提供可衡量的优势。IT 运维主管可快速从自动执行的变更管理以及简化的底层硬件配置和管理中受益。而最深远的影响可能是，SDDC 方法可让基础架构和安全团队在数据中心内实现投资灵活性（可构建普通云，并快速扩展为混合云）和保护（利用现有硬件）、提高利用率并实现前所未有的安全性。事实上，安全功能被证实是 SDDC 平台最具吸引力的应用之一。

## SDDC – 武器，而非目标

乍看之下，大多数 IT 网络安全专业人士会将诸如 SDDC 之类的新方法视为新的潜在目标。实际上，与对需要保护的内容所做的变更相比，这种方法对 IT 实施安全功能的方式所造成的影响要大得多（更加积极）。换句话说，对于 IT 安全团队来说，与其说 SDDC 是目标，不如说它是武器。SDDC 方法可以实际交付一个平台，该平台能够从本质上解决数据中心设计中的某些基本体系结构局限性，几十年以来，这些局限性对安全专业人士造成了限制。

思考一下在传统安全方法中，人们通常会在知情程度和隔离之间进行的权衡。通常，为了做到知情，我们会将控制功能放置在主机操作系统中。借助这种方法，我们能够查看正在访问的应用和数据以及正在使用系统的用户，从而实现良好的知情程度。但是，由于控制功能位于攻击域，因此攻击者首先会禁用控制功能。这就是失败的隔离。这种方法相当于将家庭警报系统的开关安装在房屋外部。还一种重视隔离而非知情程度的替代方法，就是将控制功能放置在物理基础架构中。这种方法可将控制功能与其所保护的资源隔离，但知情程度较差，因为 IP 地址、端口和协议对用户、应用或事务上下文而言是非常糟糕的代理。此外，到目前为止，从未出现过内置在基础架构中且无所不在的强制实施层。

SDDC 使用的数据中心虚拟层与无所不在的强制实施层相结合，可提供理想的位置，从而同时实现知情与隔离。数据中心虚拟层中运行的控制功能可利用安全的主机自检，能够提供无代理且高清晰的主机上下文，同时在虚拟化管理程序中保持隔离，免受攻击者尝试发出的攻击。

数据中心虚拟层在应用和物理基础架构之间的理想位置，再加上自动化调配和网络与安全策略管理、嵌入在内核中的性能、分布式实施以及横向扩展容量，正使得数据中心安全性面临完全转型的边缘，并使数据中心安全专业人士能够实现过去在操作上无法实现的安全级别。

## 真正微分段数据中心网络的曙光

针对企业数据中心的以边界为中心的网络安全策略经证实存在不足。新型攻击可以突破仅限于边界的防御体系，随授权用户混入，然后在数据中心边界内的各个工作负载之间横向扩散，并且很少有或没有控制功能来阻止其传播。最近公布的许多违规情况都证明了这一点：从钓鱼式攻击或社交工程攻击开始，在数据中心内产生恶意软件、利用漏洞、发出命令和控制以及不受拘束地横向扩散，直到攻击者找到他们的目标，然后再撤出。

数据中心网络的微分段可提供巨大帮助来限制这种未经授权的横向扩散，但它无法在传统数据中心网络中操作。究竟是什么原因呢？

传统防火墙以及高级的新一代防火墙在网络上以物理或虚拟“瓶颈点”的形式实施控制功能。由于应用工作负载流量肯定会流经这些控制点，因此可以强制实施防火墙规则，并且能够阻止或允许数据包通过。如果使用传统防火墙方法来实现微分段，将很快遇到两个主要运维障碍：吞吐容量和运维/变更管理。首先，容量障碍可以通过投入一定的成本来克服。用户可以购买足够的物理或虚拟防火墙来交付所需的容量，从而实现微分段。但其次，运维障碍会随着工作负载的数量以及当今数据中心日渐动态化的特性呈指数增加。如果每次添加、移动或停用虚拟机都需要手动添加、删除和/或修改防火墙规则，那么变更率很快便会使 IT 运维不堪重负。正是这一障碍导致了大多数安全团队为实现全面微分段或“零信任”战略而制定的完美计划执行失败。

VMware SDDC 方法可利用 NSX 网络虚拟化平台来提供诸多相对于传统网络安全方法的显著优势，包括自动执行调配、自动移动/添加/变更工作负载、在每个虚拟接口处和内核中执行分布式实施、横向扩展防火墙性能、分布于每个虚拟化管理程序以及内嵌到平台中。

### 性能

需要注意的重要一点是，NSX 平台中提供的防火墙性能并非旨在替换用于南北向边界防御的硬件防火墙平台。硬件防火墙平台的性能容量旨在对来自数百或数千个工作负载的流量进入或离开数据中心边界的行为进行控制。

也就是说，NSX 平台的防火墙性能和容量极为强大。NSX 平台可交付 20 Gbps 的防火墙吞吐量，并支持每台主机每秒 80,000 个连接。此性能仅适用于其虚拟化管理程序上的虚拟机，并且每次向 SDDC 平台新添加一台主机时，都会再增加 20 Gbps 的吞吐容量。

### 自动化

借助自动化的调配和移动/添加/变更,系统可在以编程方式创建工作负载时调配正确的防火墙策略，这些策略会在数据中心内的任何位置或在数据中心之间随工作负载移动。此外，如果应用被删除，其安全策略也会随之从系统中删除。这可以消除使交付真正的微分段解决方案变得不可行的主要障碍。

此外，NSX 合作伙伴体系还可以充分利用 SDDC/NSX 平台的分发和自动化功能，使企业能够将各种高级安全服务串联到一起，并基于不同的安全情形实施不同的服务，从而结合应用不同的合作伙伴功能。例如，可根据标准防火墙策略调配某个工作负载，这些策略可允许或限制该工作负载对其他类型的工作负载的访问。相同策略也可以定义以下内容：如果在常规漏洞扫描期间在工作负载上检测到漏洞，则将应用限制性更强的防火墙策略，从而将工作负载限制为仅由那些用于修复漏洞的工具进行访问。所有这一切均自动执行，始终开启，无需人为干预。

通过结合使用 NSX 平台交付的性能和自动化，可具体到对每个虚拟接口设计和实施操作上可行的微分段。

## 由 NSX 提供支持的 SDDC 中的原生安全功能 隔离和分段

VMware NSX 平台可从本质上在数据中心内交付三个级别的安全性：隔离、分段以及通过高级服务实现的分段。

### 隔离

隔离是大多数网络安全机制的基础，无论是为了保持合规性和控制力，还是仅仅用于防止开发、测试和生产环境进行交互。虽然过去使用物理设备上手动配置和维护的路由、ACL 和/或防火墙规则来建立和强制实施隔离，但隔离和多租户架构是网络虚拟化的固有功能。虚拟网络彼此隔离，并且默认情况下与底层物理网络隔离，从而实现最少特权安全原则。无需使用任何物理子网、VLAN、ACL 以及防火墙规则，即可实现这种隔离。这一点值得重复…无需任何配置。除非专门将虚拟网络连接在一起，否则它们以隔离方式创建并且始终保持隔离状态。

任何隔离的虚拟网络均可以由分布在数据中心中的任何位置的工作负载组成。同一虚拟网络中的工作负载可以驻留在相同或不同虚拟化管理程序中。此外，多个隔离的虚拟网络中的工作负载也可以驻留在同一虚拟化管理程序中。下面是一个非常有用的示例：虚拟网络之间的隔离允许重叠的 IP 地址，从而能够实现相互隔离的开发、测试和生产虚拟网络，每个网络都包含不同的应用版本，但却拥有相同的 IP 地址，所有网络均可同时运行，并且全部位于同一底层物理基础架构中。

虚拟网络还将与底层物理基础架构隔离。由于虚拟化管理程序之间的流量是封装的，因此运行物理网络设备的地址空间与工作负载用于连接到虚拟网络的地址空间完全不同。例如，虚拟网络可以基于 IPv4 物理网络支持 IPv6 应用工作负载。这种隔离可以帮助基础物理基础架构抵御由任何虚拟网络中的工作负载发起的任何可能的攻击。再次说明，这一切都不依赖于过去创建这种隔离所需的任何 VLAN、ACL 或防火墙规则。

### 分段

分段与隔离相关，但应用于多层虚拟网络中。过去，网络分段是物理防火墙或路由器的一项功能，旨在允许或拒绝各网段或各层之间的流量。例如，对 Web 层、应用层和数据库层之间的流量进行分段。过去定义和配置分段的过程非常耗时，而且极易出现人为错误，从而导致大量安全违规情况。实施过程需要对设备配置语法、网络寻址、应用端口和协议具有精到、专门的专业技能。

与隔离一样，网络分段也是 VMware NSX 网络虚拟化的一项核心功能。虚拟网络可以支持多层网络环境，这意味着多个第 2 层网段（每个第 2 层网段上有第 3 层分段或微分段）可以使用工作负载安全策略定义的分布式防火墙规则。如上面的示例中所示，这些层可以表示 Web 层、应用层和数据库层。物理防火墙和访问控制列表可提供成熟的、受网络安全团队和合规性审核员信任的分段功能。不过，人们对在云数据中心中采用这种方法的信心已经动摇，因为越来越多的攻击、违规和停机都是由于过时的手动网络安全调配和变更管理流程中的人为错误引起的。

在虚拟网络中，配备有工作负载的网络服务（第 2 层、第 3 层、ACL、防火墙、QoS 等）以编程方式创建并分发给虚拟化管理程序虚拟交换机。包括第 3 层分段和防火墙在内的网络服务在虚拟接口中实施。虚拟网络内的通信绝不会离开虚拟环境，因此无需在物理网络或防火墙中配置和维护网络分段。

### 通过高级安全服务插入、串联和流向引导实现的分段

基础 VMware NSX 网络虚拟化平台提供基本的有状态检测防火墙功能，以便在虚拟网络内提供分段。在某些环境中，需要更高级的网络安全功能。在这些情况下，客户可以利用 SDDC 平台在虚拟化网络环境中分发、启用和强制实施高级网络安全服务。NSX 平台将网络服务分发到虚拟交换机中，以形成适用于虚拟网络流量的服务的逻辑管道。可以将第三方网络服务插入此逻辑管道中，从而允许在逻辑管道中使用物理或虚拟服务。

每个安全团队都使用各种网络安全产品的独特组合来满足其环境的需求。目前，VMware 的整个安全解决方案提供商体系都在使用 VMware NSX 平台。网络安全团队经常面临协调多个供应商所提供网络安全服务的关系的挑战。NSX 方法的另一个强大优势是它能够构建策略来利用 NSX 服务的插入、串联和流量引导功能，以便基于其他服务的结果推动服务在逻辑服务管道中执行，从而能够协调多个

供应商提供的本来毫不相关的网络安全服务。

例如，我们与 Palo Alto Networks（请参阅此处的博文）的集成将利用 VMware NSX 平台来分发 Palo Alto Networks 虚拟机系列的新一代防火墙，从而在每个虚拟化管理程序上本地提供高级功能。为调配或移到该虚拟化管理程序的应用工作负载定义的网络安全策略将插入虚拟网络的逻辑管道中。在运行时，服务插入功能将利用本地提供的 Palo Alto Networks 新一代防火墙功能集，在工作负载虚拟接口交付和强制实施基于应用、用户以及上下文的控制和策略。

另一个示例包括我们的合作伙伴 Rapid7，Rapid7 可定期对虚拟机自动执行漏洞扫描，并能实现可在虚拟机不满足特定标准时自动隔离虚拟机的策略。将此功能与 Palo Alto Networks 的 NGFW 结合使用后，我们可以在 Rapid7 漏洞扫描出现故障时自动隔离易受攻击的工作负载，而隔离网段将受到 Palo Alto Networks NGFW 策略的保护，该策略只允许修复工具入站，禁止一切出站行为。

## 成本

通过利用 VMware NSX，SDDC 方法不仅使微分段在操作上变得可行，而且经济高效。通常，微分段设计的第一步是将东西向流量设计为以 U 字形通过高容量物理防火墙。如上文所述，此方法成本高昂且需要大量操作，在大多数大型环境中均不可行。整个 NSX 平台通常只占到这些设计中物理防火墙成本的一小部分，并且可以随着客户增加工作负载而以线性方式横向扩展。

## 更加安全的数据中心 – 软件定义的新常态

现在，我们仍然需要使用边界安全控制，但数据中心网络内部的控制不仅变得必要，而且还值得庆幸的变得可行。作为软件定义的数据中心体系结构的一个关键要素，VMware NSX 网络虚拟化平台已在您已拥有的物理基础架构上为安全团队打开了全新运维模式的大门。无需新的网络连接硬件。只要您做好准备，即可或多或少地对您的数据中心环境执行虚拟化。

本文只是浅显地介绍了 SDDC 方法和 VMware NSX 网络虚拟化平台所能提供的安全功能。随着越来越多的数据中心采用软件定义的数据中心体系结构，我们将看到大量 VMware 和合作伙伴解决方案开始利用 SDDC 数据中心虚拟层所提供的独特优势。关于虚拟机和应用流程负责人的详细知识以及自动化调配速度和运维效率是这一激动人心的新方法的基础，可应对某些非常陈旧的数据中心安全挑战。

**VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001**
**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 3 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**