微分段无比强大且易于添加的七个原因

为何数据中心需要更强的防御系统

针对数据中心的攻击在不断增加，而物理安全设备并不足以抵御这些攻击。独立研究表明，攻击得逞的情况越来越常见，令人震惊之余，也让受到攻击的公司蒙受损失。毫无疑问，如果数据中心行业要结束这一局面，而不是任由其发展下去，我们需要新的模式来保护数据中心的安全。

边界防火墙或许是忠诚而坚定的“守门者”。然而，一旦恶意软件进入数据中心（通常是通过寄生在合法流量上的方式），几乎没有任何反制措施来遏制其肆意扩散。

“以边界为中心”的安全模式能够应对由南至北的流量，也就是从客户端到服务器之间的流量。但它不能处理东西向流量，也就是服务器之间的通信流量。在数据中心内配置足够的物理防火墙来保护成百上千的工作负载，这在技术上或经济上都是不可行的。

普遍性、精确度和动态安全必须融入数据中心的 DNA 中

VMware NSX® 网络虚拟化平台可提供诸多突破性益处，微分段便是其中之一。NSX 可创建一个独立于底层 IP 网络硬件的虚拟网络。管理员能够以编程方式对复杂网络执行创建、调配、拍摄快照、删除和还原操作，而且这一切都能以软件方式实现。

VMware 将微分段描述为一种“将安全机制植入网络的 DNA 中”的能力。就好比在分子或细胞级别对植物进行工程设计，使之有能力抵御病虫害。

因为 hypervisor 已在数据中心内广泛分布，所以您可以通过 VMware NSX 在任意位置创建策略来保护任意数据，让安全真正无所不在。从某种意义上说，物理安全就像戴上手套来防范细菌。这是外在的、有限的保护措施（如果有人对着您的脸打喷嚏，您可能还是会感冒或染上流感）。微分段就像是强化数据中心的免疫系统：让“细菌”（即恶意软件）对它无能为力。或者，如果有漏网之鱼，该系统会在该恶意软件开始扩散之前就将其关闭。

策略绑定到虚拟机，执行效力可向下延伸至虚拟网卡 (NIC)，这种精确度是传统的硬件设备无法比拟的。

您也可以使用灵活的参数来定义安全策略，例如虚拟机名称、工作负载类型和客户操作系统类型。

微分段无比强大且易于添加的七个原因

1. **无需更换您目前拥有的设施，亦不会对其造成不利影响**
   VMware NSX 可在任意网络硬件上运行，因此您无需购买或更换任何设备。此外，NSX 不会给您的计算机和网络基础架构或应用造成中断。
2. **降低不断攀升的硬件成本**
   为处理数据中心内日益增多的工作负载量而部署更多物理设备的成本过于高昂。仅从资金开销的角度衡量，VMware NSX 可以让企业组织的实际开销节省 68%[1]。这一节省比例基于以下估算，即 IT 管理员要实现接近微分段的控制力需要多大的物理防火墙开销。
3. **遏制防火墙规则剧增状况**
   数量激增的防火墙规则是安全管理领域里的一个大问题。年复一年，管理员积攒了不少不必要的和多余的规则，而且无法使用简单的方法来找出哪些规则是不再需要的。防火墙规则剧增使得安全审核成为噩梦般的负担。过时的和矛盾的规则甚至可能成为安全漏洞的意外导火索。

   借助微分段和 VMware NSX，策略可集中编排并关联到它们所保护的虚拟机，因此您只需通过一个界面，就能自动管理整个数据中心的安全策略。当您调配、移动或删除虚拟机时，它的防火墙规则也会随之添加、移动或删除。

[1] 《使用 VMware NSX 实现网络虚拟化和安全》(Network Virtualization and Security with VMware NSX)，业务案例白皮书；分析结果基于使用防火墙技术时的成本。

4. **通过更高效的流量模式调高性能**
   在物理网络中，工作负载流量通常需要穿过不止一个网络分段到达路由器和防火墙，然后才能返回至相邻的工作负载（这是一种低效的模式，称为“发夹式传输”）。如果使用微分段，流量通常可以停留在同一个虚拟网络分段中，减少了对物理网络的影响。因此，您可以消除因超额预订核心链路而导致的额外成本和低效率。

5. **满足不同 LOB（业务线）和部门的独特需求**
   由于 VMware NSX 和微分段独立于物理基础架构，因此无论是移动资源，还是确保安全性与时俱进紧跟变化，您都能获得极大的灵活性。因为安全工作是通过软件处理的，可在几分钟内就创建并运行策略，所以您能够消除因安装更多安全硬件或重新配置网络系统而导致的滞后。

   图 1 显示了您可以多么轻松地更新安全策略以满足各个业务线和部门的需求。在这个例子中，IT 部门决定将整个人力资源 (HR) 部门的桌面实现虚拟化。借助微分段，为人力资源部门的虚拟桌面创建和应用安全策略只需几分钟的时间。您只需为所有相关系统标记“HR”，VMware NSX 会自动应用正确的安全策略。

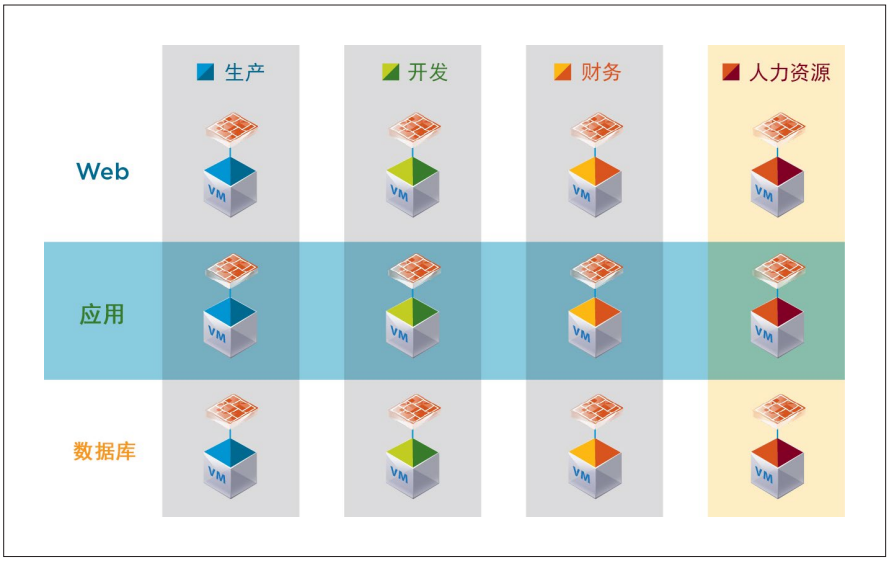

图 1 借助微分段，创建基于 VDI 的新安全策略只需几分钟，而且不会更改已经部署到位的其他策略。

6. **为您的网络专家增加有价值的新知识领域**
   管理员依旧运用他们已经掌握的 VMware 虚拟化技能，因此即使是重大安全改进，也不需要投入太多学习精力。硬件网络专家将获得新的软件技能，让他们在硬件、软件网络安全技术领域都能先人一步。对网络管理员和架构师来说，软件定义的数据中心 (SDDC) 和网络虚拟化领域的开发知识是对他们自身专业技能的极大补充。

7. **打造面向未来的运营**

   微分段让保护工作负载变得更容易、更快捷、更便宜。因此，您可以自信、放心地支持各种变化，甚至将资源重新分配到新的项目领域。

   使用 VMware NSX 实现网络虚拟化也是迈向 SDDC 模式的重要一步，而且不会有中断。这意味着您不仅在当下巩固了安全性，也为未来的 SDDC 奠定了重要基础。

了解更多

利用 VMware NSX 网络虚拟化，在以 Intel® Xeon® 处理器和 Intel® 以太网 10GB/40GB 融合网络适配器为特色的强大行业标准基础架构上，打造一个从根本上更加敏捷、高效和安全的应用环境。

有关更多信息，请访问 www.vmware.com/cn/go/nsx。有关产品规格和系统要求的详细信息，请参见 VMware NSX 文档。

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