您想了解（但还没问）的“微分段”相关内容

VMware NSX® 所实现的微分段，让“零信任”模式成为现实

确保新式数据中心的安全需要微分段

Gartner 和 Forrester 等分析机构对此看法一致，数据中心安全要求已变得愈发复杂，远非边界（物理）防火墙所能满足。以下是其中几个原因：

- 边界防火墙的任务是守住大门，而入侵防御和反病毒机制旨在保护从客户端到服务器（由北向南）而非服务器到服务器（由东向西）的数据传输
- 为保护具有精细策略和集中访问控制的成百上千的工作负载而在数据中心装满物理防火墙（或带虚拟防火墙的物理防火墙）是不切实际的做法
- 物理防火墙需要耗费过高的管理开销才能快速适应几乎时刻在变的动态工作负载；此外，它们也没有能适应环境的、精细化或自动化功能，无法“随着”工作负载迁移

随着数据中心继续加大计算、网络连接和存储资源的虚拟化程度，基于边界的传统安全措施变得更加低效。数据中心安全性的新模式将是：a) 基于软件，b) 运用微分段原则，以及 c) 支持零信任[1] (ZT) 模式。

直到现在，数据中心都在“信任区”基础上搭建，信任区中所有相似计算系统上的流量会被认为可信任。但是在信任区中，恶意软件可毫无阻碍地在服务器间移动。ZT 模式主张，在虚拟化程度更高的环境中，在受信任和不受信任的网络或分段之间应无明显差异 - 保护必须无所不在、精细入微。

为构建 ZT 模式，您需要具有能够提供微分段的虚拟化网络。

可确保数据中心安全性的新模式

- 基于软件
- 采用微分段的原则
- 采用零信任 (ZT) 模式

1. “Leverage Micro-Segmentation to Build a Zero Trust Network”，Forrester Research，2015 年

“物理网络分段和微分段之间有何区别？”

数据中心的物理网络安全性是基于设置安全分段、创建子网和虚拟 LAN 以及围绕这些要素创建策略来构建的。大体来说，该模式需要将策略锁定至工作负载所处的物理位置。这样僵化的网格结构需要手动进行耗时的管理，并导致配置频繁出错、性能受影响以及应用部署延迟 - 其带来的限制和问题还远不止这些。

借助 VMware NSX 平台，微分段将原生融入而非附加到网络体系结构上。这好比能够在分子或细胞级别就抗病虫害对植物进行改造。这正是 VMware 将微分段称为“将安全性植入网络 DNA 中”的功能的原因。

“网络 hypervisor”与服务器虚拟化模式极为类似，它以软件形式重现第 2 至 7 层的网络连接服务。这些服务可在几秒内组建为任意组合，从而生成新的网络配置。物理网络成为容量传输池。

由防火墙控制（已整合在 hypervisor 中）所实施的安全策略已广泛分布于具有 NSX 的整个数据中心。这意味着整个数据中心将即时获得全面保护。（您的现有物理防火墙和物理网络可全部保持不变，但您可以更自由地混用和选择符合您需求的供应商。）

鉴于 NSX 在 hypervisor 中的位置，它会同时提供环境和隔离功能：也就是说，它离应用和工作负载足够近，具有丰富的环境信息；但又足够远，可以将这些资产与威胁隔离。

微分段的其他突出优势有：

- 安全策略与虚拟网络、虚拟机和操作系统关联，可精细到虚拟网卡级别（实际上，微分段使您能够围绕每一个机器或工作负载来部署安全保护，这正是安全性可以如文件般添加、删除、更改和移动的原因）
- 您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
- 安全策略可在几秒内更新完毕 - 甚至可自动执行 - 以应对应用拓扑中的安全威胁或变化
- 策略将自动随工作负载移动，即使物理 IP 地址变化也无妨

NSX 会同时提供环境和隔离功能：这意味着它离应用和工作负载近到足以拥有详尽的环境信息，但是又远到足以将这些资产与威胁隔离。

VMWARE 安全合作伙伴生态体系

数据中心的安全性本身就是一个多供应商的环境。安全控制是 NSX 的固有特性，这意味着它提供集成平台。行业领先的安全产品均可得到自动部署和动态调整。下面是 VMware 的一些安全合作伙伴：

- Check Point
- Fortinet
- Intel Security/McAfee
- Palo Alto Networks
- Symantec
- Trend Micro

“哪些安全项目能够因为实施微分段获得最大好处？”

您可以按自己的时间表部署网络虚拟化，首先小步实施，然后在规划阶段或适时展开。您的安全策略可以随网络虚拟化部署或推动网络虚拟化。下面列出了三个项目示例：

数据中心安全

我们介绍了微分段可如何凭借精细的安全策略保护数据中心内的各个工作负载。要保护成百上千的工作负载，集中控制和自动化同样重要。创建虚拟机后，其安全策略会即时自动附加到虚拟机。策略会随虚拟机而移动。虚拟机停用后，策略会自动删除。有了自动化，防火墙规则将绝不可能变陈旧并造成潜在漏洞。

安全桌面用户环境

借助微分段，您可以针对单个桌面用户打造个性化的边界防御手段。例如，用户下载病毒，则“个性化 DMZ”将防止病毒从该用户的桌面以及任何其他共享信息的桌面扩散，也能防止病毒在桌面和数据中心之间散播。

DMZ 无处不在

微分段使您能够隔离任何分段并将其放在 DMZ 中。高级策略和实施与 IP 地址无关。创建 DMZ 时不再受限于网络上的特定位置，而是可与其保护的工作负载关联。

即使是“属性”也不必受拓扑或晦涩难解的防火墙命名规范限制。管理员可以将策略和安全服务设置为映射至单个基于角色的工作负载、逻辑分组（例如所有 HR 系统）、桌面操作系统，甚至是“所有处理敏感信息的虚拟机”。

总结

备受关注的数据中心泄露仍在继续导致代价高昂的损害和中断。为了应对这种情况，IT 团队提高了传统物理安全性方面的开支，但是这些大笔投资并未阻挡持续升级的攻击，原因很简单，物理网络安全性，尤其是边界防火墙并不能圆满解决数据中心安全的需求。

微分段已被广泛视为更胜一筹的数据中心模式，在如今 IT 向软件定义的数据中心 (SDDC) 和混合云模式发展的趋势下更是如此。VMware NSX 使微分段成为现实。管理员首次能够运用精细的策略来隔离和保护应用与工作负载。网络安全既可以如数据中心所要求的那样无所不在，又可以如它们所保护的资产那样动态应对各种需求。

如需了解更多信息，请访问：vmware.com/cn/products/nsx

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