Akamai

白皮书

重新审视防火墙

基于软件的分段技术令人信服的经济理由

执行摘要

网络和安全团队为何仍在依赖传统防火墙实现内部网络分段？通过策略保护的应用程序和网络分段迅速增加，而事实证明，物理防火墙设备过于复杂、缺乏灵活性，无法有效应对当今日渐动态化的混合云环境带来的安全挑战。而且其成本远高于团队可能意识到的水平。除了防火墙和硬件的巨额前期成本之外，还有可观的下游成本，包括项目管理、人工、维护成本，以及漫长的实施时间造成资产暴露时间过长而带来的实际风险。要想受益于敏捷 DevOps、快速应用程序部署和云计算，现代企业必须找到更好的方法，通过分段来确保关键资产的安全。如今确实有了这样的方法：基于软件的分段。这种方法更简单、更快捷、更有效，而且就像本文将明确展示的那样，相较于传统分段方法，它能以更低的总拥有成本提供最好的安全性。

简介

如今，我们看到有三种力量融合，共同推动着对更加精细的网络和个别资产分段方法的需求。首先，敏捷 DevOps 和其他快速交付模式高度重视更快地将应用程序部署到生产环境中。这就不可避免地要求创建更安全的区域，并制定更精准的政策。其次，随着企业迁移到云端并采用混合 IT 基础架构，其应用程序经常要在不同环境之间迁移，这就增加了整个网络的分段间流量。第三，敏捷开发造成应用程序快速增加，给黑客提供了越来越多的攻击面。

使用防火墙实现分段的方法：巅峰不再

考虑到前述情况，严格依赖 VLAN 和防火墙进行分段的做法已难以为继。从纯粹的技术角度来看，配置多个 VLAN 和防火墙以跟上应用程序开发步调的做法既复杂又繁琐。此外，这种方法还需要大量人力，分散了团队成员的过多精力，导致他们无暇顾及优先级更高的安全项目。另一个问题是部署时间，这会增加了资产长时间暴露、易于受到攻击的风险。最重要的是，其实施成本极高，不仅有防火墙和支持额外流量的新硬件的前期成本，还有与持续管理、修改和维护安装相关的成本。

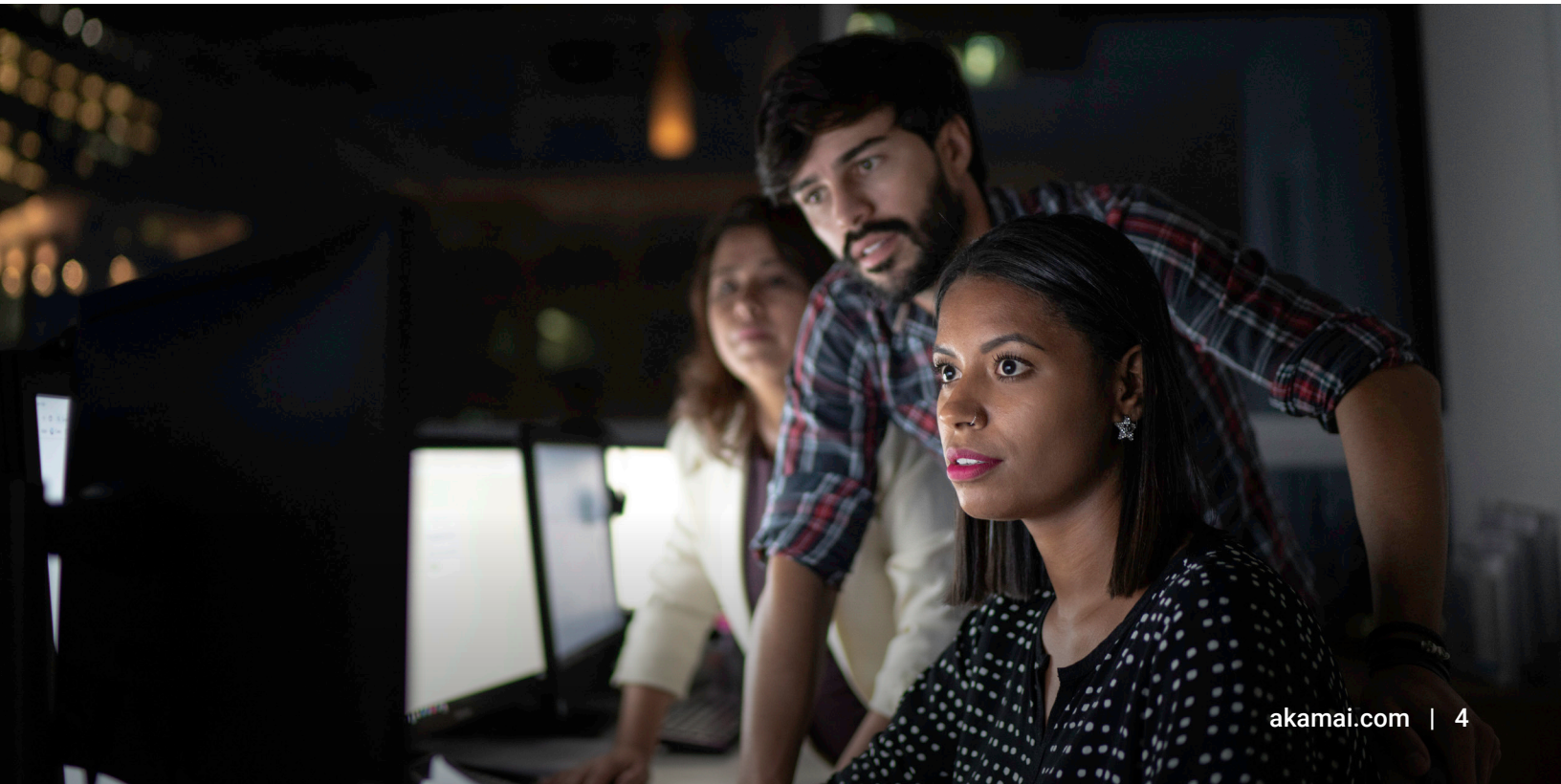
简而言之，传统网络分段方法已经陷入困境。特别是，在企业寻求利用动态云和混合环境时，依靠内部防火墙来确保安全性只会制约其灵活性、策略创建和执行速度，以及安全扩大运营规模的能力。企业比以往更迫切地需要找到一种分段方法来取代传统防火墙，这种方法应该有着现代化、简化、成本更低的特点，归根结底，它应该更加有效。基于软件的分段应运而生。

企业比以往更迫切地需要找到一种分段方法来取代传统防火墙，这种方法应该有着现代化、简化、成本更低的特点，归根结底，它应该更加有效。

痛点—高昂的防火墙管理成本

在深入探究基于软件的分段方法的优势之前，有必要将其与现状进行对比。随着企业发展壮大，应用程序的数量和相关数据流量也在不断增加，从而推动了对更多网络分段、更复杂的安全策略的需求。如果您依靠由防火墙保护的 VLAN，那么就要将所部署的每个新 VLAN 添加到每一个分段间流量经过的交换机中继端口。您还需要为每个新 VLAN 创建一个 IP 子网，为防火墙创建一个子接口，然后还需要创建防火墙策略。其中每一项更改通常都需要审批、维护时间段，还有可能造成停机时间，也就是说，网络中断风险更高。

添加 VLAN 和防火墙是一个非常痛苦的多步骤过程，需要多达五个团队参与其中，分别负责交换、路由、防火墙实施、ESXi 服务器和安全策略创建。所有这一切都延长了实施时间，延长了企业的风险暴露，并且增加了软件、硬件和人工成本。此外，从工程师的视角来看，这是一项高风险、低回报的工作—劳民伤财、得不偿失，还会占用其他高优先级风险管理活动的时间和资源。遗憾的是，在防火墙保护的 VLAN 环境中，变更管理过程中几乎没有任何步骤可以自动化。



寻找良方—基于软件的分段，仅需简单三步

传统的外围防火墙技术根本无法满足更精确、带宽更有限的精细内部分段需求。近年来，基于软件的分段已成为一种切实可行、更快、更有效且成本更低的替代方案，可满足当今动态环境中对更多、更密集的网络分段的需求。要实施基于软件的分段方法，核心就是“分布式防火墙”的概念，它比传统的网络防火墙设备更灵活、更易于管理。

> 基于软件的分段的部署速度可达到传统防火墙的 **10 倍乃至 20 倍**，所需人员更少，而且几乎不会出现停机或中断。

在基于软件的分段解决方案领域，业界优秀的产品之一就是 Akamai Guardicore Segmentation。我们这款基于软件的分段解决方案杜绝了漫长、昂贵且复杂的 VLAN 防火墙实施过程，仅需要三个步骤：

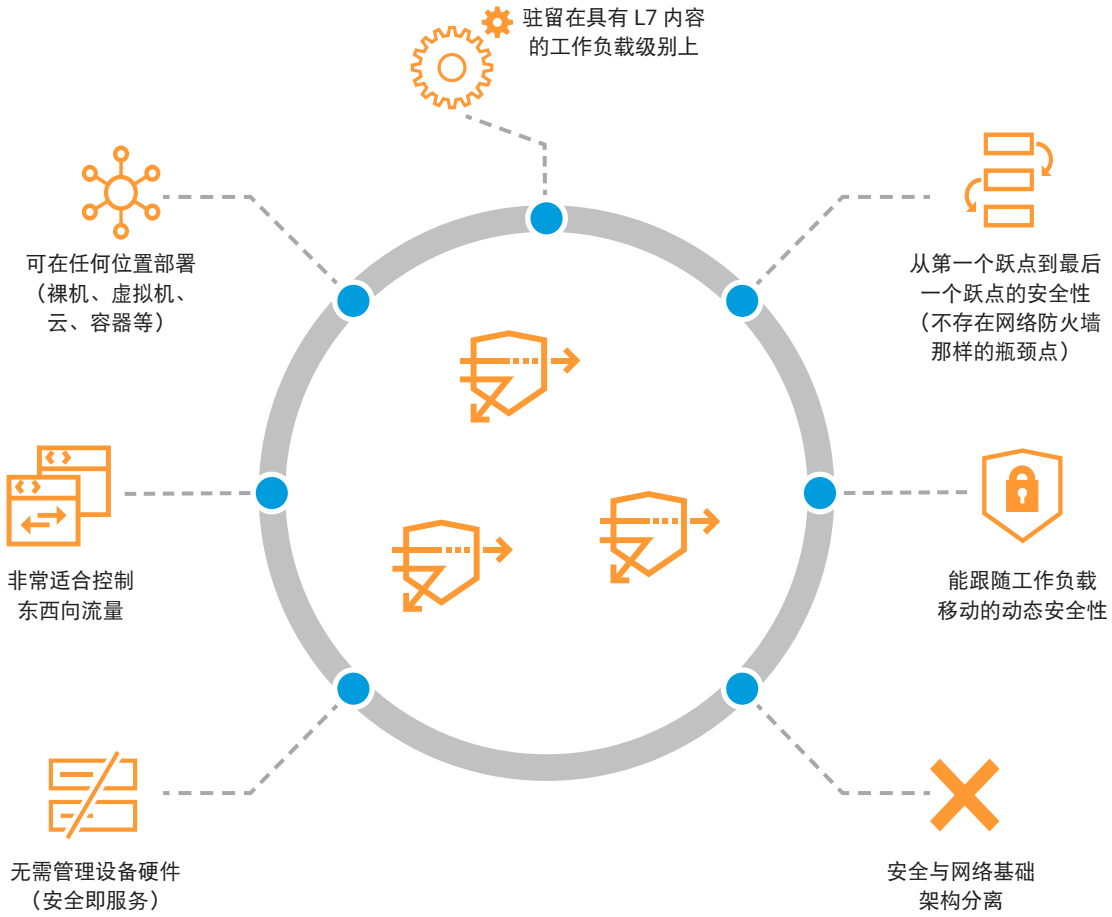
1. **识别和标记资产：**在传统防火墙实施流程中，一个主要障碍就是监测需要保护的资产的能力不足。Akamai Guardicore Segmentation 包含一项可视化功能，让操作人员可以识别并标记整个企业基础架构中运行的所有应用程序及其依赖关系。

2. **直观显示并按标签分组：**有了情景监测能力，操作人员就能根据标签将应用程序整理成逻辑分组，并映射其间的依赖关系。我们的标记流程非常灵活，您可以根据自己的业务情景，使用自己熟悉的术语对应用程序进行分组。

3. **创建策略：**随后，操作人员可创建精细的安全策略，根据实际观察到的流量来决定允许哪些应用程序彼此通信。针对常见应用场景的预构建策略模板进一步简化了流程。现在，无论应用程序和工作流处于环境中的何处，都能有效地相互隔离。

基于软件的分段的部署速度可达到传统防火墙的 10 倍乃至 20 倍，所需人员更少，而且几乎不会出现停机或中断。此外，一旦开始可视化和分段流程，您就可以轻松地基于标签进一步划分网络，或是添加不同的策略，同时实现流程自动化、处理安全事件，并根据业务或监管要求迅速做出更改。

分布式防火墙的优势


驻留在具有 L7 内容
的工作负载级别上
可在任何位置部署
（裸机、虚拟机、
云、容器等）
从第一个跃点到最后
一个跃点的安全性
（不存在网络防火墙
那样的瓶颈点）
非常适合控制
东西向流量
能跟随工作负载
移动的动态安全性
无需管理设备硬件
（安全即服务）
安全与网络基础
架构分离

案例研究：大型食品加工商通过分段节省 85% 的成本

美国一家大型猪肉产品加工商需要对部署在两个地点的 45 个应用程序进行分段，平均每个应用程序涉及到 5 台服务器。该公司的目标是消除扁平网络，将服务中断降至最低，并尽快实施相关策略。

在评估多种备选方案后，该公司选择了 Akamai 基于软件的分段解决方案。实施速度和简易性固然是决定性因素，但分析表明，与使用领先防火墙供应商的 VLAN 相比，这种方案在三年期内可省下 90 多万美元（相当于 85% 的成本节约）。具体如下：

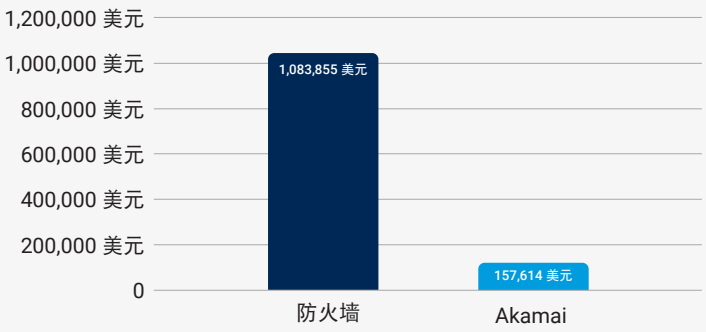
- Akamai Guardicore Segmentation 的许可费用比实施 VLAN 防火墙的硬件成本低 55%。
- 与持续时间更长的 VLAN 项目相比，Akamai 的人工成本（假设为每周 2,000 美元）整整低了 93%。

此外，Akamai 还满足了客户对快速策略实施的需求，在短短六周内就为 45 个应用程序实现了安全保护，而且没有造成中断。

防火墙总拥有成本*
1,083,855 美元

Akamai TCO*
157,614 美元
-926,241 美元

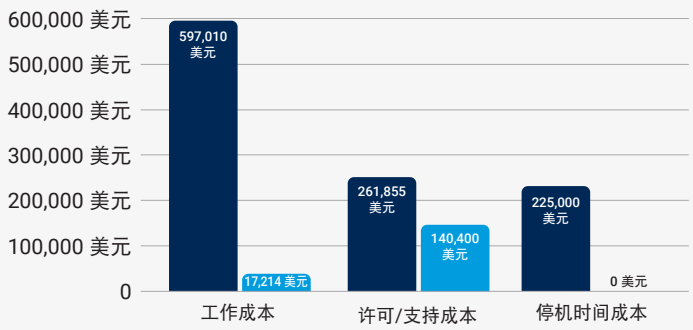
*3 年期成本



Akamai 工作成本*
17,214 美元
-579,796 美元

Akamai 许可/支持成本*
140,400 美元
-121,455 美元

Akamai 停机时间成本*
0 美元
-255,000 美元



这一切的意义

相较于传统防火墙方法，基于软件的分段技术有三大优势：

更有效地降低风险：基于软件的分段技术可在十分精细的层面上快速进行应用程序分段，从而大大减少攻击面。Zero Trust 原则要求对尝试访问网络资产的任何用户、设备或应用程序进行严格的身份验证，基于软件的分段技术运用这一原则，可以防止威胁在数据中心或网络环境中的横向移动。这进一步降低了数据泄露的影响，即便攻击者成功突破外围防御，也无法接管任何流程。它还能让企业更迅速地实现合规性，根据法规要求将关键、敏感应用程序与一般网络流量清晰隔离。

快速改善安全态势：简而言之，基于软件的分段能帮您更安全、更迅速地支持安全团队跟上敏捷 DevOps 应用程序的部署步调，并确保生产环境中的每个应用程序都得到适当的保护。这也意味着，分段项目长期占用的资源（技术或人力资源）更少。团队可以将时间集中投入到其他重要项目之中。

大幅降低总体拥有成本：这是真正影响利润的因素，从业务角度来看，或许也是最重要的优势。相较于购买防火墙设备和额外的硬件，基于软件的分段解决方案仅需软件解决方案即可实现，资本开支 (CapEx) 要低得多。随着时间的推移，它还能节省持续维护和管理所需的人力和资源，从而大大降低运营开支 (OpEx)。

仅根据这些指标计算，在 10 个应用程序分段的情景中并排比较基于软件的分段解决方案与防火墙解决方案时，Akamai 方法就有可能实现 85% 的总体节约，总额接近 100 万美元。

当然，尽管从部署的第一周起就能看到可衡量的节省，但总体拥有成本 (TCO) 的含义不仅限于前期采购成本或持续的自付成本。虽然从价格来看，优势可能并不明显，但基于软件的分段几乎杜绝了停机时间和服务中断，节省了大量相关成本。此外，企业还可避免数据泄露造成的经济损失，以及因不合规而受到的处罚。这些解决方案还能帮助企业显著降低遭遇入侵后信誉下降、业务流失的风险。原本被防火墙变更管理占用的 IT 团队和资源可以重新调遣，投入到更有成效的项目之中。对选择基于软件的分段解决方案的企业来说，所有这些成本因素都有助于降低总体拥有成本，并带来更高的利润。

案例研究：面临合规制裁的大型全球银行改为采用 Akamai Guardicore Segmentation

在审计期间，某大型欧洲金融机构发现其扁平式网络存在安全风险，面对大量要求更严格分段的新法规，该机构启动了一个使用 VLAN 和防火墙规则的分段项目。该项目耗费了大量时间，需要多个利益相关者和团队参与其中，造成了生产系统停机，制定的策略也模糊不清。结果，除了投入高额的实施成本外，该银行还因不合规缴付了罚款。

其 IT 团队很快就找到了替代解决方案，Akamai 在安全运营方面的自动化水平打动了他们。该银行在多个地区和多种类型的 IT 基础架构中部署了 Akamai Guardicore Segmentation。整个项目用时不到三个月，速度达到最初根据传统分段方法预计的 10 倍。该银行不仅改善了安全态势，还满足了 10,000 多项资产的合规要求。快速部署让他们得以更快降低风险，同时显著节约了成本和内部资源。

结论：汇而总之

防火墙并没有被淘汰。在确保网络边界安全方面，它们仍有自己的一席之地。但在当今的动态环境中，“边界”已成为一个难以明确界定的概念。为了在安全性与敏捷性之间实现必要的平衡，企业不仅要能够在 L4 网络级别上保护数字资产，还要能够在 L7 应用级别上保护数字资产，也就是要保护各进程的安全。防火墙不仅不适合这些用途，甚至还妨碍了进步。尝试使用防火墙进行精细分段要耗费大量资源，包括人力、技术和财力。

相较于防火墙，基于软件的分段已经证明能够显著降低安全风险、加快整体价值实现进程，其总体拥有成本 (TCO) 也显著低于传统方法，因此能更快地实现更高的 ROI。此外，这并非未来愿景—基于软件的分段解决方案已经实现，各行各业的企业都在从中受益。

IT 发展研究

科技的发展史就是一部不断改进、不断简化、不断降低成本的历史。分段技术也不例外。

以存储为例，在不到二十年的时间里，存储技术就从软盘发展到闪存驱动器，然后发展到网络连接存储 (NAS)，最终发展到如今的云存储。再以计算运行时环境为例，它从服务器发展到虚拟机、云计算、容器，最终发展到如今的无服务器计算。其中每一项技术发展的关键驱动因素都是降低成本、提高灵活性。当然，这背后也少不了技术飞速发展的支持。

分段技术也有着相似的发展演变历程，它从物理防火墙设备，发展到从网络中抽象出来的基于软件的分布式防火墙。背后的动力也是相同的：降低成本、提高灵活性（能转化为更快的部署），同时通过支持 Zero Trust 的更精细方法稳步提高安全策略的有效性。

网络和安全团队采用新型分段保护模式的时机已经成熟，就像在其他技术领域中一样—用于分段的物理防火墙就如同当初的软盘一般，正走向没落。

想了解我们的解决方案的实际应用?
立即申请演示：akamai.com/guardicore