Akamai

白皮书

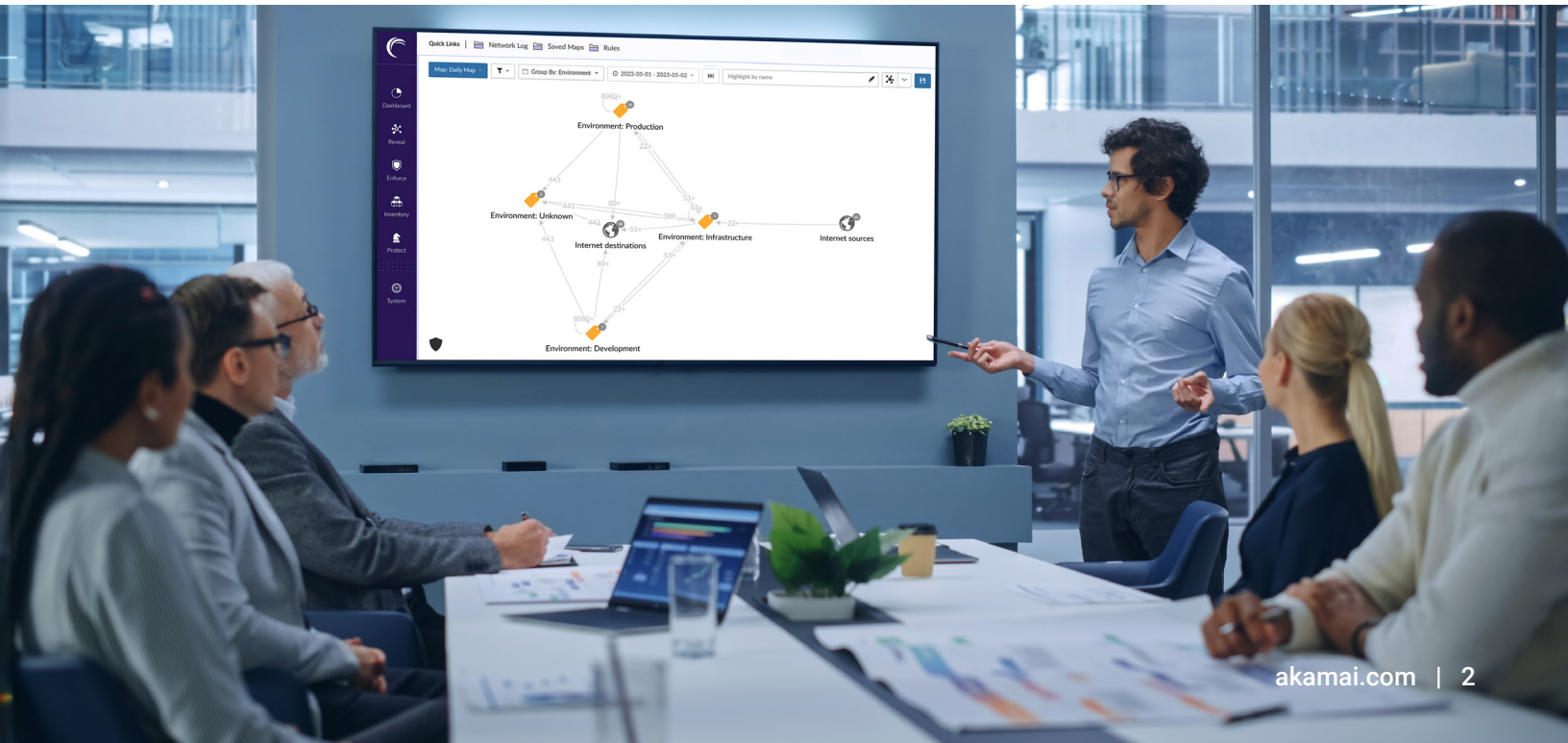
面向数据中心运营商的软件定义分段技术

对于多租户数据中心的运营商来说，对计算环境进行分段极其重要，已经成为其运营模式的基础。首先，他们需要将自己的基础架构与其客户的环境分开，并在共享特定资源的同时阻止访问其他资源。其次，他们需要避免客户各自的环境之间出现意外或恶意的“交叉污染”。这包括阻止成功的入侵事件或恶意软件感染从一个客户环境传播到另一个环境。最后，在所拥有的运营应用程序中，需要实施有效隔离以限制潜在入侵带来的影响。通过更深入地了解数据中心提供商的运营网络，发现存在三种情景。在这三种情景中，如果能高效实现分段，可以显著改善安全态势并降低成本。

1. 从企业网络（提供商的内部系统，包括计费系统）和客户网络中**分离运营网络**（DCIM、BMS 等）

2. **降低运营网络内发生横向移动的风险**，该网络中有很多难以修补的系统，如不进行合理分段，将会带来风险

3. **在面向客户的网络之间创建高效的安全连接**——例如客户门户所在的 DMZ，该区域需要安全地访问运营网络中的数据（例如，读取电源状态）和企业网络中的数据（读取计费信息）



现在，这些场景都是通过非常复杂、实施缓慢且低效的网络架构、VLAN、临时网络等进行处理。如果能够实施软件定义的解决方案，而不依赖任何复杂网络配置，不仅可以显著降低成本，还能对连接进行更严格、更稳健的控制。

此外，客户难以在其应用程序（托管或本地）中实施并保持有效的分段。这为数据中心运营商带来了一个重要的机会，让他们能够利用自己的内部分段专业知识、工具和运营模式为客户提供托管服务，并且能够围绕分段实践创造极具吸引力的收入来源。而且，运营商还能够通过正确的方法、工具和流程将安全策略扩展到客户本地环境，从而能够访问并监测非托管应用程序，这有助于更快地安全迁移到托管数据中心，推动核心业务实现增长。

Equifax：最坏的情况

如果您想知道在环境分段较差、无效或没有环境分段的情况下“可能出现的最坏后果”，那么广为人知的 2017 年 Equifax 数据泄露事件就是典型的历史教训。此次事件导致 1.43 亿美国人高度敏感的个人信息遭到泄露。美国政府审计办公室 (GAO) 的调查显示，攻击者最初利用 Apache Struts Web 框架中名为 CVE 2017-5638 的漏洞入侵了这个征信机构巨头的客户纠纷解决门户。入侵成功后，攻击者在这家公司的系统中几乎畅通无阻地游荡了 76 天。GAO 报告将此次自由横向移动归因于缺少分段，导致攻击者能够轻松、随意地访问数据库——这几乎是一个无限大的攻击面。

问题是如何以更有效、更高效且更经济的方式实现这种分段。运营商过去依赖传统防火墙或 VLAN 来分隔多租户或多用户架构内的环境。但是，实施和维持此类措施通常都非常困难，不仅需要大量人工操作，而且非常耗时且成本高昂。再者，这些技术绝非无懈可击，可能会暴露出非常大的攻击面。针对外围防御设计的解决方案在数据中心环境内会出现显著的功效问题，因为大多数此类环境都包含各种虚拟机、虚拟机管理程序、容器甚至云组件，并且工作负载会根据情况不断地自动启动和关闭。还有一点也非常重要，利用 VLAN 进行分段需要应用程序停机，对于至关重要的运营控制措施来说，这可能是一票否决的问题。

出于所有这些原因，共享环境运营商都在深入了解现代的软件定义分段技术，包括微分段技术。微分段技术取得了很大的进步，使它成为所有类型的公司都可以实行的选项，并且可能是实现 Zero Trust 安全模式的理想选择。同样重要的是，借助正确的工具和较为周密的计划，微分段实施起来比上述方法更快、更轻松，并且更易于管理和维护。实际上，近期的测试表明，与传统防火墙实施相比，微分段可以将部署时间缩短多达 30 倍。另外，还有一个至关重要的好处是：利用软件定义的分段时，不需要进行任何网络更改，也不需要应用程序停机。由于节省了时间并提高了效率，因此显著降低了整个部署生命周期中的成本。

传统方法的潜在问题

要想了解软件定义的分段或微分段的优势，比较有用的办法是列出本地和云端采用的标准技术的一些缺点和局限性，然后进行对比。这可能包括物理或虚拟防火墙以及网络配置的某种组合，例如 VLAN。通常，这些方法都是资源密集型和劳动密集型方法。创建安全策略是一个非常麻烦的过程。必须手动执行添加和修改，这样不但会拖累现有运行效率，还会增加出现漏洞的风险。

尤其是内部防火墙的获取成本很高，而且设置起来非常复杂。它们还会干扰正常流量，进而改变模式并产生最终会阻碍系统性能的迂回流量。随着行业不断地深入研究，大家发现防火墙并不适用于数据中心内的分段，还有一些提供商甚至认为防火墙并不属于数据中心的一部分。

在尝试向正在运行的现有生产环境中引入分段时，最困难的挑战之一是使用传统方法需要应用程序停机。停机的代价高昂。它只能在特定时间窗口内发生，而这样的窗口期往往根本不存在。

另外一项值得注意的挑战是，创建任何内部分段都需要熟悉东西向应用程序依赖关系。这种深入了解通常是不存在的。如果没有能够绘制应用程序依赖关系图的简单方法，那么分隔待利用环境不仅困难重重，而且风险很大。

为什么软件定义的分段更为有效

高效运营、更强大的安全态势：软件定义的分段可以解决传统技术的固有低效问题，并且可能更为重要的是，它能够增强多用户环境的安全性。顾名思义，软件定义的分段采用了网络分段的概念，在实施的时候无需进行任何基础架构更改。它需要围绕单个应用程序或按逻辑分组的应用程序创建安全策略，而不必考虑这些应用程序驻留在混合数据中心内的什么位置。这些策略规定了哪些应用程序可以相互通信，哪些应用程序不能，真正实现 Zero Trust。

无需手动更改，也无需停机：软件定义的分段不需要进行任何网络更改或创建任何 VLAN，这将节省大量运营成本。此外，由于无需迁移到新 VLAN，因此它不需要任何应用程序停机或更改。这一点非常重要。对于停机成本高昂或不可能停机的很多应用程序来说，这是提供这项关键安全措施的唯一方法。

广泛的监测：此外，高级的软件定义分段解决方案专门用来解决东西向流量分段难题，它提供了一个集成监测工具，可以帮助确定分段边界以及应用程序之间的依赖关系。这不仅提高了流程效率，而且消除了创建策略时的操作错误。

策略和控制自动化：软件定义的分段也使得以动态方式应用策略成为可能，因此随着工作负载的启动或关闭，它们也可以自动归因于正确的策略。这样就无需手动移动、添加或更改策略，因此节省了大量资源。

基础架构无关：软件定义的分段有一个关键优势，即它与基础架构无关。它可以跨任何基础架构提供监测能力和分段，包括裸机、虚拟机、PaaS、云、容器等。借助单一管理平台和单一工作流程即可管理所有基础架构。这样大大提升了操作的自由度，不仅能够实现安全标准，对底层基础架构的选择也不会形成任何约束。

更多收入，更密切的关系：最重要的一点是，它为数据中心运营商带来了重要的机会。在管理和提供内部分段时，他们可以利用培训、工具和流程向客户提供急需的托管服务，在同一工具和同一管理平台中既可以管理托管应用程序的分段，也可以管理客户本地环境中或云端的应用程序的分段。这不仅可以带来额外的潜在收入，而且会形成客户对运营商更强的依赖性，进而建立更长久的关系并获得更高的收入。

为什么选择 Akamai

为了实现这些优势，软件定义分段解决方案必须满足一些必要条件。它必须具备深度的进程级监测能力以监测计算环境中运行的所有应用程序，还必须能够绘制这些应用程序之间的所有数据流。为了进行高效部署和管理，还必须能够灵活地为资产正确添加标签以完成策略创建，并在工作负载规模自动伸缩时自动修改标签。而且，解决方案需要与平台和基础架构无关。策略必须能够适合相应的应用程序，并且在多个环境中一致地执行。最后，解决方案应允许采用自动且简化的操作模式，以便进行策略创建、管理和实施。

毫无疑问，Akamai Guardicore Segmentation 符合所有上述条件。软件定义的分段是我们的核心功能。此解决方案提供了卓越的图形可视化功能，用户可以查看环境中的各种资产以及它们之间的依赖关系，包括裸机、虚拟机、公有云、容器以及物联网设备。这种深度监测能力显著加快了围绕应用程序微分段进行安全策略确定、分组和创建的过程。

如需了解更多信息，请访问 akamai.com/guardicore。

无论您在何处构建内容，以及将它们分发到何处，Akamai 都能在您创建的一切内容和体验中融入安全屏障，从而保护您的客户体验、员工、系统和数据。我们的平台能够监测全球威胁，这使得我们可以灵活调整和增强您的安全格局，让您可以实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，进而信心十足地持续创新、发展和转型。如需详细了解 Akamai 的安全、计算及交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2023 年 6 月。

扫码关注，获取最新CDN前沿资讯