Akamai

白皮书

现代企业环境中的网络分段和微分段

概述

为安全性的目的实施分段并不是什么新鲜理念。在传统上，大多数公司都使用外围防火墙以及 VLAN 和 ACL，以此实现 IT 基础架构的分段和保护。然而，时过境迁。容器化、软件定义网络、公有云和多云基础架构的使用日渐普及，接入互联网的设备不断扩增，这带来了一系列新的安全问题。要想解决这些问题，需要一种专为有着不同安全要求的异构 IT 环境而构建的解决方案。此外，对于当今的任何企业来说，勒索软件以及与民族主义和国家主义有关联的攻击者都是不容忽视的风险。攻击者的狡诈程度日渐增加，企业监测 IT 环境的难度也与日俱增。无论是传统外围安全措施，还是基于深度数据包检测或签名检测的下一代防火墙，都难以应对当今企业数据中心的庞大流量。本文将审视适当的微分段技术如何弥补其他替代网络分段方法的不足，从而成为企业的理想之选。

混合云环境已成为标准，它们有着一系列传统边界安全措施无法满足的特殊要求

传统防火墙无法满足东西向流量的需求

在实施 IT 环境分段时，企业最先考虑的可能就是传统边界安全设备。遗憾的是，这些设备在构建时的目的是监控南北向流量，即从客户端到服务器的流量。这包括从任何外部来源传入数据中心的流量。近年来，数据中心内部的服务器间流量（通常称为东西向流量）呈指数级增长。这在很大程度上源自虚拟化和融合基础架构（如虚拟机管理程序、VPC 和基于容器的计算）的发展。

传统防火墙等边界安全措施无法帮助企业抵御受感染设备的侵害，也无法阻止攻击者利用东西向流量来扩大其立足点。随着 TLS 加密的兴起，以及利用“捎带”攻击技术，借开放的合法应用程序端口轻松隐藏恶意流量的能力，许多攻击都能长驱直入，即便有防火墙也不例外。这造成您无法发现现有入侵，也无法解决或转移攻击。这也意味着您无法轻易限制攻击者在您网络中停留的时长。停留时间越长，入侵造成的后果就越严重。Sophos 发布的《2022 年度活跃攻击者手册》(Active Adversary Playbook 2022) 发现，平均停留时间的中位数为 15 天，但在小型企业和特定行业中，平均停留时间要长得多，最长可达到 34 天。[1]攻击者在企业网络中潜藏的时间越久，能造成的破坏就越严重。

企业无法设置足够的虚拟防火墙来保护数以千计的应用程序或工作负载。即便可以创建虚拟化解决方案，考虑到当今工作环境不断变化的动态，其管理或控制也是不可能完成的任务。在涉及到混合云时，使用传统防火墙的难度更大，因为它们需要在多种不同的环境中工作，跟踪多种不同云环境中的工作负载，还要通过单独一个点加以控制。为了尝试解决这些问题，业界推出了数种网络分段方法。

可以考虑的三种分段方法

在认识到防火墙（即使是虚拟化防火墙）不足以保护混合云数据中心后，企业希望通过三种基本方式在东西向基础架构内应用分段。如前所述，如果不具备强大的分段策略和安全措施，端口或服务器彼此之间的通信几乎不受约束。这意味着，如果服务器防火墙被攻破，攻击者可以轻松转移到网络中任意数量的其他服务器。要制约服务器之间的连接，最有效的方法就是网络分段。网络分段有三种基本类型，其中微分段技术可支持企业执行更加精细的策略和控制措施。用户可以结合使用下列三种分段策略，为关键或存在风险的应用程序构建更精细的策略。

环境分段

这种方法将不同的环境彼此隔离开来。比如，企业可以通过这种方式将开发环境与生产环境彼此分隔。对于任何分段策略来说，这都是至关重要的第一步，完成这一步后才是创建更精细的策略。

应用程序分段

用“围栏”隔离高价值应用程序则让分段更进一步，将每一个特定关键应用程序与网络的其他部分隔离开来。优秀的微分段解决方案甚至可以在进程层级上控制这种隔离。

层级分段

最严格的分段形式是应用程序内部分段。此时您可以创建策略，规定如何管理同一应用程序集群中各层级之间的通信，例如控制 Web 服务器、应用程序服务器与数据库服务器之间的流量。还有一种选择是在进程级别上执行此类控制。

网络分段方法——通过 VLAN 进行网络分段

大多数公司最初都是利用 VLAN 实现分段。这些虚拟局域网允许企业利用防火墙或路由器本身的访问控制列表 (ACL)，为每个分段制定其自己的通信路径。VLAN 是一种常用的网络分段方案，但如果深入探究，就会发现它存在不少问题。VLAN 无法满足当今的安全需求，下面我们来进一步探索其原因。

有许多企业选择 VLAN 作为分段方法，原因并不难理解。这种方法可以利用现有架构实现，让人感觉成本低廉、部署轻松。但这种分段方法极其僵硬和复杂，维护成本可能相当高，而且在实施时需要停机。

若要使用 VLAN，您首先需要先熟悉每个分段中的服务器和依赖关系，然后为要分段的一台或多台网络交换机创建必要配置。这项任务由网络工程师负责完成，而且往往涉及多个地点，因此可能耗时多天，需要付出的时间和资金都过于高昂。在配置期间，流量可能会中断或减速。

在敏捷性成为主要竞争优势乃至必备能力的时代，高昂的变革成本和缓慢的变革速度只会给企业的利益造成灾难性影响。福布斯认为，适应力是生存的关键：“技术颠覆不是新鲜事儿，但当今颠覆的速度、复杂性和全球化性质前所未有。...能够生存下来的不是规模最大或财务状况更稳定的企业，而是在呈指数级加速的变革中迅速适应环境的企业”。[2]

VLAN 在诞生之初并未考虑分段，认识到这一点非常重要。它们的初衷是减少网络拥塞，用它们来控制通信并非利用现有技术的明智方式，从很多角度来说，都可以说是误用。有鉴于此，使用 VLAN 实施分段会面临诸多限制也不该令人意外。

- **云技术**——VLAN 和其他传统网络分段策略无法扩展到云。如果您使用内部分段式防火墙 (ISFW) 或 ACL 来控制可以访问网络分段的用户，那么很可能需要在云环境中依靠 SDN（软件定义的网络）。这通常是通过使用虚拟化防火墙或子网的第三方软件提供商实现的。
- **容器**——考虑到容器在 IT 环境中的广泛采用，安全性仍然是重大问题。由于每个容器都在同一个内核上运行，一旦发生漏洞利用攻击，所有容器都可能面临风险。隔离历来都是难题，无法通过常用的网络分段方法解决。
- **协议限制**——VLAN 有 4,096 个分段的上限，这制约了在大型数据中心中提供足够多的分段的能力。更精细的分段方法不存在这种限制。

从网络分段到应用程序分段——引入第 4 层控制措施

通过在云环境中使用安全组、在本地虚拟化环境中使用基于虚拟机管理程序的防火墙实现应用程序分段，上述许多问题都得到了改善。传统应用程序分段可实施第 4 层控制措施，让您能够将服务层级彼此隔离开来，为应用程序划定安全边界。每个层级都只能获得其提供完整功能所需的访问权限级别，不能获得更高的权限。一个应用程序的层级之间有明确隔离，将潜在入侵威胁控制在最低限度。

我们想想一家标准企业中可能存在的层级——从负载均衡器、数据库，到位于您自有 DMZ 内部/外部的应用程序服务器。通过将这些层级隔离开来，就能确保每个层级都有自己的安全规则和功能。应用程序分段允许合理控制各个层级、限制其敏感信息和通信，同时在必要时允许广泛的用户访问，从而为企业提供支持。例如，企业可以全面阻止某些数据库与互联网通信，还能确保即便攻击者攻破了简单的负载均衡器，也不能访问数据库层级上更加敏感的信息。

随着解决方案的精细程度进一步提高，企业可通过应用程序分段将整个应用程序集群与企业的其他领域隔离开来。如前所述，这可以减小攻击面，降低攻击者从一个层级横向移动到另一个层级的能力。

第 4 层控制措施的限制

传统应用程序分段可能缺乏纵深度，这会直接影响监测能力。在路由时，网络层负责在系统间移动数据、分配 IP 地址和协议，具体规定数据分段到达目的地的路径。应用程序分段通常使用第 4 层网络控制措施，关注数据本身的传输方式。较大的数据段会分割成更小的数据段或数据块，并且可在目的地重新组合起来。流量控制可以根据发送或接收信息的设备的需要，动态地加快或减慢这一过程。

在当今威胁环境中，对这些层级的控制非常关键，但在某些情况下，您可能希望能够在更精细的水平上设置策略。攻击者已经展示了他们伪装 IP 地址的能力，并在允许的端口上利用“捎带”攻击技术来入侵网络。此外，第 4 层保护并不限制应用程序或层级内部的横向移动，所以给您留下的攻击面仍可能超出预期。

需要比第 4 层更精细的控制的绝佳示例之一就是合规性计划。在一定程度上来说，传统应用程序分段技术可使公司能够满足某些特定合规性规定，例如按照 PCI-DSS 规定将 CDE 分离开来，或按照 HIPAA 规定保护 PHI。虽然第 4 层技术在过去被视为展现合规性的有效手段，但事实已经证明，它可能还不够。根据《Verizon 2022 年度支付安全报告》(Verizon 2022 Payment Security Report)，只有 43% 的公司“完全合规”。[3] 更糟糕的是，即便 100% 合规，也不代表着 100% 安全。尽管第 4 层控制措施在合规性方面或许对您有所帮助，但它们缩小攻击面的程度有限，无法在安全角度上产生有意义的影响。这就是事实。攻击者可以利用两个层级之间开放的第 4 层端口和单独的进程（第 7 层），获得他们想要的一切。

黑暗中的分段——网络和应用程序分段缺乏可见性

企业已经发现，应用程序分段无疑是朝着正确方向迈出的一步，但还不足以解决粗略分段方法的全部固有问题。另一个仍需应对的挑战是可见性。在分段过程的每一个阶段，都必须能够精准、实时地查看网络概况，而许多分段方法在这方面都存在局限性。

在开始之前，您需要直观显示应用程序的依赖关系，以便制定准确的策略规则。在实施分段后，您需要证明分段按预期发挥作用，这不仅是为了确认安全态势足够强大，也是为了在必要时证明自身的合规性。

如果不具备实时和历史信息可见性，就无法获得您自己或第三方利益相关者和监管机构需要的证据。手动收集这些证据需要耗费时间和资金，而且还有可能存在配置错误和失误的问题。如果一种分段解决方案无法提供这种可见性，就算不上够格。

扩展至第 7 层（应用层）的微分段

相比之下，在应用层（第 7 层）上进行分段可以十分有效地限制横向移动，即使在应用集群内也不例外。第 7 层是网络服务与操作系统集成的一层。HTTP、FTP、TFTP 和 SMTP 等协议都属于第 7 层协议。相较于其他解决方案相比，微分段技术的最新进步支持在这一层实施更深入的分段，支持您的企业监测和控制第 7 层及传统第 4 层的活动。这就意味着，在配置策略时，企业可以使用特定的进程和流量，而不必依赖 IP 地址和端口。这能让分段的好处不仅限于特定层级，甚至不限于特定应用程序集群。它也让您可以发现潜在威胁，包括哈希值错误这样的细节，甚至是攻击者对授权进程或路径实施镜像的情况。

在策略创建方面，通过对第 7 层进行分段，您就能制定高度具体化的允许列表规则或例外项，仅允许确切的进程或流量，默认阻止所有其他通信。这可以在系统之间执行数据隔离，但仍允许必要或业务关键型数据流的通信。

理想的微分段解决方案具备帮助企业提高敏捷性所需的可见性

在整体化的微分段解决方案中，每个工作负载（无论是基于虚拟机管理程序，还是基于 VPC、容器、裸机服务器，甚至是物联网/OT 系统）都有代理，可为企业提供整个 IT 基础架构的完整可视化信息图。真正的智能解决方案包括数据中心、云、多云和混合云环境以及远程设备。传统的应用程序分段解决方案很难获得这种整体化视图，原因往往在于它们使用的是以网络为中心的技术组合。

通过全面的环境可视化信息图，您还能实时看到已经具备并在执行哪些安全策略。您的工程师和安全专业人员应该能一目了然地看到策略范围内存在哪些有待填补的潜在漏洞，或者他们需要实施或从头创建哪些额外的策略。

凭借这样的可见性，在新软件或现有系统的更新尚未准备就绪时，您的企业还可以提前创建规则，对全新或更新的应用程序进行分段。在更新上线后，您的安全团队就能获得所需的实时信息，以便检测和解决异常的应用程序活动，确保不会有遗漏或转变为有效漏洞的安全风险。在发生事件后，您的企业可以利用有上下文的工具，将事件与历史数据进行比较，并了解导致异常情况发生的确切环境。您可以收紧策略、调整分段，还可以详细说明事件，以支持合规性工作，或开展进一步研究。

采用 Zero Trust 模式

微分段的另外一项附加优势是它能采用 Zero Trust 安全模式。Zero Trust 是 Forrester 早在 2010 年提出的概念，但微分段等技术正在帮助这一概念化为现实，研究人员和安全专家也在坚持不懈地广泛宣传这种模式的好处。[4]

其思路非常简单：就是不信任任何流量或用户，无论其来源是外部还是内部，在每一次连接尝试时，都要经过证明和许可。强大、精细的微分段策略全面支持 Forrester 提出的 Zero Trust[5] 三大原则：

- 默认不信任任何实体
- 实施全面的安全监控
- 强制实施最小访问权限

Zero Trust 与纯边界安全机制迥然相异，后者指的是使用很深的护城河保护城堡入口，并假设城堡内的人都可以安全进入。由于大多数公司都不再拥有封闭的网络或数据中心，“城堡”的概念已经过时，只有 Zero Trust 这样的最小权限策略，才能确保您随时了解和控制内部人员。

利用微分段确保您的企业未来无忧

网络分段无疑超越了边界安全，环境分段和第 4 层及以下应用程序分段是构建分段策略的重要步骤。但随着 IT 环境日趋复杂化，您可能会发现，您需要的解决方案应能通过层级分段实现更高的精细度，并在应用程序和层级阶段实现直至第 7 层的进程级执行，

现代企业基础架构已不再是各自为营。它们通常依靠云端 SDN、容器或裸机虚拟机管理程序等技术。它们跨越不同地理位置和实体数据中心发挥作用。

为了抵御外部和内部威胁，唯一可行之道就是采用这样一种解决方案：它能检查和控制所有流量（包括东西向和南北向），并且对于关键或高风险的应用程序，它能为您提供比仅凭第 4 层方法更高的可见性。通过在应用程序或层级的级别上实施直至第 7 层的微分段，您就能准确了解整个 IT 环境，并轻松创建和执行符合 Zero Trust 模式的精细安全策略。优秀的微分段解决方案不会要求您在安全性与敏捷性之间做出选择，因此合理做出选择能让您在全企业范围内实现更好的整体安全态势。

请访问 akamai.com/guardicore 以了解更多信息。

1 Shier, John。2022 年。《2022 年度活跃攻击者手册》(The Active Adversary Playbook 2022)。Sophos。6 月 7 日

2 Gonda, Rob。2018 年。《适应能力已成为数字达尔文主义时代的生存关键》(Adaptability Is Key To Survival In The Age Of Digital Darwinism)。福布斯5 月 24 日。

3 https://www.verizon.com/business/reports/payment-security-report/

4 Holmes, David。2022 年 6 月。《Zero Trust 微分段最佳实践》(Best Practices For Zero Trust Microsegmentation)。Forrester。4 月

5 Holmes, David 和 Jess Burn。2022 年 1 月。《现代 Zero Trust 的定义》(The Definition Of Modern Zero Trust)。Forrester。4 月

Akamai 可在您创建的一切内容和体验中融入安全性——无论您在何处进行构建，将其分发到何处，从而保护您的客户体验、员工、系统和数据。我们的平台具备监测全球威胁的能力，这让我们得以帮您调整并增强安全状况，从而实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，让您信心十足地不断创新、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 5 月。