基于软件的分段

利用由内而外的方法提升对安全性的信心

目录

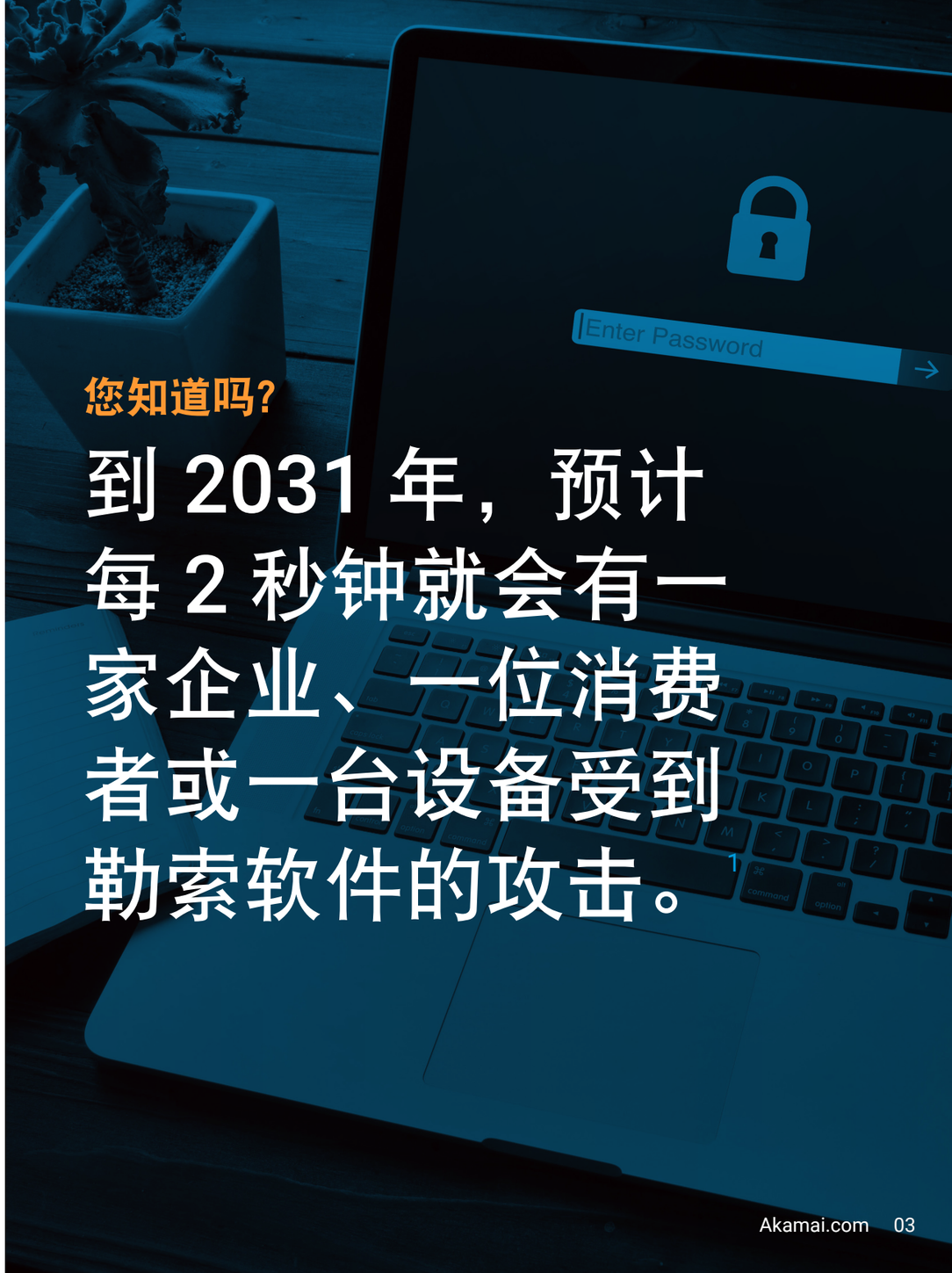
传统防火墙的没落

我们明白。您已经厌倦了您那老旧的本地防火墙。IT 环境和安全要求飞速发展变化，这些传统防火墙的功能已经远远无法满足当下的需求。而且，网络安全形势也在不断变化：攻击方法变得更加复杂，网络犯罪分子的数量也远超过以往。已有几十年历史的陈旧设备架构根本无法抵御最新的恶意软件、僵尸网络攻击、网络钓鱼方案、社会工程和数据勒索。

但是，即便传统防火墙有着无数问题（昂贵、无法移动、缺乏监测能力，等等），我们仍然必须承认一个现实：这些防火墙不会很快淘汰。它们在外围防御层发挥着重要作用（负责处理南北向流量），并为企业提供坚实的保护层。

但防火墙无法管理本地数据中心和云环境内的东西向流量。

基于软件的分段才能处理这项任务。



您知道吗？

到 2031 年，预计每 2 秒钟就会有一家企业、一位消费者或一台设备受到勒索软件的攻击。[1]

成功解决！

传统防火墙存在的 3 个问题

1. 存在的问题：缺乏可见性

   由于无法监测数据流动，企业很难实施和维护规则。因此，防火墙往往具有极其冗长的规则集，而且其中许多规则过度宽松，甚至根本没有存在的必要性。

解决方案

寻找具备如下特点的解决方案：将可视化地图、资产分类和应用程序依赖关系映射与策略创建和管理功能集成到一起。

成功解决！

传统防火墙存在的 3 个问题

2. 存在的问题：防火墙难以维护

很少有应用程序所有者和防火墙管理员知晓需要通信的相应 IP 端口和协议。因此，防火墙管理变成了一个反复迭代的故障排查过程。

解决方案

与其围绕固定的网络“管道”（比如 IP 和端口）制定策略，不如让策略基于有意义的属性，例如应用程序使用的进程、完全限定域名 (FQDN) 和用户身份。这样一来，属性将保持不变，而您的策略也将继续生效，即使您对数据中心做出了变更或将工作负载转移到了云端，也是如此。

成功解决！

传统防火墙存在的 3 个问题

3. 存在的问题：防火墙缺乏敏捷性

通常情况下，无论您要对防火墙做出任何变更，都需要安排停机。当应用程序所有者需要做出变更时，他们可能要等待一周或更长时间，以便在维护窗口期内审查和实施变更。

解决方案

现代 IT 企业已经不再采用变更窗口期的模式，而是改为采用 DevOps 模式，在这种模式下，应用程序的上线和更新将保持连续。找到具备如下特点的技术解决方案：可以使用您用于应用程序本身的相同 DevOps 工具来为该解决方案实现自动化。这样一来，随着应用程序的不断演变，实施的安全方法也能够相应调整。

随时随地提供保护

我们来谈谈传统的防火墙管理策略。那种策略十分复杂，也不具备灵活适应能力。用于管理传统防火墙的老式方法基于位置执行分段，而用户无法轻松更改该位置。这个位置往往基于一个硬编码的 IP 地址，或者路由到某个数据中心。这意味着，您必须以物理方式将想要保护的内容移到防火墙后面，此过程的宗旨就是规避风险，但会耗费大量资源，而且十分缓慢。云迁移？监测能力？足够的安全性？别想了。

把您的传统防火墙留在原地。做个深呼吸，迎接全新解决方案的到来。您可以轻松实施基于软件的分段，将其与您的现有防火墙配合运行，而且这种方案具有出色的适应能力。借助基于软件的分段，您可以对您的环境、数据中心和网络做出变更，并根据观测结果设置策略。工作负载和策略可以出现在任何地方：云端、数据中心，或者其他任何位置。此外，您可以应用和调整安全策略，而不需要对网络进行更改，且系统停机时间为零。

揭示您的内部网段

您会相信您无法亲眼看到的东西吗？答案一定是否定的。但是，当您在防火墙后建立安全策略时，恰恰就是在做这种傻事。您无法真正看到内部的情况。这就好比看着一栋大楼，而无法看到里面的人。

基于软件的分段依靠的不是几率。它可以对网段进行分段，使您完全了解您的工作负载涉及的所有活动。在您弄清楚环境内部的各种元素之后，即可制定一个计划，并根据具体应用场景将这些网段细分成有意义且有效的单元。

在企业边界之外仍能保障安全

传统防火墙无法适应变化。虽然防火墙在企业边界中发挥着重要作用（比如 DDoS 防护以及流量过滤和检查），但人们很难利用防火墙来实现网络内部的安全性。为什么？部署方式导致它们自然而然地成为阻塞点，也就是说，执行的每一次分段都会造成操作上的阻碍，例如，为了实施分段，企业需要更改和移除网络及应用程序。这很繁琐，也会耗费大量资源。

基于软件的分段可以帮助您突破这些操作上的难题，并能让您在端点和企业边界之外延续您的安全做法。首先，它采用了分布式防火墙方法（而不是阻塞点）。其次，它以工作负载为中心，这意味着，它可以从主机系统收集数据，然后将其应用于资产分类，还能为规则采用更精细的方法，比如进程级内容和策略。总体而言，基于软件的分段可通过适应性更强、更精细的方法来保护网络内的关键资产，相比防火墙而言，它需要企业投入的精力和资源更少。

分段的 4 个基础类型

分段比以往任何时候都重要。攻击面进一步扩大化。复杂的攻击（比如勒索软件）在入侵后会发生横向移动，您必须考虑企业边界之外的应用程序依赖关系。但分段不是一蹴而就的。

下面我们来看看四种常见的分段、它们之间的区别，以及您为什么需要它们：

1. 环境分段

将系统分隔在不同的开发环境中，比如开发环境、QA 环境、暂存环境和生产环境。这是一种广义分段，其最终目标是将系统分隔到不同的环境中，以确保只为必要的用户和应用程序提供访问权限。很多合规举措要求企业确保非生产系统无法访问生产系统。

2. 网络分段

是一种与架构有关的做法，可将网络分割成多个子网络，每个子网络都是一个规模更小的网段。网络分段为 IT 运营商提供了一个工具，以更好地控制网络流量、提高性能和改善安全性。

3. 微分段

是一种更精细的分段方式，用于将工作负载相互隔离并为它们分别提供保护。这种分段方式能够为进程、容器、用户、域名和设备等元素设置分段规则。这种方法在控制东西向流量和防止横向移动方面具有优势。

4. 基于身份的分段

不仅可以像微分段那样保护单个端点、设备、工作负载或容器，它还支持通过动态规则来评估身份（可以是用户、设备或上下文），进而判断是否允许通信。基于身份的分段策略可以基于精细的设置（不仅仅基于 IP 或端口），比如标记、操作系统类型或应用程序特征。

误区与真相：破解 5 个与分段有关的误区

误区 1

分段项目难度太大，需要的时间太长，因此难以完成。

真相：首先建立监测能力，并清楚了解您的环境内部现状，这能将完成分段项目所需的时间从数月缩短到数周乃至几天。现代分段技术也可以使用 AI 来进一步加快这个过程。

误区 2

要实施分段项目，需要更改网络基础架构和停机。

真相：基于软件的分段解除了安全功能与基础架构之间的关联，因此，分段项目可以单独开展，而不会影响到底层基础架构，不需要做出变更或停机。

误区 3

分段会阻止我的网络中的合法流量。

真相：通过监测您的环境，并使用基于软件的分段策略，您可以首先查看这些策略将对您的业务活动产生怎样的影响，然后实时执行策略。

误区 4

分段会阻碍用户正常访问，并带来不必要的延迟。

真相：通过使用基于软件的分布式分段策略，而非强制所有流量流经特定的防火墙阻塞点，即可消除网络瓶颈。能够感知应用程序和身份的更精确的策略可以减少无意中发生用户访问问题的风险。

误区 5

我没法在云端使用与本地环境相同的分段工具。

真相：如果您解除了分段策略与基础架构的关联，那么，在数据中心内使用的策略也可以在云端生效。

降低内部风险

攻击者总会伺机入侵。这些入侵会导致您的业务瘫痪、盗用您的数据、损害您的品牌，并造成数百万美元的损失。

仍然认为防火墙可以面面俱到？再好好想想。一旦攻击者入侵网络、环境或数据中心，它将利用横向移动来窃取数据并造成破坏，比如接管应用程序服务器或访问数据库服务器。

实际上，如今 70% 的攻击都会尝试进行横向移动。[2]

防火墙会将横向移动视为网络内部的合法流量，而基于软件的分段可以拦截这类流量。基于软件的分段是安全计划的重要组件，它可帮助您限制横向移动，即便您确实遭到了入侵，攻击者也更难在您的环境内部四处移动。这会给您带来十分宝贵的机会，您可以采取行动以保护数据和关键应用程序，缩短攻击停留时间，甚至可以检测到攻击者。这种方法的可扩展性更强，并且简单易用，使您可以在不更改网络或系统的情况下快速实施分段。

Zero Trust 并不复杂。

Zero Trust 的关键在于管理“谁对谁做什么”以及“他们采取的做法”。换句话说，明确控制“谁可以在您的网络内做什么”。

如果允许用户访问网络内的所有资产，那代表您给予了他们过多的信任，最终会将整个企业置于风险之中。首先，员工会经常犯错，这可能会导致严重的安全问题。有些人甚至心存恶意。

此外，除了 VPN 网络和设备以外，还有很多数据中心入口点需要您去考虑。例如，攻击者可以通过生产服务器（SolarWinds 数据泄露就属于这种情况）、易受攻击且面向互联网的应用程序或易受攻击的 VPN 以及其他途径进入网络。在这种情况下，您只是因为某台服务器位于网络内便对它给予信任，但实际上，这让攻击者可以访问任意内容，并且可以不受限制地进行横向移动。

要在您的生产网络中实现 Zero Trust，您必须阻止所有未被明确允许的活动。

传统防火墙根本无法精细地完成这项任务，因为这需要在比 IP 地址和端口更深的层级识别各项属性。

不同于传统防火墙，基于软件的分段能让您详细了解正在发生的事情，并创建精准、具备身分识别能力且容易理解的策略。

您的 Zero Trust 检查清单：6 种实现明确控制的方法

简而言之：信任应基于网段的规模，要保护关键数据、资产和应用程序，网段越小越好。以下是实现 Zero Trust 的六个步骤，操作起来一点都不复杂：

1 使用可视化标签来标识您的敏感数据。

2 使用自动流动和依赖关系映射来映射您的敏感数据流。

3 使用正确的工具来快速定义任意分段或微分段策略，以此来构建您的 Zero Trust 微边界。

4 借助实时监测和分析，持续监测您的 Zero Trust 生态系统。

5 通过 API 和技术集成，实现安全功能的自动化和编排。

6 部署相应的功能，支持不再信任某人或某物，这样一来，如果您遭受攻击，您就可以利用预设属性，取消对任何设备的信任，而不论其用户或网段如何。

结论

现在，您或许很想知道该如何淘汰掉传统解决方案，改善网络内部的安全态势。

好的。

把您的传统防火墙留在原地，它们可以很好地保护网络边界。但它们的作用也仅限于此。

最为重要的事物存在于企业的核心：位于企业边界之外的数字化资产、数据和应用程序，这些元素才是企业基础架构的核心。将关注重点从外部转向内部，实施基于软件的分段和 Zero Trust 框架，这样您就能获得必要的监测能力和控制力，以便检测和阻止横向移动、应用精细且具备适应性的策略，并阻止各种网络攻击（比如勒索软件）在您的网络中传播。

申请演示或**了解详情**，包括分段如何帮助解决勒索软件、Zero Trust、云安全等问题。

1 Cybersecurity Ventures，《2022 年勒索软件对手方分析报告》(2022 Who's Who In Ransomware Report)。Conceal，2022 年。

2 Kellerman, Tom 和 Greg Foss，《全球事件响应威胁报告》(Global Incident Response Threat Report)。VMware Carbon Black，2020 年 10 月。

3 《2023 年网络安全统计趋势与数据》(2023 Cyber Security Statistics Trends & Data)。PurpleSec，2023 年 2 月 22 日。