将微分段和零信任相结合

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Adopting Microsegmentation Into Your Zero Trust Model, Part 1		
原文作者	珍妮弗·格雷戈里（Jennifer Gregory）	原文发布日期	2021 年 4 月 27 日
作者简介	珍妮弗·格雷戈里是一位致力于网络安全的自由作家。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/adopting-microsegmentation-into-zero-trust-part-1/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	将微分段与零信任相结合，可以抵御威胁，为企业提供强大的保护。员工不能再随意访问所有系统或某些系统，他们只能根据工作需要进行访问。每次访问都需要进行身份验证，这使他们更难访问与其工作无关的敏感数据。更重要的是，在网络微分段的情况下，即使员工对应用程序或数据发起攻击，他们能够造成的损害也是有限的。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

将微分段和零信任相结合

珍妮弗·格雷戈里

2021 年 4 月 27 日

有一天，我边排队边通过蜂窝数据阅读网络安全文章，突然想到了将微分段与零信任模型相结合。

撰写这篇文章时，我使用了不同的设备，包括连接到家庭无线网络的笔记本电脑和连接 Wi-Fi 的平板电脑。每次我切换设备或无线网络，或者同时切换两者时，我遭受攻击的风险就会增加。这是因为，我为潜在攻击者打开了新的入口点，或新的数据泄露端点。

像我一样，全国各地的员工和企业都在使用手头上的设备和网络进行工作。在过去的一年中，工作与家庭之间的界限几乎已经消失了。如果将这种情况扩展到整个员工队伍，企业的安全风险和漏洞会显著增加。

接下来，我们将讨论企业如何使用网络微分段和零信任模型来管理内部关系。

转向零信任模型

现在，“随处办公”已经是一种新常态。过去，企业领导者专注于边界保护。但是，随着企业转向远程办公，以及多个云环境和个人设备的使用，这种方法已经不再奏效。要想保护当今的工作环境（可能是世界上的任何地方），企业不仅需要购买新的技术或基础架构，还需要新的方法。在整个数据环境中管理权限和对工作负载的访问，需要对安全策略、技术和流程进行很大的改变。

越来越多的公司开始转向零信任模型。这意味着，企业要假设，请求访问网络的每个人或设备均未经授权。这些人员或设备要想获得访问权限，必须通过验证。通过正确使用零信任模型，用户和设备可以从任何位置访问所需的数据和系统。同时，该模型可以阻止攻击者，防止数据泄露。

微分段是什么？

在“良好的防御”与“访问数据和系统的需求”之间取得平衡非常重要。通过网络微分段，企业可以在各个网段之间创建带有“墙”的小访问区域。

可以把这想像成一个带有围墙的花园，这个花园里面还有很多个小花园，每个小花园都有围墙，而且是上锁的。只有拿到正确的钥匙，才能进入这些花园。所有植物都位于各自的花园中。如果发生火灾或动物啃食，只有特定花园中的植物会遭殃。

将微分段理论应用到数据和网络上，可以得到相同的保护。使用此策略时，如果发生攻击，则只会泄露特定区域的数据。或者说，如果攻击者进入企业网络，他们只能访问并破坏一个区域。微分段限制了一次攻击可能造成的损害，从而降低了风险。在远程办公的情况下，微分段的作用更加重要。现在，越来越多的医疗机构开始使用物联网设备，这些设备包含敏感的健康数据。因此，这些医疗机构开始采用微分段策略来保护设备和数据。

但是，在当今复杂的工作环境中，企业需要制定微分段策略，并将其谨慎地应用于不同的用户和设备。

为工作负载、应用程序和设备制定策略

我们会想当然地认为，我们使用了几十年的“基于角色的访问”很容易转变为微分段——即，简单地将新的用户类型添加到久经考验的“管理员”和“用户”中。但是实际上，我们需要考虑员工办公所需的数据访问权限，并了解每项工作负载。企业应对数据流和基础架构进行全面分析，从而启动内部微分段，以查看内部员工工作负载的位置。

但是，内部关系不仅仅包括“人”，还包括需要访问系统、云网络和数据的每个内部设备和应用程序。零信任策略不仅要确定哪些用户可以访问特定网段外，还要确定哪些应用程序和设备可以直接相互连接。在设计网络微分段时，企业必须能够实现分段应用以及流量的可见性。

随着远程办公越来越普遍，员工不仅使用公司的设备，还使用授权的个人设备，这使情况变得更加复杂。企业可以在设备级别采用精细而灵活的策略，以迅速适应业务规模的扩展。这种策略可以承袭，企业不必在每次发生变化时都重新定义工作负载策略了。

通过零信任微分段减少内部威胁

微分段能够为员工创建访问权限，从而提高其工作效率。此外，微分段还有助于防止内部威胁。根据《2020 年内部人员威胁报告》，68%的企业指出，在过去一年中，内部人员威胁有所增加。企业必须采取适当的措施，在“为员工提供完成工作所需的访问权限”与“防止内部人员网络攻击”之间取得平衡，而这通常难以实现。

将微分段与零信任相结合，可以抵御这类威胁，为企业提供强大的保护。员工不能再随意访问所有系统或某些系统，他们只能根据工作需要进行访问。每次访问都需要进行身份验证，这使他们更难访问与其工作无关的敏感数据。更重要的是，在网络微分段的情况下，即使员工对应用程序或数据发起攻击，他们能够造成的损害也是有限的。

从表面上看，微分段的概念很简单——为微服务创建单独的分段。但是，将其应用到实践中就非常复杂了，对于内部连接而言更是如此。微分段的最大优势之一是易于扩展和更改策略。通过使用这种策略，企业可以获得敏捷性，随时对员工、设备、工作负载和应用程序进行内部更改，以响应不断变化的业务需求。借助微分段和零信任，企业可以创造当今世界所需的安全性和灵活性。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com