保护分布式企业需要将 SASE 和 ZTNA 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	Protecting Distributed Businesses Requires Combining SASE and ZTNA		
原文作者	尼拉夫·沙阿（Nirav Shah）	**原文发布日期**	2021 年 5 月 24 日
作者简介	尼拉夫·沙阿是 Fortinet 公司产品和解决方案副总裁。		
原文发布单位	Information Week		
原文出处	https://informationweek.com/strategic-cio/protecting-distributed-businesses-requires-combining-sase-and-ztna/d/d-id/1341031		
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	对于那些劳动力高度分散的企业，将 ZTNA 与安全连接解决方案（例如“安全访问服务边缘”[SASE]网络架构）相结合非常重要。SASE 将 VPN 和 SD-WAN 等工具与云原生安全功能（例如安全 Web 网关、云访问安全代理和下一代防火墙）相结合，帮助企业保护进出云的数据、工作流和应用程序，在远程用户/设备以及云应用程序之间建立并维护灵活安全的连接。		
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。		

保护分布式企业需要将 SASE 和 ZTNA 相结合

尼拉夫·沙阿

2021 年 5 月 24 日

如今，企业的运行依赖于其客户或员工使用的各种应用程序。这些应用程序能够支持协同，提高生产力，使员工能够远程工作，并使客户能够远程购买解决方案和访问个人账户。企业 IT 团队最关心的问题包括：开发用户友好的应用程序、保持关键服务的最佳性能，监控用户体验以及保护对重要资源的访问。

应用程序可以在企业网络内运行并可以访问关键信息，因此对网络犯罪分子来说，它们很有吸引力。通过秘密监控进出家庭办公室的流量，网络犯罪分子能够检测到用户使用的应用程序。之后，他们可以利用家庭网络中的漏洞，访问这些应用程序。这样一来，他们就能入侵和利用关键应用程序，获得对关键数据和资源的访问权限，并找到机会来入侵网络。

为了防止这种情况发生，企业需要采取三项措施：（1）确保所有进出网络资源的连接都是安全的；（2）确保应用程序得到适当的强化；（3）仅允许有需要的人员获得应用程序的访问权限。

“零信任网络访问”(ZTNA) 由 VPN 演变而来，旨在为应用程序创建逻辑访问边界。通过验证用户和设备的身份和情境信息，ZTNA 不仅能限制对应用程序的访问，还能禁止被授予应用程序访问权限的人员在网络中横向移动。此外，ZTNA 还可以隐藏应用程序，使其不被发现，从而减少企业的潜在攻击面。

对于那些劳动力高度分散的企业，将 ZTNA 与安全连接解决方案（例如“安全访问服务边缘”[SASE]网络架构）相结合非常重要。SASE 将 VPN 和 SD-WAN 等工具与云原生安全功能（例如安全 Web 网关、云访问安全代理和下一代防火墙）相结合，帮助企业保护进出云的数据、工作流和应用程序，在远程用户/设备以及云应用程序之间建立并维护灵活安全的连接。

当 ZTNA 和 SASE 一起使用时，可保护应用程序和远程用户，使其免受针对家庭办公室及其不安全网络（以访问业务应用程序和关键资源）的网络犯罪分子的侵害。

但是，在设计基于 ZTNA 和 SASE 的安全连接/安全访问策略时，企业需要注意一些挑

战。

首先，当今很少有网络完全基于云。因此，SASE 和 ZTNA 解决方案还需要与边缘安全解决方案（例如边缘安全、SD-WAN 和零信任访问[ZTA]解决方案）无缝集成，以确保一致的端到端保护。无论在云中部署哪种安全和连接解决方案，都需要能够查看部署在每个网络边缘（包括数据中心、总部、分支机构和家庭办公室以及端点设备）的安全解决方案并与之互操作。否则，策略执行可能会变得不一致，可见性就会有局限性，网络犯罪分子就能发现和利用孤立的安全部署之间的漏洞。

其次，大多数混合网络跨多个云。因此，网络某部分的策略必须与其他部分部署的策略一致，包括作为 SASE 解决方案一部分的策略或部署在每个云实例中的策略。与其在每个边缘部署独特的安全解决方案，不如跟踪在网络中移动的数据和工作流。企业需要跨整个分布式网络部署一种通用策略、一种通用管理配置和一种通用实施策略。这需要将 ZTNA、SASE 和其他网络/安全工具作为统一安全平台的一部分运行，该平台可以部署在任何地方、在不同环境之间进行通信、提供统一的可见性，并对检测到的威胁启用一致、同步的响应。

最后，SASE 和 ZTNA 解决方案是集成技术的融合。很少有供应商能够提供可以解决网络、连接和安全问题的全套企业级解决方案。随着企业添加其他云、数据中心、分支机构和家庭办公室、应用程序以及最终用户环境和设备，能够做到这一点的供应商就更少了。要想找到支持和保护动态、不断扩展的网络环境的解决方案，企业需要依赖第三方测试和验证、分析师和客户评审，以及供应商的跟踪记录。这将帮助他们找到像宣传地那样有效，而且可以随着网络不断扩展和增长的解决方案。毕竟，企业不仅要保护今天的网络，还要保护未来不断发展的网络。

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