为 SASE 铺平道路：实现连接和安全的四个方法

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	Paving your path to SASE: 4 tips for achieving connectivity and security		
原文作者	克雷格·康纳斯（Craig Connors）	**原文发布日期**	2022 年 6 月 1 日
作者简介	克雷格·康纳斯是 VMware 公司 SASE 业务副总裁兼总经理。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/06/01/ideal-sase-solution/		
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	随着分布式员工的数量持续飙升，连接到公司网络的新设备数量也随之增加。这导致 IT 团队无法有效应对所有的互联网连接和安全挑战。为了应对该问题，越来越多的企业开始使用“安全访问服务边缘”（SASE）。企业应采取下述四个方法：（1）向 SD-WAN 和 SSE 赋予同等的重要性；（2）将 SD-WAN 作为 SASE 和 SSE 的起点；（3）将成熟的 NaaS 供应商作为 SD-WAN 供应商；（4）将最佳 SD-WAN 和 SSE 解决方案相结合，以获得最佳结果。		
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。		

为 SASE 铺平道路：实现连接和安全的四个方法

克雷格·康纳斯

2022 年 6 月 1 日

如今，优化的网络连接和安全都是企业的优先事项；IT 团队不应顾此失彼。

随着分布式员工的数量持续飙升，连接到公司网络的新设备数量也随之增加。这导致 IT 团队无法有效应对所有的互联网连接和安全挑战。

为应对该问题，越来越多的企业开始使用“安全访问服务边缘”（SASE）。SASE 将基于云的 SD-WAN 与云交付 SSE 安全服务（包括访问控制、威胁防御、数据保护、安全监控等）相结合，从而提供无限的安全边界，同时从根本上提高性能。

当企业考虑构建或修改 SASE 架构并开始寻找供应商时，他们会发现，为融合性 SASE 解决方案寻找唯一的供应商是非常困难的。“安全即服务”（SECaaS）供应商通常的做法是阻止流量，而非及时交付关键服务，因此他们在 SD-WAN 方面表现平平。而一些“网络即服务”（NaaS）供应商逐渐证明，他们有能力将安全/网络连接融合到 SASE 解决方案中。

此外，企业还需要考虑其他一些问题，包括：是否应优先部署 SD-WAN 而非 SSE？如何成功部署 SSE？如何将最好的 SD-WAN 和 SSE 组件集成，以实现理想的 SASE 解决方案？

在下文中，我们将逐一探讨这些问题。

1. 向 SD-WAN 和 SSE 赋予同等的重要性

大多数公司会优先考虑 SD-WAN 而非 SSE。这是因为，如果企业无法连接到他们的资源，就无法赚钱。

举例来说，当 IT 团队考虑安全性时，会采用简单粗暴的粗方法——他们会监控网络，但不会进行任何可能导致业务暂停（从而导致数百万美元的损失）的重大安全升级。因此，优化连接仍然是必要的。

但是，如果企业将连接优先于安全，就会出现很大的问题。我们都知道，勒索软件攻击不断登上头条新闻，没有什么企业能够免受勒索软件攻击或网络安全漏洞的影响。甚至，国家支持的攻击者也在发动网络攻击。因此，企业需要在整个网络中部署 SSE。如果没有安全

看门机制，任何交易都无法进行。

2. 将 SD-WAN 作为 SASE 和 SSE 的起点

如果企业没有通过可靠的 SD-WAN 奠定连接基础，实施 SSE 将会非常困难。他们无法轻松地将连接性与安全性相结合，也无法轻松控制流量。这就像回到 1990 年一样：在命令行界面埋头打字，而非使用 Web 界面、API 和自动化手段。而 SD-WAN 的秘诀正是在 5 分钟内解决 1000 分钟的工作。

要想构建理想的 SASE 解决方案，关键是什么呢？企业应寻找能够提供下述服务的 SD-WAN 供应商：

- 强大的合作伙伴生态系统
- 为大型全球客户提供服务的良好记录
- 成熟的 SD-WAN 解决方案，可与知名 SSE 工具以及可能已经在企业混合环境中的第三方 SASE 解决方案无缝集成。

3. 将成熟的 NaaS 供应商作为 SD-WAN 供应商

为什么大多数 SECaaS 供应商未能提供真正的 SD-WAN 解决方案呢？或许，他们在构建 SD-WAN 解决方案时走了捷径。

很多 SECaaS 供应商可能在一个领域(如 SSE)表现出色，但在另一个领域(如 SD-WAN)却缺乏经验。

为了弥补自己的不足，这些供应商可能会购买另一家公司，而他们购买的公司可能也无法提供最佳 SD-WAN 平台。

或者，他们可能会购买和组装 SD-WAN 组件，进而调用该 SASE，而非构建真正的 SASE 平台。

举例来说，SSE/SECaaS 供应商一直在努力解决连接问题。他们要么收购 SD-WAN 供应商，要么选择与最佳的 SD-WAN 供应商合作。不幸的是，这种方法导致基于组件的解决方案无法像真正集成的 SASE 解决方案那样具备优化的性能。

优化网络解决方案的最佳方法是，选择能够提供成熟 SD-WAN 解决方案的供应商。该

解决方案能够帮助企业在 WAN 内创建连接其他知名 SSE 工具的访问层，同时确保最终用户能够快速、可靠和安全地访问他们的应用程序。

4. 将最佳 SD-WAN 和 SSE 解决方案相结合，以获得最佳结果。

如果企业开始其 SASE 之旅（特别是如果他们拥有大型 IT 环境），可能会考虑采用集成的多供应商 SASE 方法。这种方法能够为企业提供多种选择和灵活性，以便将理想的 SASE 解决方案拼凑在一起，从而获得企业所需的性能。这种灵活性使企业可以单独评估组件，跨 SD-WAN 和 SSE 供应商选择最佳的组件。我们可以把这个看成是，在各个技术领域都有“王牌”。

因此，在这种情况下，企业不必一次性地购买所有服务，而是可以寻找支持分阶段迁移的供应商，这更易于管理。

如果企业有独立的安全和网络团队，这种混合解决方案也能大大减少团队间的协商，使其运作更加容易。例如，如果网络团队想要升级 SD-WAN，那就可以升级，甚至无需与安全团队协商。归根结底，这种“政教分离”是有益的。

多供应商集成解决方案只是一个短期的解决方案，企业的最终目标是融合的单一供应商 SASE 解决方案。当企业开始其 SASE 旅程时，不仅要考虑从哪里开始，还要考虑选择受信任的供应商，例如选择在支持大型客户（包括许多全球 500 强企业）方面具有良好记录的供应商。

安天简介

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势，打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足客户对于包括终端杀毒、终端防护（EPP）、终端检测与响应（EDR）、云工作安全防护（CWPP）等系统安全层面需求；整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力；基于流量产品探海有效应对客户对于网络威胁检测与响应（NDR）和网络流量分析（NTA）的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到高级威胁（APT）的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

安天为网信主管部门、军队、部委、保密行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，已连续七届蝉联国家级网络安全应急支撑单位。安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑。

目前，安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过三十亿部智能终端设备提供了安全检测能力，已经成为“国民级”引擎。

安天已发展成为以哈尔滨为总部基地，建有六地研发中心、两个控股子公司，参与一个国家工程实验室建设，拥有两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在多地设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

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*