企业云网融合治理从 SD-LAN 切入

目前 SD-LAN 最令人接受的企业云网融合治理切入点是它的面向各种监控应用和物联设备的边界隔离——用于实现零信任网络访问架构优化。通过全面的 SD-LAN 策略，可在企业园区或车间网络级别实施基本的零信任方法，以阻止除明确允许之外的所有设备连接和内容。也就是说，SD-LAN 可以作为软件定义边界（SDP）的虚拟隔离层。

在部署了 SD-LAN 默认情况下会阻止大多数横向网络流量，例如异地间笔记本电脑 A 与笔记本电脑 B 通信，阻止来自受感染的设备大量恶意病毒或软件在传统 VPN 管道中扩散传播。

以现在的经典场景为例，攻击者使用损坏的物联网设备作为平台攻击工作站，而 SD-LAN 会阻止该过程。那些损坏的网络摄像头、数字电表或自动售货机只能看到它们的管理工作站并与之通信，而不是整个网段。如果攻击中涉及的端口、协议或流量违反了管理连接的任何访问规则，他们甚至可能无法破坏该管理工作站。

SD-LAN 的优点

- 可帮助实现更广泛和更有效的 LAN 间的 IP 管理虚拟化和运维自动化。
- 更好地发现、绘制和审核网络当前状态的能力。例如，网络团队可以跟踪和审计网络上的关键设备节点
- 能够显著地改善企业网络安全状况，管控各个局域网的边界和连接许可

SD-LAN 也面临很多挑战。其中一些挑战包括：

- 利用现有基础设施部署 SD-LAN 的能力和可行性方案
- 梳理和升级过程中发生的网络不中断和结构的调整
- 云网融合过程中内外网一体化的安全边界治理和隔离策略

随着企业开始广泛转向更高的网络自动化和更严格的安全性，SD-LAN 将成为推进企业目标的越来越重要的工具。