关于远程协同、居家办公的传统 VPN 替代方案的解答

问：因为疫情很多公司都居家办公或远程协同技术服务，使用传统 VPN 经常忘记密码，连接不稳定掉线，长期连接还总是担心被肉鸡，影响正常工作还造成很多无效加班，有没有可以替代 VPN 的产品？

答：VPN 作为接入内网的关键设备，是网络安全的第一道防线，已经成为很多黑客攻击的目标。但传统 VPN 技术建立之初，更多的是为了解决远程接入中心及传输加密的问题，并未过多考虑自身受到攻击及多用户与多应用间的频繁连接作业的稳定体验问题。

现在越来越的企业采用基于 SD-WAN 技术的零信任 EDGE 边界接入便携设备或云网盾客户端专网连接到指定的应用服务器或业务平台。这类零信任安全接入网关支持人、机随机多因子认证和鉴权能力，通过手机号码绑定的动态短信等进行身份认证，提高使用流畅、便捷、安全的体验。

- 安全传输：万联云网盾 EDGE-SEC 客户端与安全接入网关 EDGE 系列硬件设备间建立双向加密隧道，实时监控隧道连接状态，保护连接安全，在资源访问全生命周期维护隧道链接。
- 网关隐身：EDGE 零信任安全接入网关（比如万联的边边互联 N、S、R 系列）默认关闭所有端口，外部扫描不到任何网关的端口，只有安装零信任客户端的终端，经过内置硬件和客户端的非对称验证算法与云服务端的身份鉴权系统认证，才能够通过单包敲门的方式建立连接。
- 应用隐身：EDGE-SEC 零信任客户端与 EDGE 系列安全接入网关成功连接之后，此时内部的业务应用还是隐身状态。只有通过后台的隧道管理平台的用户，才能看到有访问权限的应用系统。
- 用户认证：支持动态认证与静态密码混合认证，免密认证，识别用户真实身份，提升认证体验，支持短信验证码、一键授权确认等认证方式，满足全场景认证需求。
- 设备认证：通过提取设备的硬件、操作系统、协议栈和网络状态相关的特征，结合机器学习算法，生成连接设备的 UID，标识可信设备，在登录及访问过程中持续验证设备身份，实现无感设备认证。
- 应用代理：支持 B/S、C/S 架构应用，支持多种协议访问代理，包括但不限于 http/https、TCP/UDP 等，支持基于隧道流量精细化控制，按需授权，实现应用级端口代理和流控。