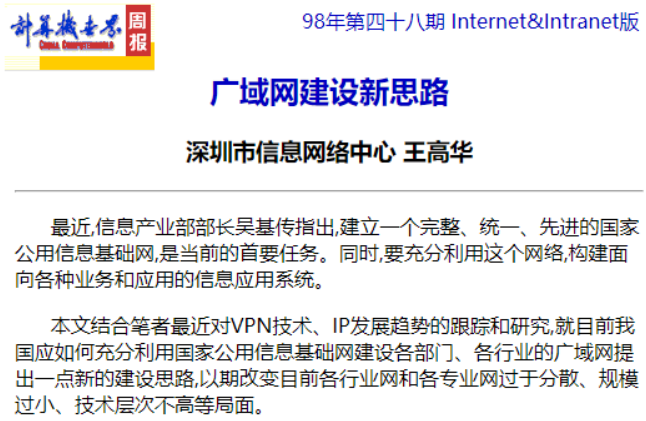
企业 VPN 将退出历史舞台？

无论是搜索英文网站还是中文网站，都能找到关于“企业 VPN 是否已死”的话题，这个话题当然是由于现在零信任太火了，有人认为企业 VPN 必死，必将被零信任安全所取代。当然也有人认为 VPN 仍然有效，有些 VPN 厂商也已经开始研发和销售零信任 VPN 产品。本文就谈谈笔者对这个问题的看法。

笔者早在 1998 年 12 月、1999 年 1 月和 3 月相继在《计算机世界》报和《中国计算机报》发表了 VPN 技术相关的文章《广域网建设新思路》、《政府上网 VPN 出力》和《怎样选择 VPN 方案》，当时我还在深圳市信息网络中心(现已更名为**深圳市大数据资源管理中心**)担任总工程师，负责深圳市政务骨干网设计、建设和运维。可以说，我是一个资深的 VPN 技术专家，个人创业创立沃通 CA 后，我也是一直在推动 SSL VPN 设备的 SSL 证书应用和全自动部署，并已成功帮助一家 VPN 厂商实现了全球信任的 SSL 证书全自动部署到 SSL VPN 设备中。今天重写 VPN 话题，当然是因为我又重新创业创立了零信技术。笔者认为：零信任使得 VPN 将逐渐退出历史舞台，而 Gartner 预测到 2023 年将有 60%的 VPN 被零信任取代。



计算机世界 周报 98年第四十八期 Internet&Intranet版

广域网建设新思路

深圳市信息网络中心 王高华

最近,信息产业部部长吴基传指出,建立一个完整、统一、先进的国家公用信息基础网,是当前的首要任务。同时,要充分利用这个网络,构建面向各种业务和应用的信息应用系统。

本文结合笔者最近对VPN技术、IP发展趋势的跟踪和研究,就目前我国应如何充分利用国家公用信息基础网建设各部门、各行业的广域网提出一点新的建设思路,以期改变目前各行业网和各专业网过于分散、规模过小、技术层次不高等局面。

计算机世界 周报 1999年3月22日

《网络与应用》版 网络技术与方案

怎样选择VPN方案

深圳市信息网络中心王高华

目前，虚拟专用网(VPN)技术已成为国际网络市场最热门的话题，据估计，今天2亿多美元的VPN市场到2001年将增长到119亿美元，人们会很快认可VPN技术，VPN系统在调查用户计划购置的10个产品中排名已升至第三位。

CCIDNET.com 赛迪网

最新动态 | 热线联络 | InfoWeb地图 | 关于InfoWeb | 关于报社 | 搜 索

◀ 媒体全文 | 全文检索 | 浏览其他期

出版日期：1999-01-14 总期号：794 本年期号：04

中国计算机报

本期导读 0

要闻综合 1

软件 2

政府上网VPN出力

深圳市信息网络中心 王高华

1999年将是我国的“政府上网年”，电信部门为了促进“政府上网工程”推出了一系列优惠措施。各级政府部门应如何借此东风推进内部办公自动化建设，如何加强各个政府部门的网络互联和内部信息资源共享，如何采用新技术既确保网络安全又充分利用电信部门提供的联网线路，这些是本文要讨论的问题。

VPN 技术产生于 1996 年，1998 年开始在国内出现，笔者当时认为这是一个非常好的技术，在阅读了大量国外有关产品资料后连续就 VPN 技术发表了 3 篇文章。可以说，企业 VPN 在过去的 25 年为政府用户和企业用户远程接入内部办公系统立下了汗马功劳，也造就了一批 VPN 产品厂商的崛起。特别是当下的疫情大流行期间，由于大量员工需要远程办公，使得 VPN 的使用处于历史最高水平，因为企业希望保持专有信息和敏感通信的安全。

但是，VPN 是 25 年前基于网络边界防护而开发的产品，旨在扩展可信网络范围，目标是满足有特定远程访问需求的相对较小比例的用户。然而，随着当今基于云基础设施（公有、私有和混合）的普及应用，VPN 已经无能为力去保护非企业自建的云基础设施，不仅不可能，即使想办法实现也是效率低下，并为攻击者打开了大门。VPN 不是通过线性访问来保护扁平网络，而是尝试保护外围网络。更大的问题是，VPN 根本不够安全，无法抵御当今日益复杂的威胁，远程办公更是如此。2020 年，网络犯罪分子推出了专门用于通过 VPN 获取敏感信息的钓鱼诈骗。由于涉及如此多的设备和位置，如果发生攻击，潜在的损害是巨大的，因为 VPN 通常允许用户访问整个网络。

简单通俗点讲，VPN 存在的基础已经变了，现在的网络设施已经无法基于网络边界来实现安全防护了，必须基于新的安全理念来实现安全防护。这就是零信任！是时候考虑从传统的 VPN 转向基于零信任网络接入（ZTNA）的现代替代方案了。零信任的核心原则是“永不信任和始终验证”，而不是通过 VPN 接入后就可以畅通无阻！零信任模型不是假设企业防火墙后面发生的所有事情都是安全的，而是假设每次连接都是攻击，所以必须验证每个请求，无论它来自何处，就好像它来自一个开放的网络一样。在授予访问权限之前，每个访问请求都经过身份验证、授权和加密。这与 VPN 等传统安全模型刚好相反。零信任与传统 VPN 安全模型的不同之处在于，它不断验证所有尝试访问网络的用户或设备，而 VPN 使用一次身份验证过程，并假设如果用户在网络内，一切都很安全。

那该如何实现零信任来取代 VPN？由于零信任只是一个理念，并不特指某个产品，所以，已经有许多安全厂商包括 VPN 厂商出台了各种零信任安全解决方案。据微软官网介绍，微软在疫情大流行时普遍采用远程工作方式使用了零信任策略来保护微软办公网络，作为公司零信任安全战略的一部分，Microsoft Digital 的员工通过采用拆分隧道配置重新设计了公司 VPN 基础结构，从而进一步支持公司的工作负载迁移到云。这不仅减轻了 VPN 的压力，并为员工提供了更多的带宽来安全地完成工作。80% 的远程工作流量流向启用了拆分隧道的云端点，但员工远程执行的其余工作（需要在企业网络上锁定）仍然通过公司的 VPN 进行。

零信技术提供基于密码技术的零信任解决方案，实现零信任的五大安全目标中的网络身份可信、网络设备可信、网络流量加密、网络应用可信、网络数据加密，这五大目标都是通过采

用密码技术的数字签名和加密来实现。每个用户都有可信身份证书，每个设备都有可信身份证书，用户使用可信身份和可信设备可以安全地通过互联网接入公司内网和接入云服务，而无需通过 VPN 设备。所有数据连接直接通过 https 加密而无需通过 VPN 通道加密，所有电子邮件也是实现端到端加密而无需 VPN 通道连接到内网邮件服务器。也就是说，原先必须通过 VPN 设备实现的通道加密已经通过数字证书来实现了身份认证、传输加密和数据加密，使得 VPN 设备已经不再有存在的意义了，所以，笔者的结论是：随着零信任理念、密码技术和相关解决方案的普及应用，企业 VPN 一定会因为没有了应用场景而逐渐退出历史舞台。

王高华

2021 年 12 月 27 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。