

虚拟专用网：面向 Fabrikam 公司的技术概述

2023 年 12 月 15 日

虚拟专用网 (VPN) 是一种常用的网络安全解决方案，可帮助加密网络流量。

VPN 充当安全隧道并对 Internet 流量进行加密，使第三方难以跟踪活动和窃取数据¹。

实现 VPN 的优点：

- VPN 通过加密 Internet 流量提供了一层隐私和安全保护。这使得第三方难以跟踪活动和窃取数据。
- 在机场或图书馆使用公共 Wi-Fi 时，VPN 可帮助避免遭受黑客攻击。这是因为 VPN 充当了安全隧道并对 Internet 流量进行了加密。
- 使用 VPN 可防止 Internet 服务提供商知道你访问了哪些网站，因为进出计算机的流量全都通过 VPN 的服务器或 VPN 付费使用的服务器传输¹。
- VPN 可通过屏蔽 IP 地址并加密 Internet 连接，绕过对内容²的地理限制。连接到 VPN 服务器时，你的 Internet 流量会通过 VPN 服务器进行路由，该服务器会为你分配一个新的 IP 地址。这使你看起来像是从其他位置访问 Internet，从而能够绕过对内容的地理限制

实现 VPN 的缺点：

- 连接速度可能比 ISP 慢。[这是因为 VPN 为 Internet 流量增加了一层额外的加密和路由²。](#)
- VPN 在某些专制国家/地区被禁止使用。[在某些国家/地区，VPN 被禁止使用或受到严格监管²。](#)
- 使用免费 VPN 会有遭遇广告、恶意软件和泄露的风险。[免费 VPN 可能会将用户数据出售给第三方广告商，或在网页中植入广告²。](#)

安装细节：

- [VPN 在运行 VPN 客户端的系统和 VPN 服务器之间建立加密隧道，然后 VPN 服务器通过隧道将流量代理到企业网络的其余部分⁴。](#) 步骤包括
 1. VPN 客户端安装在用户的设备上，对设备与 VPN 服务器之间的所有流量进行加密。
 2. VPN 服务器解密流量并将其转发到预期目标。
 3. 目标服务器响应请求，将流量发送回 VPN 服务器。
 4. VPN 服务器对流量进行加密，并将其发送回 VPN 客户端。
 5. [VPN 客户端解密流量并将其发送到用户的设备¹。](#)
- 若要安装和配置 VPN 服务器，请按照下列步骤操作：
 1. 在计算机上创建 VPN 配置文件。
 2. 单击“开始”，然后单击“设置”以打开设置菜单。
 3. 在设置菜单中，单击“网络和 Internet”，然后单击“VPN”。
 4. 选择“添加 VPN 连接”。
 5. 在“添加 VPN 连接”窗口中，需要执行几项任务。
 6. [保存所做的更改⁵。](#)

风险和缓解措施：

- 攻击者意识到远程工作是一种威胁途径已有一段时间。出于多种原因，远程工作环境对攻击者特别有吸引力。首先，家庭网络环境缺乏专业管理。最关键的是，这意味着家庭网络上的很多系统没有定期修补，其中许多系统在漏洞缓解方面已经过时。要在企业网络上持续存在，攻击了系统的攻击者必须避开检测，并抵抗住修正。在这方面，家庭网络对攻击者也更加友好；威胁检测通常几乎不存在，修正也只是偶然进行，例如当电脑因运行缓慢而重新安装或停用时。要确保远程工作环境的安全，必须进一步扩展零信任假设。[不仅是网络，一切不在企业控制范围内的东西都应被视为有敌意⁴](#)。
- [使用最新的软件补丁和安全配置更新 VPN、网络基础结构设备和用于远程访问工作环境的设备⁶](#)。

有关实现的最佳做法：

在企业网络中实现 VPN 的最佳做法包括：

- [选择使用 Internet 密钥交换/Internet 协议安全性 \(IKE/IPSec\) 等公认标准的基于标准的 VPN，这些 VPN 通常比使用自定义代码通过 TLS 发送流量的安全套接层/传输层安全性 \(SSL/TLS\) VPN 风险更低、更安全¹²](#)。
- 使用具有强大加密功能的 VPN。验证 VPN 使用的加密算法、身份验证算法和协议是否强大且经过 FIP 验证。[将所有 VPN 配置为使用多重身份验证 \(MFA\)，并尽可能使用通过数字证书（存储在智能卡上）进行的客户端身份验证来取代基于密码的身份验证¹²](#)。
- 管理软件漏洞。利用 VPN 漏洞是网络罪犯常用的攻击途径。请选择在漏洞修补方面有良好记录的 VPN 供应商，并要求提供软件物料清单 (SBOM)，以验证第三方代码是否是最新且安全的。此外，还要寻找能够在运行时对其代码进行验证的产品，以检测潜在的入侵。[部署 VPN 后，定期检查并及时应用软件更新¹²](#)。
- 为使用量激增做好准备。[IT 安全人员应测试 VPN 限制，为大规模使用做好准备²](#)。
- 避免使用免费 VPN。[使用免费 VPN 会有遭遇广告、恶意软件和泄露的风险³](#)。