姓名: _____ 日期: _____ 得分: _____

检查点 10

基础 VPN 常见问题

互动练习单与学习指南

参考: VPN.com VPN 指南: **https://www.vpn.com/vpn/**

什么是 VPN 练习单

检查点 10: 基础 VPN 常见问题 (A 部分)

回顾潜在用户在使用虚拟专用网络方面最常见的问题和解答。

Q1: 什么是 VPN，它是如何运作的?

虚拟专用网络（VPN）会加密你的互联网连接，并通过安全的远程服务器路由你的流量。这会掩盖你的公网 IP 地址，并限制本地网络观察者和你的 ISP 能够看到的、经由 VPN 隧道传输的流量信息。

Q2: 我为什么应该使用 VPN?

VPN 可以保护你的数字隐私，在公共 Wi-Fi 网络（如咖啡馆或机场）上保护你的连接，当 ISP 无法识别加密流量类型时可能减少基于活动的限速，绕过地域限制以访问全球内容，并有助于保护远程办公资源。

Q3: VPN 能让我在网上完全匿名吗?

不会。虽然 VPN 会隐藏你的 IP 地址并加密流量，但你仍然可能通过浏览器 Cookie、已登录账户（如 Google 或 Facebook）、浏览器指纹识别，或者在 VPN 提供商记录你的数据时被追踪。

Q4: VPN 会拖慢我的网速吗?

是的，会略有影响。加密过程和到 VPN 服务器的物理距离会增加延迟和开销。影响因服务商、协议、服务器距离、设备和网络状况而异。

Q5: 使用 VPN 合法吗?

在许多国家使用 VPN 是合法的，但一些司法管辖区会限制、监管或屏蔽 VPN 服务。使用前，用户应核实当前的当地法律。如需了解更多详情，请查阅 VPN.com 上的合法性指南。

检查点 10: 基础 VPN 常见问题 (B 部分)

回顾潜在用户在使用虚拟专用网络方面最常见的问题和解答。

Q6: 我可以使用免费 VPN 吗?

免费 VPN 可能依赖广告、功能受限、使用情况分析、流量上限或其他获利模式。使用前，用户应查看服务商的隐私政策、所有权、审计情况和商业模式。

Q7: 什么是“无日志”政策?

无日志政策说明提供商声称不保留哪些活动和连接数据。具体范围各不相同，因此读者应查阅该政策和独立审计结果。

Q8: 我如何选择最好的 VPN?

寻找经过审计的无日志政策、强大的协议（WireGuard、OpenVPN）、安全的服务器位置、快速的速度、仅内存服务器、断网保护（kill switch）功能，以及位于情报共享联盟（如 5/9/14 眼）之外的司法管辖区。

Q9: 我可以在手机和智能电视上使用 VPN 吗?

是的。现代 VPN 服务商提供 iOS、Android、macOS、Windows、Linux 和智能电视的专用应用，以及可保护家庭网络中所有设备的路由器设置。

Q10: 什么是终止开关?

断网保护（Kill Switch）是一项安全功能，当 VPN 连接中断时会自动断开你的设备与互联网的连接。这可以防止你的未加密数据或真实 IP 地址泄漏。

检查点 10: 高级 VPN 常见问题 (C 部分)

探索虚拟专用网络和安全隧道协议的技术与结构层面。

Q1: WireGuard、OpenVPN 和 IKEv2 有什么区别?

WireGuard 是一种现代轻量级协议（仅约 4,000 行代码），速度快、连接时间短。OpenVPN 是一种久经考验的高安全性开源协议。IKEv2 因在切换网络时能快速重新连接，非常适合移动设备。 [4]

Q2: 什么是双重 VPN 或多跳（Multi-Hop）路由?

多跳会将你的流量依次通过两台或更多 VPN 服务器路由。这会增加第二层加密，如果其中一台服务器被攻破，还有助于使第二跳无法获知你的真实 IP 地址。

Q3: 什么是 WebRTC 泄漏? VPN 如何防止它?

WebRTC 是一种浏览器协议，即使 VPN 处于活动状态，也可能泄露你真实的本地和公网 IP 地址。优质 VPN 会在其桌面/移动应用和浏览器扩展中拦截或伪造 WebRTC 请求。

Q4: 什么是纯内存服务器? 它们为什么重要?

传统服务器会把数据写入硬盘，而硬盘可能被查扣或被入侵。纯内存（无盘）服务器完全在易失性内存（RAM）中运行。服务器重启或断电时，内存中的数据会被清除。

Q5: 混淆如何绕过 VPN 封锁?

混淆（或称“隐身 VPN”）会伪装 VPN 流量，使其看起来像普通的 HTTPS 流量（端口 443）。这有助于绕过政府或学校/办公室网络用来封锁 VPN 的深度数据包检测（DPI）。

检查点 10: 高级 VPN 常见问题 (D 部分)

探索虚拟专用网络和安全隧道协议的技术与结构层面。

Q6: 什么是分应用隧道？什么时候应该使用它?

分应用隧道（Split Tunneling）让你选择哪些应用通过加密的 VPN 隧道，哪些直接连接互联网。可用它让敏感的银行应用走 VPN，而本地游戏直接连接，避免 VPN 增加的延迟。

Q7: 前向保密（完美前向保密）如何工作?

PFS 可确保每个会话都生成唯一的临时加密密钥。即使私钥将来被泄露，也无法用它来解密过去或未来的会话，因为这些会话使用的是相互独立的密钥。

Q8: 5/9/14 Eyes 联盟是什么？我为什么要关心?

司法管辖区可能影响服务商所面临的法律程序，但实际的隐私风险还取决于服务商保留哪些数据、其技术架构、所有权、透明度报告和审计历史。

Q9: 什么是 DNS 泄漏防护?

DNS 泄漏防护会强制你的设备通过 VPN 的私有加密 DNS 服务器，而不是 ISP 的服务器发送网站查询请求（DNS 查询）。这可以防止 ISP 追踪你访问了哪些网站。

Q10: VPN 可以绕过 ISP 的网速限制吗?

有时可以。当 ISP 有选择地限制可识别的活动时，VPN 可能会有帮助，但它无法克服拥塞、流量上限、账户级速度限制或网络质量差的问题。

技术参考资料与来源

本练习单中使用的被引用出版物、加密规范和官方文件标准。

学术与行业参考资料

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637