姓名: _____ 日期: _____ 得分: _____

如何隐藏你的 IP 地址练习单

隐藏 IP 地址、位置伪装、代理、Tor，以及防止 DNS/WebRTC 泄漏

VPN 学习概述

学习者

学生身份

网络防御者路线

安全

连接状态

保护数据包

已开启

防泄漏保护

DNS 与 IPv6 泄漏防护

欢迎！ 本活动手册将带你了解虚拟专用网络（VPN）的基本原则。你将探索加密隧道如何保护你的数据、网络协议如何运作，以及如何识别并减轻隐私泄漏。

练习单检查点

- [ ] **第 1-4 部分: 掌握 VPN 概念和协议。**
- [ ] **第 5-7 部分: 解答填字游戏和单词搜索谜题。**
- [ ] **第 8-9 部分: 解答案例研究和密码挑战。**
- [ ] **第 10 部分: 查看基础和进阶 FAQ 页面。**
- [ ] **第 11 部分: 探索 10 个有趣的现实事实。**
- [ ] **附加: 快速思考挑战。**

打开 VPN.com VPN 指南

URL: https://www.vpn.com/vpn/

你的 VPN 学习路线图

- 解释 IP 地址如何运作以及如何泄露位置。
- 对比代理、Tor 与 VPN 在隐藏网络地址方面的差异。
- 识别检测和防止 DNS 与 WebRTC 泄漏的方法。
- 了解网站如何通过你的公网 IP 追踪用户。
- 评估用于 IP 保护的多跳路由和加密隧道。

IP 保护练习单说明

回答单项选择题和判断题，使用词库完成填空句，配对定义，并解答填字游戏和找词游戏。将所学知识应用于隐藏你的 IP 地址和防止泄露。 最后完成附加活动: 快速思考。

隐藏你的 IP（简介）

你的 IP 地址就像一个数字邮寄地址，会暴露你的实际位置和上网习惯。隐藏 IP 是抵御在线跟踪、目标画像和地理位置封锁的第一道防线。了解如何安全地隐藏你的地址，有助于保护你的在线隐私。

仔细阅读每个检查点，选择或写出正确的答案。

检查点 1: 单项选择挑战

1. 设备的公共 IP 地址会向你访问的网站透露什么?

- A. 用户的信用卡号
- B. 你的大致位置和 ISP 的名称
- C. 完整的本地文件目录
- D. 键盘语言设置

2. 哪种方法可隐藏你的 IP 并加密整个系统的所有流量?

- A. 标准网页代理
- B. 清除你的浏览器 Cookie
- C. 虚拟专用网络（VPN）
- D. 禁用你的原生防火墙

3. 使用免费网络代理的一个主要隐私局限是什么?

- A. 它不会加密公共网络上的数据流量
- B. 它需要安装外部操作系统
- C. 它在美国完全违法
- D. 它需要专用电话线连接

4. Tor 网络如何为用户提供高度匿名性?

- A. 通过加快连接速度
- B. 通过三个由志愿者运营的中继节点路由流量
- C. 通过在全球数据库中登记你的姓名
- D. 通过仅限政府机构访问

5. 什么是 DNS 泄露?

- A. 将电子邮件发送到错误地址的错误
- B. 当 DNS 查询绕过 VPN 隧道直接发往 ISP 时
- C. 本地路由器电源的硬件故障
- D. 本地网络适配器驱动程序的更新

检查点 2: 判断正误挑战

6 问题 6

6. 代理服务器会像 VPN 一样加密后台操作系统流量。

○ 正确 ○ 错误

7 问题 7

7. Tor 路由安全性很高，但会降低网络浏览速度。

○ 正确 ○ 错误

8 问题 8

8. WebRTC 泄露可能在 VPN 会话期间暴露你的真实 IP。

○ 正确 ○ 错误

9 问题 9

9. 开启 VPN 且没有泄漏时，你的 ISP 无法看到你访问了哪些网站。

○ 正确 ○ 错误

10 问题 10

10. 隐藏你的 IP 地址可以阻止通过浏览器指纹进行的跟踪。

○ 正确 ○ 错误

检查点 3: 关键术语填空

阅读下面的每个句子，并从词库中选出正确的术语填空。

1. 绕过安全隧道而暴露域名查询的情况称为 _____ 。
2. 基于浏览器的 _____ 通信接口可能会意外泄漏你的原生 IP 地址。
3. 网页 _____ 会重定向浏览器流量，但不会加密数据包内容。
4. _____ 网络的多层加密提供了很高的匿名性。
5. 你的公共 _____ 由电信运营商分配，会暴露你所在的区域。
6. 通过 _____ 伪装可以绕过地区性的媒体封锁。

词汇词库

代理　服务器网络　实时　网络地址　网络追踪　位置　洋葱　域名泄漏

在此写下你的答案:

1.
2.
3.
4.
5.
6.

检查点 4: 网络概念配对

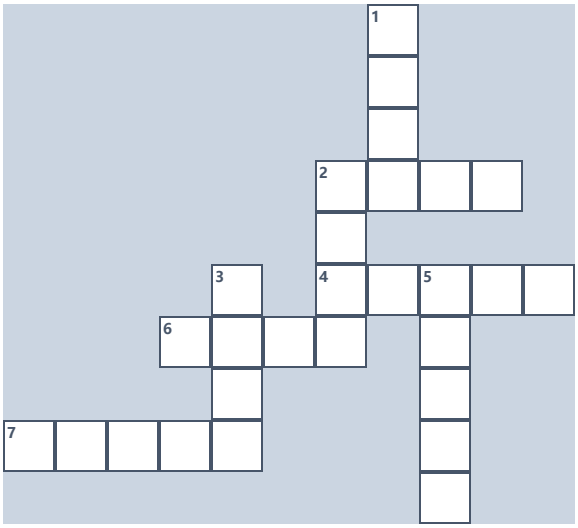
定义配对

将左侧的每个词汇与右侧正确的定义配对，在可填写的输入框中写出对应的字母（A-H）。

	1. IP 地址	**A**	加密设备的所有流量并通过 VPN 服务器路由。
	2. VPN 隧道	**B**	通过三个志愿者服务器路由数据，并在每一步加密一层。
	3. Tor 网络	**C**	通过另一个国家的服务器路由连接，以绕过地理封锁。
	4. 网络代理	**D**	标识互联网上设备接口的唯一数字标签。
	5. DNS 泄露	**E**	在应用层重定向浏览器流量，但不进行系统级加密。
	6. WebRTC API	**F**	你的电信运营商对未加密互联网流量目的地的记录。
	7. 位置掩蔽	**G**	在 VPN 隧道之外解析的查询，会向 ISP 暴露所访问的域名。
	8. ISP 跟踪	**H**	用于语音/视频的浏览器功能，可能绕过隧道并暴露真实 IP 地址。

检查点 5: 填字游戏

在活动的白色方框中输入汉字，完成填字游戏。数字对应下面的提示。



横向

2. 在互联网上标识设备接口的唯一数字标签 (4)

4. 位于用户与目标网站之间负责转发请求的服务器 (5)

6. 替你的设备转发网络请求的中间节点 (4)

7. 电信运营商对未加密上网流量目的地的记录 (5)

纵向

1. 通过三台志愿者服务器路由数据，并在每一步加密一层 (4)

2. 在应用层重定向浏览器流量，但不进行系统级加密 (4)

3. 通过网络活动记录来追踪用户的行踪或行为 (4)

5. 分布在多地、协同转发用户流量的一组服务器 (5)

检查点 5 替代活动: 无障碍填字线索

使用屏幕阅读器和键盘的用户可以直接在下面的文本框中输入填字游戏的答案。

横向

2 横向: 在互联网上标识设备接口的唯一数字标签 (4 字):

4 横向: 位于用户与目标网站之间负责转发请求的服务器 (5 字):

6 横向: 替你的设备转发网络请求的中间节点 (4 字):

7 横向: 电信运营商对未加密上网流量目的地的记录 (5 字):

纵向

1 纵向: 通过三台志愿者服务器路由数据，并在每一步加密一层 (4 字):

2 纵向: 在应用层重定向浏览器流量，但不进行系统级加密 (4 字):

3 纵向: 通过网络活动记录来追踪用户的行踪或行为 (4 字):

5 纵向: 分布在多地、协同转发用户流量的一组服务器 (5 字):

检查点 6: 隐藏单词搜索

在下方网格中找出隐藏的 8 个关键词汇。单词可以是水平、垂直或对角线方向。

安 信 录 用 私 洋 公 踪 输 务 火 击 攻 协 护
统 火 全 共 服 安 管 名 网 击 私 商 服 器 安
身 络 私 访 输 身 户 风 户 络 统 域 务 数 理
营 网 络 护 址 隧 问 访 营 险 追 理 记 安 件
域 葱 器 域 葱 服 认 运 统 代 息 踪 系 火 密
管 洋 访 保 份 务 设 运 认 统 代 网 络 代 理
软 险 加 人 传 器 输 用 营 议 地 数 网 数 加
击 追 议 域 追 网 协 代 共 商 名 务 件 认 址
址 服 访 身 证 络 协 软 系 隐 追 证 证 件 备
地 理 共 公 护 据 传 软 险 接 管 踪 据 记 服
络 代 理 服 务 器 输 运 道 加 营 记 息 名 网
网 私 商 服 证 务 设 葱 系 据 隧 全 网 页 商
份 服 协 络 务 险 务 信 隐 访 服 备 代 件 认
用 访 管 营 传 信 设 览 户 络 络 理 设 攻 身
系 共 代 软 域 管 人 理 码 身 页 数 息 管 葱

词汇列表

洋葱网络 **网络地址** **服务器网络** **代理服务器** **网络追踪** **网页代理** **运营商追踪** **网络代理**

检查点 6 替代活动: 无障碍词汇配对

将词语搜索中的 8 个词汇与其正确的定义配对，在空白处写出字母（A-H）。

词汇术语
A. 洋葱网络
B. 网络地址
C. 服务器网络
D. 代理服务器
E. 网络追踪
F. 网页代理
G. 运营商追踪
H. 网络代理

定义与配对字段
1. 位于用户与目标网站之间负责转发请求的服务器。
2. 电信运营商对未加密上网流量目的地的记录。
3. 在应用层重定向浏览器流量，但不进行系统级加密。
4. 通过三台志愿者服务器路由数据，并在每一步加密一层。
5. 分布在多地、协同转发用户流量的一组服务器。
6. 替你的设备转发网络请求的中间节点。
7. 通过网络活动记录来追踪用户的行踪或行为。
8. 在互联网上标识设备接口的唯一数字标签。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的 VPN 概念和术语。把答案写在可填写的输入框中。

1. 网洋络葱 _____

2. 服络网器务 _____

3. 踪网追络 _____

4. 商踪追运营 _____

5. 址网地络 _____

6. 务代服器理 _____

7. 代网理页 _____

8. 网理代络 _____

附加活动: 快速思考

每个类别写出 3 个答案。最先填完列表的人获胜。

1	旅行时使用 VPN 的原因			
2	你知道的浏览器			
3	VPN 可以隐藏的内容			
4	与隐私相关的词语			
5	你想记住的本练习单中的词语			
6	网站可以根据你的 IP 推测出的信息			
7	IP 地址中的数字或符号			
8	关于 VPN 的误解			
9	你知道的 VPN 服务			
10	你的网络服务商能看到的内容			
11	优质 VPN 服务商作出的承诺			
12	可能泄露你真实 IP 的因素			
13	隐藏你所在位置的原因			
14	隐藏 IP 地址的方法			
15	可以使用 VPN 的设备			

检查点 8: VPN 案例研究

运用你所学的概念来解决下面的真实情景。

莎拉（咖啡馆学生）

👩‍💻 “嘿！我正坐在 Coffee & Bytes。这里有一个名为‘Free_Wi-Fi_No_Password’的不安全公共网络。我想登录学校邮箱并上传作业，但我担心黑客。不使用 VPN 而使用这个网络有哪些风险，VPN 又如何保护我的数据？”

ALEX（旅行学生）

👩‍💻 “糟糕！我因项目出国旅行，想观看托管在我祖国服务器上的一部生物纪录片。但网站显示‘此视频在你当前所在地区不可用。’我为什么被屏蔽，VPN 如何帮我观看？”

检查点 9: 破解密码

要完成你的 IP 隐藏训练，请解密这条关于隐藏数字痕迹的秘密信息。

汉字转数字加密密钥

运=1 数=2 据=3 你=4 器=5 密=6 地=7 加=8 藏=9 页=10
隐=11 务=12 代=13 葱=14 踪=15 营=16 追=17 络=18 网=19 商=20
理=21 统=22 全=23 用=24 服=25 址=26 系=27 安=28 洋=29 的=30

24	11	9	27	22		11	9		4	30	7	26

解码后的信息:

提示: 每个数字对应下方密钥中的一个汉字。

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: 网页代理能隐藏我的 IP 地址吗?

是的，但仅限通过它发送的流量，通常是你的浏览器。大多数网络代理不加密你的数据，因此你的 ISP 或网络运营商仍然可以看到你发送和接收的内容。

Q5: 隐藏我的 IP 合法吗?

在许多国家是合法的，但有些国家限制或禁止使用 VPN 以及其他用于隐藏 IP 地址的工具。隐藏 IP 并不会让违法行为变得合法，因此在使用之前请先查看当地法律。

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: Tor 能隐藏我的 IP 吗?

是的。Tor 将你的流量通过三个志愿者中继（入口、中间和出口）发送，因此网站看到的是出口中继的地址，而且没有任何单个中继同时知道你是谁以及你要去哪里。 [1]

Q7: 我的 IP 会泄露什么?

你的公网 IP 通常会暴露你的 ISP 和大致位置，例如你所在的国家或城市。网站还可以用它把你的多次访问关联起来，并实施地理封锁。

Q8: 我如何检查它是否已被隐藏?

连接到 VPN，然后访问 IP 检测网站并运行 DNS 和 WebRTC 泄漏测试。显示的 IP 和 DNS 服务器应属于 VPN，而不是你的 ISP。如果出现你的真实 IP，请开启泄漏防护。

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: 为什么在我隐藏 IP 地址后，网站仍然可以跟踪我?

隐藏 IP 并不能阻止浏览器指纹识别。跟踪者可以把屏幕分辨率、已安装字体和浏览器设置等细节组合成一个标识符，Cookie 或已登录的账户也可以识别你，因此还应使用注重隐私的浏览器。 [3]

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: IPv6 流量会泄漏我的真实 IP 地址吗?

是的，如果你的 VPN 只对 IPv4 建立隧道。这样你的设备可能会在隧道之外发送 IPv6 流量，暴露由 ISP 分配的地址。请使用对 IPv6 建立隧道或将其阻止的 VPN，并用 IPv6 泄漏测试加以确认。

Q5: 混淆如何绕过 VPN 封锁?

混淆（或称“隐身 VPN”）会伪装 VPN 流量数据包，使其看起来像普通的 HTTPS 网络流量（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: 分应用隧道会暴露我的真实 IP 地址吗?

是的，对于你排除的应用而言。隧道外发送的流量会使用你的真实 IP，而且 RFC 8828 指出，除非浏览器加以限制，否则 WebRTC 可能会暴露分流隧道 VPN 之下的 ISP 地址。 [2]

Q7: 什么是共享 IP 地址？它如何有助于保护隐私?

使用共享 IP 时，许多 VPN 用户会同时以同一个地址上线。这使网站比使用仅供你一人使用的专用 IP 时更难将某次访问与你联系起来。

Q8: 我的 ISP 能看出我在使用 VPN 来隐藏 IP 吗?

通常可以。你的 ISP 能看到你连接到某个 VPN 服务器的 IP 地址、连接时间以及发送了多少数据，但看不到你访问的网站或加密隧道内的内容。

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: 隐藏我的 IP，用代理还是 VPN 更好?

VPN 通常更好。它会对设备上的每个应用隐藏你的 IP 并加密流量，而网页代理通常只覆盖浏览器，而且往往不加密。

第 11 部分: 10 个有趣的 VPN 事实与现实洞察

回顾这些极具价值的、有关 VPN 历史、市场和技术的真实事实与见解。

1. 第一个 VPN 协议

PPTP（点对点隧道协议）是 1990 年代由 Microsoft 牵头的团体推出的早期 VPN 协议，现在被认为不安全，因此现代 VPN 使用 WireGuard 或 OpenVPN。

2. 指纹识别

隐藏 IP 并不能阻止浏览器指纹识别，它可以根据屏幕分辨率和已安装字体等细节识别出你。 [3]

3. WireGuard 革命

WireGuard 的代码库高度精简，注重效率，比传统协议更容易审计安全漏洞。

4. WebRTC 地址暴露

RFC 8828 警告说，除非浏览器加以限制，否则 WebRTC 可能会发现 VPN 的公网地址以及 VPN 所运行的 ISP 地址。 [2]

5. “五眼”联盟的起源

由美国、英国、加拿大、澳大利亚和新西兰组成的五眼情报合作关系，源于二战时期盟国之间的信号情报合作。

6. 深度包检测

高级防火墙部署深度包检测（DPI）来分析网络数据包元数据，并拦截标准 VPN 连接特征。

7. TOR 线路复用

Tor 会重复使用同一条线路约十分钟，然后建立新线路，这使你的浏览活动更难被关联起来。 [1]

8. 去中心化 VPN

去中心化 VPN (dVPN) 将流量分散到由对等方运行的节点网络中，减少对单一中心化提供商的依赖。

9. TOR 与 VPN 的匿名性

VPN 通过单一提供商传输流量，而 Tor（洋葱路由器）通过三个志愿者中继节点（入口、中间、出口）发送流量，以最大限度地保护隐私。 [1]

10. 代理与 VPN 隧道

网页代理会改变网站看到的你浏览器流量的 IP 地址，但与 VPN 不同，它通常不会加密该流量，也不会覆盖设备上的其他应用。 [5]

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] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

答案: 隐藏 IP 地址、位置伪装、代理、Tor 以及防止 DNS/WebRTC 泄露

1 问题 1

正确答案: B

教学提示

设备的公共 IP 地址会向你访问的网站透露什么？ → 你的大致位置和 ISP 的名称

2 VPN 系统加密

延迟

正确答案: C

教学提示

与只重定向浏览器流量的代理不同，VPN 会创建覆盖整个系统的加密隧道，保护后台应用、游戏和操作系统查询。引用: Tor Project Relays, W3C WebRTC API。

3 代理缺少加密

WI-FI 安全

正确答案: A

教学提示

网络代理只转发浏览器流量，不加密数据包内容，这意味着你的网络运营商或 ISP 仍可追踪你的内容流量。引用: IETF Proxy Vulnerabilities。

4 问题 4

正确答案: B

教学提示

Tor 网络如何为用户提供高度匿名性？ → 通过三个由志愿者运营的中继节点路由流量

5 DNS 隧道泄漏

隐私

正确答案: B

教学提示

当域名解析请求绕过 VPN 隧道、直接发送到你的 ISP 的解析器时，就会发生 DNS 泄漏，从而暴露你访问过的域名记录。引用: DNSSEC Tunnel Testing，EFF Tracking Evasion。

答案: 检查点 2 – 判断题（正确或错误）

6 **代理限制详情** IP 伪装 正确答案: 错误

教学提示

代理在应用层运行，缺少 VPN 隧道那样的系统级网络驱动程序集成。 引用: IETF Proxy Vulnerabilities。

7 **问题 7** 正确答案: 正确

教学提示

通过三个志愿者中继节点转发流量并进行分层加密会增加延迟，因此 Tor 通常比直接连接慢。

8 **问题 8** 正确答案: 正确

教学提示

WebRTC 可能泄露本地地址，在某些 VPN 设置下还会泄露隧道下方由 ISP 分配的公共 IP（RFC 8828）。

9 **问题 9** 正确答案: 正确

教学提示

没有 DNS 或 WebRTC 泄漏时，ISP 只能看到前往 VPN 服务器的加密流量，而看不到你访问的网站。

10 **指纹识别的局限** 无日志 正确答案: 错误

教学提示

指纹识别针对设备配置指标（屏幕分辨率、字体、插件），即使隐藏了 IP，这些指标仍然可见。引用: EFF Tracking Evasion。

词汇答案与评分标准

教师评分标准: 每个正确配对得 1 分（共 8 分），每个语境术语得 1 分（共 6 分）。

检查点 4: 答案 – 概念配对

D 1. IP 地址	A 2. VPN 隧道	B 3. Tor 网络	E 4. 网络代理
G 5. DNS 泄露	H 6. WebRTC API	C 7. 位置掩蔽	F 8. ISP 跟踪

检查点 3: 答案 – 关键术语

1 域名泄漏	2 实时	3 代理	4 洋葱
5 网络地址	6 位置		

检查点 6 替代活动: 答案 – 词语配对

1 D – 代理服务器	2 G – 运营商追踪	3 F – 网页代理	4 A – 洋葱网络
5 C – 服务器网络	6 H – 网络代理	7 E – 网络追踪	8 B – 网络地址

教师讨论提示

关键术语:
检查学生能否用自己的话解释IP 地址、VPN 隧道和Tor 网络，并为每个术语举例。

案例研究:
请学生用练习单中的事实而不是个人观点来支持自己的建议。

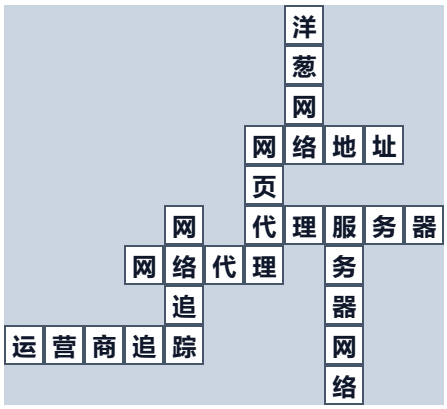
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

安	信	录	用	私	洋	公	踪	输	务	火	击	攻	协	护
统	火	全	共	服	安	管	名	网	击	私	商	服	器	安
身	络	私	访	输	身	户	风	户	络	统	域	务	数	理
营	网	络	护	址	隧	问	访	营	险	追	理	记	安	件
域	葱	器	域	葱	服	认	运	统	代	息	踪	系	火	密
管	洋	访	保	份	务	设	运	认	统	代	网	络	代	理
软	险	加	人	传	器	输	用	营	议	地	数	网	数	加
击	追	议	域	追	网	协	代	共	商	名	务	件	认	址
址	服	访	身	证	络	协	软	系	隐	追	证	证	件	备
地	理	共	公	护	据	传	软	险	接	管	踪	据	记	服
络	代	理	服	务	器	输	运	道	加	营	记	息	名	网
网	私	商	服	证	务	设	葱	系	据	隧	全	网	页	商
份	服	协	络	务	险	务	信	隐	访	服	备	代	件	认
用	访	管	营	传	信	设	览	户	络	络	理	设	攻	身
系	共	代	软	域	管	人	理	码	身	页	数	息	管	葱

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 网络地址 在互联网上标识设备接口的唯一数字标签 (4 字)

4 横向: 代理服务器 位于用户与目标网站之间负责转发请求的服务器 (5 字)

6 横向: 网络代理 替你的设备转发网络请求的中间节点 (4 字)

7 横向: 运营商追踪 电信运营商对未加密上网流量目的地的记录 (5 字)

纵向

1 纵向: 洋葱网络 通过三台志愿者服务器路由数据，并在每一步加密一层 (4 字)

2 纵向: 网页代理 在应用层重定向浏览器流量，但不进行系统级加密 (4 字)

3 纵向: 网络追踪 通过网络活动记录来追踪用户的行踪或行为 (4 字)

5 纵向: 服务器网络 分布在多地、协同转发用户流量的一组服务器 (5 字)

乱序单词与密码答案

词汇还原练习和秘密密码挑战的评分答案。

汉字重组答案

1. 网洋络葱 — **洋葱网络**
2. 服络网器务 — **服务器网络**
3. 踪网追络 — **网络追踪**
4. 商踪追运营 — **运营商追踪**
5. 址网地络 — **网络地址**
6. 务代服器理 — **代理服务器**
7. 代网理页 — **网页代理**
8. 网理代络 — **网络代理**

秘密密码挑战答案

“用隐藏系统隐藏你的地址”

案例研究答案

A 情景 A: 公共网络安全

嗅探与加密 莎拉的困境

评分指南

学生的回答应涵盖以下要点:

- 风险: 数据包嗅探、数据拦截和中间人攻击。同一咖啡馆网络上的人可能会截获她的登录信息或作业文件。
- VPN 保护: 加密网络数据包的有效载荷，在 VPN 配置正确时，使被拦截的隧道流量对被动的本地网络窥探者不可读。

B 情景 B: 访问被屏蔽的资源

地理封锁与 IP Alex 的两难处境

评分指南

学生的回答应涵盖以下要点:

- 被阻止的原因: 流媒体主机使用地域封锁，它将旅行者的本地 IP 地址映射到其所在的实际国家，并依据地域版权许可予以阻止。
- VPN 如何提供帮助: 通过位于他本国的服务器路由流量来隐藏他的真实位置。网站看到的是本国 IP，因此可以访问。