姓名: _____ 日期: _____ 得分: _____

WireGuard 与 OpenVPN 对比练习单

比较 WireGuard 和 OpenVPN 协议、代码库规模、速度和加密标准

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

- 比较各协议的代码库复杂度和审计速度。
- 分析在内核空间运行所带来的性能提升。
- 对比 OpenSSL 加密算法与 WireGuard 的现代密码学。
- 为对等端握手设置公钥和私钥对。
- 通过 TCP 和 UDP 防火墙端口路由 VPN 流量。

协议对比练习单说明

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。将所学知识应用于审计现代协议。最后完成附加活动: 快速思考。

WIREGUARD 与 OPENVPN 对比（简介）

选择 VPN 协议需要在速度和配置选项之间取得平衡。OpenVPN 数十年来一直是标准，提供灵活的 TCP/UDP 配置。WireGuard 是一种现代替代方案，直接在内核空间运行，只有 4,000 行代码。了解协议之间的差异是优化你的安全网络的关键。

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. WireGuard 协议的代码库大约有多大?
   - A. 大约 70,000 行
   - B. 超过 100,000 行
   - C. 少于 1,000 行
   - D. 约 4,000 行

2. WireGuard 在操作系统的哪个空间中运行?
   - A. 用户空间
   - B. 内核空间
   - C. 应用空间
   - D. 虚拟空间

3. OpenVPN 主要依赖哪个加密库?
   - A. ChaCha20-Poly1305
   - B. OpenSSL 加密库
   - C. Noise 协议框架
   - D. 明文 DES 编码

4. 与 OpenVPN 相比，WireGuard 的一个主要性能优势是什么?
   - A. 更快的连接握手和更低的延迟
   - B. 无需使用公共 IP 地址
   - C. 对传统拨号上网的内置原生支持
   - D. 在移动设备上零电量开销

5. WireGuard 如何验证对端连接?
   - A. 通过交换标准用户密码
   - B. 验证域名注册证书
   - C. 通过使用静态的公钥和私钥对
   - D. 通过检查硬件序列号

检查点 2: 判断正误挑战

6 问题 6

6. WireGuard 紧凑的代码库使其审计起来容易得多。

○ 正确 ○ 错误

7 问题 7

7. OpenVPN 通常比 WireGuard 更快，因为它运行在内核空间。

○ 正确 ○ 错误

8 问题 8

8. OpenVPN 高度可配置，同时支持 UDP 和 TCP 协议。

○ 正确 ○ 错误

9 问题 9

9. WireGuard 使用 ChaCha20 等现代加密技术实现快速的数据包加密。

○ 正确 ○ 错误

10 问题 10

10. WireGuard 需要复杂的证书颁发机构设置才能进行身份验证。

○ 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. 现代的 _____ 协议直接在操作系统内核中运行。
2. 传统的 _____ 协议依赖 OpenSSL 加密库。
3. 在 _____ 中执行代码可减少上下文切换开销。
4. OpenVPN 在 _____ 中运行，通过虚拟接口路由数据包。
5. WireGuard 使用公钥和私钥 _____ 来识别连接对端。
6. 较小的代码量可提高软件的安全 _____ 。

词汇词库

传输协议　可审计性　密钥对　内核空间　用户空间　OPENSSL　OpenVPN　WireGuard

在此写下你的答案:

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

检查点 4: 网络概念配对

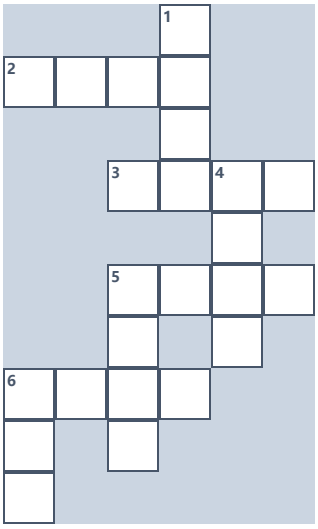
定义配对

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. WireGuard	A	OpenVPN 运行的执行区域，会产生上下文切换开销。
	2. OpenVPN	B	WireGuard 代码库体积小巧，因此更容易审计。
	3. 内核空间	C	OpenVPN 依赖的加密算法密码库。
	4. 用户空间	D	OpenVPN 支持的传输协议；WireGuard 本身仅通过 UDP 运行。
	5. 4,000 行	E	WireGuard 为提升速度而运行的操作系统执行区域。
	6. OpenSSL	F	WireGuard 用来验证对等连接的非对称令牌。
	7. 密钥对	G	为高速度和简单代码审计而设计的现代 VPN 协议。
	8. TCP/UDP	H	稳健的传统协议，使用庞大而复杂的配置代码库。

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. OpenVPN 支持的传输层协议；WireGuard 本身仅运行在 UDP 上 (4)

3. 用尽量少的代码实现功能，便于审查 (4)

5. 在操作系统内核中运行的程序代码 (4)

6. OpenVPN 运行的执行区域，会带来上下文切换开销 (4)

纵向

1. 实现某一通信协议的程序代码 (4)

4. WireGuard 代码库体积小巧，因此更容易审计 (4)

5. WireGuard 为提速而运行的操作系统执行区域 (4)

6. 程序在受限权限下运行的操作系统层面 (3)

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: OpenVPN 支持的传输层协议；WireGuard 本身仅运行在 UDP 上 (4 字):

3 横向: 用尽量少的代码实现功能，便于审查 (4 字):

5 横向: 在操作系统内核中运行的程序代码 (4 字):

6 横向: OpenVPN 运行的执行区域，会带来上下文切换开销 (4 字):

纵向

1 纵向: 实现某一通信协议的程序代码 (4 字):

4 纵向: WireGuard 代码库体积小巧，因此更容易审计 (4 字):

5 纵向: WireGuard 为提速而运行的操作系统执行区域 (4 字):

6 纵向: 程序在受限权限下运行的操作系统层面 (3 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。

全 地 共 安 信 记 用 私 录 公 内 传 务 火 击
险 协 护 系 防 全 公 服 传 安 管 名 攻 私 简
服 简 器 安 身 隐 访 传 证 输 户 份 户 统 域
务 精 数 管 精 络 护 址 隧 问 协 接 精 风 管
览 码 安 软 址 用 器 域 态 认 代 议 系 间 息
系 代 防 密 备 户 访 精 保 身 设 墙 系 空 统
风 加 共 理 传 空 用 议 简 地 数 网 数 加 攻
间 议 域 间 协 间 空 公 名 代 务 件 认 址 服
码 访 身 证 协 统 击 护 认 认 码 软 设 理 共
代 公 护 据 理 统 风 连 管 数 览 服 传 代 隧
议 内 核 空 间 加 精 览 息 名 私 简 服 证 用
协 务 件 态 内 击 据 人 全 网 简 份 服 户 协
络 务 风 务 核 户 隐 访 服 设 软 墙 态 用 访
备 精 传 信 代 件 浏 户 络 络 件 攻 证 击 公
间 统 域 备 码 共 管 码 证 核 数 息 管 态 录

词汇列表

用户态 **用户空间** **内核空间** **内核代码** **精简代码** **代码精简** **协议代码** **传输协议**

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. 用户态
B. 用户空间
C. 内核空间
D. 内核代码
E. 精简代码
F. 代码精简
G. 协议代码
H. 传输协议

定义与配对字段
1. 用尽量少的代码实现功能，便于审查。
2. WireGuard 为提速而运行的操作系统执行区域。
3. OpenVPN 运行的执行区域，会带来上下文切换开销。
4. 实现某一通信协议的程序代码。
5. OpenVPN 支持的传输层协议；WireGuard 本身仅运行在 UDP 上。
6. WireGuard 代码库体积小巧，因此更容易审计。
7. 程序在受限权限下运行的操作系统层面。
8. 在操作系统内核中运行的程序代码。

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. 户 态 用 _____

2. 内 空 间 核 _____

3. 码 精 代 简 _____

4. 码 代 协 议 _____

5. 间 用 空 户 _____

6. 代 码 内 核 _____

7. 精 代 简 码 _____

8. 传 议 协 输 _____

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	选择 WireGuard 的原因			
2	优质 VPN 服务商作出的承诺			
3	选择 OpenVPN 的原因			
4	旅行时使用 VPN 的原因			
5	你的网络服务商能看到的内容			
6	识别虚假 Wi-Fi 网络的方法			
7	关于 VPN 的误解			
8	你会使用 VPN 的场合			
9	日常生活中快速的事物			
10	VPN 无法保护你免受的威胁			
11	使代码更易于检查的因素			
12	VPN 可以隐藏的内容			
13	WireGuard 与 OpenVPN 的区别			
14	与隐私相关的词语			
15	你知道的加密算法名称			

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！我正在咖啡馆用 Wi-Fi，我的 VPN 应用可以让我选择 WireGuard 或 OpenVPN。我在咖啡馆网络和手机热点之间走动时，视频通话总是中断。我应该选哪个协议，为什么它能更好地处理这种切换？”

ALEX（旅行学生）

👩‍💻 “我在国外的酒店网络上，该网络似乎屏蔽了大部分 VPN 流量。WireGuard 根本连不上，但我需要访问家乡学校的资源。可能是什么被屏蔽了，OpenVPN 如何帮助我突破？”

检查点 9: 破解密码

要完成你的协议审计训练，请解密这条关于内核空间执行的隐藏信息。

汉字转数字加密密钥

级=1 代=2 快=3 精=4 内=5 议=6 户=7 道=8 核=9 数=10

简=11 空=12 更=13 码=14 的=15 络=16 开=17 你=18 态=19 网=20

全=21 隧=22 源=23 间=24 传=25 输=26 升=27 用=28 安=29 协=30

27	1	18	15	17	23	30	6	13	3	22	8

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: 协议为什么重要?

协议决定你的 VPN 如何建立隧道、用哪种加密技术保护你的数据，以及连接和重新连接的速度。WireGuard 和 OpenVPN 是大多数 VPN 应用提供的两种开源协议，它们在简洁性、速度和可配置性之间做出了不同的取舍。

Q3: 其中一个比另一个更私密吗?

两种协议都不能让你匿名。两者都使用强密码算法加密隧道流量；你的隐私主要取决于 VPN 提供商记录什么，以及它如何管理密钥、账户和服务器。

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: 两者都是开源的吗?

是的。WireGuard 和 OpenVPN 社区版都公开其源代码，因此独立研究人员可以审查。WireGuard 的代码库很小，使完整审查快得多。

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: 哪一个更快?

WireGuard 通常更快: 它在内核中运行，使用精简的 ChaCha20-Poly1305 加密，并能快速完成握手。OpenVPN 的开销更大，但实际速度还取决于服务器负载和距离。

Q7: 两者都可以通过 TCP 和 UDP 运行吗?

不是。OpenVPN 可以通过 UDP 或 TCP 运行，TCP 模式有助于在阻止 UDP 的网络上使用。WireGuard 仅通过 UDP 发送数据包，因此在只允许 TCP 的网络上可能无法工作。 [4]

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: 我可以在手机上使用 WireGuard 和 OpenVPN 吗?

是的。WireGuard 是跨平台的，提供 Windows、macOS、Linux、iOS 和 Android 应用，同样的系统上也有 OpenVPN 客户端。大多数 VPN 应用都允许你选择其中任意一种。 [1]

Q10: WireGuard 为什么这么小?

WireGuard 只支持一套固定的现代密码算法，而不是提供多种选项。它在 Linux 上的实现不到 4,000 行代码，因此比更大的 VPN 代码库更容易审计。 [3]

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。

Q2: WireGuard 使用哪些密码算法?

WireGuard 使用 ChaCha20 与 Poly1305 进行加密，使用 Curve25519 进行密钥交换，使用 BLAKE2s 进行哈希，并使用 Noise 框架完成握手。它没有密码算法协商，因此用户不会选到薄弱的选项。 [2]

Q3: OpenVPN 可以使用哪些密码算法和库?

OpenVPN 与 OpenSSL 库紧密集成，并使用 TLS 交换密钥。管理员可以选择 AES-256-GCM 等数据通道加密算法，这增加了灵活性，但也为薄弱设置留下了空间。 [4]

Q4: 每种协议如何对对端进行身份验证?

WireGuard 对等节点通过静态公钥相互识别，很像交换 SSH 密钥，每个密钥对应允许的隧道 IP。OpenVPN 通常依赖带有 X.509 证书的证书颁发机构，并常与用户名和密码结合使用。

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: 当我从 Wi-Fi 切换到移动网络时会发生什么?

WireGuard 是无连接的：它从新地址发送数据包，经过一次快速握手后隧道即可继续运行。OpenVPN 会保持会话状态，因此网络变化可能需要重新连接，耗时稍长。

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: 如果 WireGuard 更快，OpenVPN 仍然是个好选择吗?

是的。OpenVPN 成熟且部署广泛，在 UDP 被阻止时可通过 TCP 运行，并支持基于证书的企业部署。许多服务商同时提供两种协议，因此当其中一种被阻止或较慢时，用户可以切换。

Q9: 它们使用哪些端口?

OpenVPN 的标准端口是 1194，但可以移到任何 UDP 或 TCP 端口，包括 443。WireGuard 监听配置中设置的 UDP 端口；51820 是其官方示例中使用的端口。

Q10: 哪种协议更容易手动设置?

WireGuard 通常更简单: 生成一对密钥，交换公钥并列出允许的 IP。OpenVPN 需要证书、CA 和更多选项，不过 .ovpn 配置文件会把它们打包成一个文件。

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）由包括 Microsoft 在内的厂商联盟开发，并于 1999 年 7 月以 RFC 2637 发布，用于支持远程访问 VPN。 [6]

2. 两种传输方式

OpenVPN 可以通过 UDP 或 TCP 承载其隧道，在 TLS 模式下其控制通道和数据通道共用同一个端口。 [4]

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。 [3]

4. 现代密码学

WireGuard 在 Noise 协议框架内结合了 ChaCha20、Poly1305、Curve25519、BLAKE2s、SipHash24 和 HKDF，用户无需选择密码算法，也就不会选错。 [2]

5. OpenVPN 内部的 OPENSSL

OpenVPN 与 OpenSSL 库紧密集成，其许多加密功能均源自该库，包括用于交换密钥的 TLS。 [4]

6. 深度包检测

深度数据包检测 (DPI) 会检查数据包内容和流量模式，而不仅仅是包头，一些防火墙会用它来检测并拦截常见的 VPN 协议。

7. SSH 式密钥

WireGuard 连接通过交换简单的公钥来建立，很像交换 SSH 密钥，无需证书颁发机构。 [1]

8. 跨平台

WireGuard 最初为 Linux 内核发布，现已支持 Windows、macOS、BSD、iOS 和 Android，因此同一种协议可在大多数设备上使用。 [1]

9. 前向保密

WireGuard 每隔几分钟重复一次 Noise_IK 握手以轮换对称会话密钥，即使长期密钥日后泄露，也能提供完美前向保密。 [2]

10. TUN/TAP 接口

OpenVPN 设计用于配合 TUN/TAP 虚拟网络接口，该接口在大多数平台上都可用，并承载隧道的数据包。 [4]

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

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

[3] 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/

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

[5] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

答案: 比较 WireGuard 和 OpenVPN 协议、代码库大小、速度以及加密标准

1 **WireGuard 代码量** 协议 正确答案: D

教学提示

WireGuard 极其精简，仅约 4,000 行代码。这使攻击面保持较小，也更便于审计。引用: WireGuard Project。

2 **内核空间速度** 延迟 正确答案: B

教学提示

通过直接在内核空间中执行，WireGuard 避免了上下文切换开销，从而实现高吞吐量。引用：WireGuard Project。

3 **问题 3** 正确答案: B

教学提示

OpenVPN 与 OpenSSL 紧密集成，后者提供 AES-GCM 等加密算法，使其高度可配置，但也更复杂。

4 **协议性能** 路由控制 正确答案: A

教学提示

WireGuard 能在几毫秒内建立握手，并对网络漫游（如从 Wi-Fi 切换到蜂窝网络）即时响应。引用: Microsoft Native Gateway, Apple Support。 [3]

5 **非对称加密** 隐私 正确答案: C

教学提示

WireGuard 使用加密密钥路由（Cryptokey Routing），将公钥与允许的隧道 IP 地址关联，类似于 SSH 设置配置。引用: WireGuard Project。

答案: 检查点 2 – 判断题（正确或错误）

6 问题 6

正确答案: 正确

教学提示

WireGuard 的 Linux 实现不到 4,000 行，因此安全团队审查它的速度比 OpenVPN 等大得多的 VPN 代码库快得多。

7 用户空间延迟

速度

正确答案: 错误

教学提示

OpenVPN 运行在用户空间，在内核虚拟接口之间来回传递数据包，这会增加上下文切换开销（除非使用 OpenVPN DCO 等内核卸载）。 引用: DD-WRT custom firmware。

8 OpenVPN 配置

嗅探风险

正确答案: 正确

教学提示

OpenVPN 支持通过 TCP（用于可靠性/绕过防火墙）或 UDP（用于速度）运行，使其能兼容复杂的企业防火墙。 引用: IETF Cryptographic Protocols。

9 现代密码学

防火墙

正确答案: 正确

教学提示

WireGuard 舍弃传统密码算法，转而采用 ChaCha20 和 Poly1305 等现代安全原语，它们在移动 CPU 上运行很快。引用: WireGuard Project。

10 密钥对简化

无日志

正确答案: 错误

教学提示

WireGuard 不使用证书或复杂的 CA 层级结构；它依赖对等节点之间交换的简单公钥/私钥对。引用: WireGuard Project。

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

G 1. WireGuard	H 2. OpenVPN	E 3. 内核空间	A 4. 用户空间
B 5. 4,000 行	C 6. OpenSSL	F 7. 密钥对	D 8. TCP/UDP

检查点 3: 答案 – 关键术语

1 WireGuard	2 OpenVPN	3 内核空间	4 用户空间
5 密钥对	6 可审计性		

检查点 6 替代活动: 答案 – 词语配对

1 F – 代码精简	2 C – 内核空间	3 B – 用户空间	4 G – 协议代码
5 H – 传输协议	6 E – 精简代码	7 A – 用户态	8 D – 内核代码

教师讨论提示

关键术语:
检查学生能否用自己的话解释WireGuard、OpenVPN和内核空间，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。

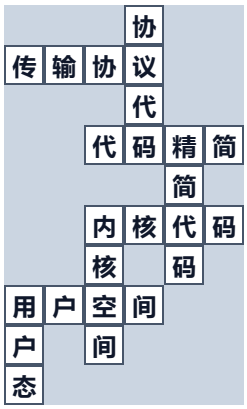
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	地	共	安	信	记	用	私	录	公	内	传	务	火	击
险	协	护	系	防	全	公	服	传	安	管	名	攻	私	简
服	简	器	安	身	隐	访	传	证	输	户	份	户	统	域
务	精	数	管	精	络	护	址	隧	问	协	接	精	风	管
览	码	安	软	址	用	器	域	态	认	代	议	系	间	息
系	代	防	密	备	户	访	精	保	身	设	墙	系	空	统
风	加	共	理	传	空	用	议	简	地	数	网	数	加	攻
间	议	域	间	协	间	空	公	名	代	务	件	认	址	服
码	访	身	证	协	统	击	护	认	认	码	软	设	理	共
代	公	护	据	理	统	风	连	管	数	览	服	传	代	隧
议	内	核	空	间	加	精	览	息	名	私	简	服	证	用
协	务	件	态	内	击	据	人	全	网	简	份	服	户	协
络	务	风	务	核	户	隐	访	服	设	软	墙	态	用	访
备	精	传	信	代	件	浏	户	络	络	件	攻	证	击	公
间	统	域	备	码	共	管	码	证	核	数	息	管	态	录

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 传输协议 OpenVPN 支持的传输层协议；WireGuard 本身仅运行在 UDP 上 (4 字)

3 横向: 代码精简 用尽量少的代码实现功能，便于审查 (4 字)

5 横向: 内核代码 在操作系统内核中运行的程序代码 (4 字)

6 横向: 用户空间 OpenVPN 运行的执行区域，会带来上下文切换开销 (4 字)

纵向

1 纵向: 协议代码 实现某一通信协议的程序代码 (4 字)

4 纵向: 精简代码 WireGuard 代码库体积小巧，因此更容易审计 (4 字)

5 纵向: 内核空间 WireGuard 为提速而运行的操作系统执行区域 (4 字)

6 纵向: 用户态 程序在受限权限下运行的操作系统层面 (3 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. 户 态 用 — **用户态**
2. 内 空 间 核 — **内核空间**
3. 码 精 代 简 — **精简代码**
4. 码 代 协 议 — **协议代码**
5. 间 用 空 户 — **用户空间**
6. 代 码 内 核 — **内核代码**
7. 精 代 简 码 — **代码精简**
8. 传 议 协 输 — **传输协议**

秘密密码挑战答案

“升级你的开源协议更快隧道”

案例研究答案

A 情景 A: 选择协议

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:

- 建议: WireGuard。其轻量级的无连接设计使隧道在她的网络发生变化时能够快速恢复，而 ChaCha20-Poly1305 则能保持较快的加密速度。
- 安全性: 两种协议都会加密她在咖啡馆 Wi-Fi 上的流量，因此只要配置正确，两者都能保护她的登录信息；选择主要影响速度和稳定性。

B 情景 B: 突破 VPN 屏蔽

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: WireGuard 仅使用 UDP，而酒店防火墙很可能阻止 UDP，或通过过滤或深度包检测识别出 WireGuard 数据包。
- OpenVPN 如何提供帮助: 它可以通过 TCP 运行，包括 HTTPS 使用的 443 端口；由于网页浏览依赖该端口，酒店防火墙很少会彻底阻止它。