姓名: _____ 日期: _____ 得分: _____

Surfshark 安全性

研究 Surfshark 的安全功能，包括 CleanWeb 广告拦截、MultiHop 动态路由、Nexus SDN 架构、纯内存服务器群和 Camouflage 模式。

SURFSHARK 安全学习概览

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Surfshark 的安全架构。你将探索纯内存（RAM-only）服务器硬件、Nexus SDN 动态 IP 轮换、CleanWeb 广告拦截器和 MultiHop 路由。

练习单检查点

- [ ] **第 1-4 部分: 掌握 VPN 和网络安全配置。**
- [ ] **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 最佳 VPN 指南

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

你的 Surfshark 安全学习路线图

- 分析 Surfshark 安全性的技术架构和配置规则。
- 配置客户端设置，防止 IP、DNS 和 WebRTC 流量泄漏。
- 将自定义定价、试用和性能功能与标准模式进行比较。

SURFSHARK 安全指南说明

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。将所学知识应用于仅内存（RAM-only）基础设施、Nexus SDN 和 CleanWeb。 最后完成附加活动: 快速思考。

纯内存服务器集群、Nexus SDN 与 CleanWeb 架构（简介）

Surfshark 通过全 RAM 服务器群、带 IP Rotator 的 Nexus 软件定义网络、CleanWeb 广告拦截和 Dynamic MultiHop 加密路径来保护用户隐私。

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 1. Surfshark 集成的广告与恶意软件拦截器叫什么名称?

- A) AdGuard
- B) CleanWeb
- C) ThreatShield
- D) NetBlocker

2 2. Surfshark 的所有服务器使用哪种硬件架构?

- A) 机械硬盘
- B) 100% 仅内存（RAM-Only）
- C) 光存储
- D) 磁带

3 3. 哪项功能通过两个不同的 VPN 服务器路由流量?

- A) Bypasser
- B) MultiHop（双重 VPN）
- C) Nexus 网络
- D) 静态 IP

4 4. 哪项混淆功能可将 VPN 流量伪装成普通网页数据?

- A) 断网保护（Kill Switch）
- B) 伪装模式
- C) CleanWeb 2.0
- D) 分应用隧道

5 5. Surfshark Bypasser 工具有什么作用?

- A) Speed Booster
- B) 分应用隧道
- C) 密码管理器
- D) DNS 解析器

检查点 2: 判断正误挑战

6 问题 6

6. 纯内存服务器在重启后会立即清除所有运行数据。

○ 正确 ○ 错误

7 问题 7

7. 伪装模式可防止 ISP 检测到你正在使用 VPN。

○ 正确 ○ 错误

8 问题 8

8. CleanWeb 2.0 在浏览器扩展中运行，以拦截 Cookie 同意弹窗。

○ 正确 ○ 错误

9 问题 9

9. Surfshark 保留临时的连接时间戳和带宽使用日志。

○ 正确 ○ 错误

10 问题 10

10. Nexus 网络会定期轮换用户 IP 地址，而不会断开连接。

○ 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. 恼人的网页广告、追踪脚本和钓鱼链接会被 _____ 过滤器拦截。
2. 因为服务器在 _____ 内存中运行，用户活动不会留下任何取证痕迹。
3. 通过两个独立的加密服务器跳转来路由数据，是由 _____ 隧道实现的。
4. 为向互联网服务提供商隐藏 VPN 的使用，用户启用 _____ 模式。
5. 允许银行应用绕过 VPN 隧道由 _____ 设置来管理。
6. 连接服务器集群的新一代软件定义网络架构是 _____ 系统。

词汇词库

多跳连接　解析服务器　仅内存　净网过滤　联结网络　绕过器　网络泄漏　伪装

在此写下你的答案:

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

检查点 4: VPN 与网络概念配对

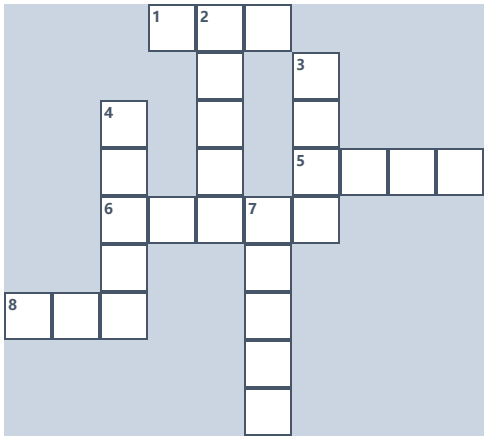
定义配对

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. 服务器网络	**A**	在 VPN 中断时阻止网络流量的自动安全功能。
	2. 联结网络	**B**	允许部分应用绕过 VPN 的分应用隧道功能。
	3. 多跳	**C**	拦截广告、恶意软件和 Cookie 同意横幅的高级过滤器。
	4. 仅内存	**D**	每次断电重启都会清除所有数据的易失性内存服务器硬件。
	5. 绕过工具	**E**	定期更改你的外部 IP 地址而不中断隧道的功能。
	6. 内存服务器	**F**	隐藏 VPN 特征、模仿常规 HTTPS 流量的混淆技术。
	7. Nexus 网络	**G**	一种双重 VPN 路由功能，通过两个不同的服务器节点加密流量。
	8. 轮换	**H**	将所有服务器连接成统一网状结构的专有软件定义网络。

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

1. 每次断电都会清除所有数据的易失性内存服务器硬件 (3)

5. 本应受保护的网络信息意外暴露在隧道之外 (4)

6. 分布在多地、协同转发用户流量的一组服务器 (5)

8. 让选定应用绕过 VPN 的分流隧道功能 (3)

纵向

2. 只把数据放在易失性内存中、断电即清空的服务器 (5)

3. 把所有服务器连接成统一网状结构的专有软件定义网络 (4)

4. 负责把域名转换为地址的服务器 (5)

7. 设在网络边界、过滤进出流量的防护系统 (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

1 横向: 每次断电都会清除所有数据的易失性内存服务器硬件 (3 字):

5 横向: 本应受保护的网络信息意外暴露在隧道之外 (4 字):

6 横向: 分布在多地、协同转发用户流量的一组服务器 (5 字):

8 横向: 让选定应用绕过 VPN 的分流隧道功能 (3 字):

纵向

2 纵向: 只把数据放在易失性内存中、断电即清空的服务器 (5 字):

3 纵向: 把所有服务器连接成统一网状结构的专有软件定义网络 (4 字):

4 纵向: 负责把域名转换为地址的服务器 (5 字):

7 纵向: 设在网络边界、过滤进出流量的防护系统 (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 息 结 用 连 结 人 存 公 务 墙 统 击 议 隐
软 器 墙 全 人 服 安 传 网 协 系 私 过 务 器
安 务 份 私 问 公 份 信 险 络 户 软 名 务 数
传 服 绕 络 隐 域 浏 地 访 绕 泄 攻 传 录 安
设 存 名 器 名 服 析 证 漏 软 仅 漏 保 软 墙
密 内 理 问 保 务 风 网 管 认 软 绕 过 器 仅
件 攻 加 道 输 器 共 用 络 防 址 数 网 数 加
系 内 防 名 内 网 议 仅 隧 防 协 务 备 证 域
络 务 问 份 身 络 议 件 统 隐 火 身 身 设 管
网 输 隧 人 护 加 输 件 攻 接 传 墙 据 联 服
结 解 析 服 务 器 公 漏 览 加 绕 联 保 协 仅
联 私 过 服 身 务 备 析 统 加 道 数 网 内 过
风 服 议 络 务 攻 务 信 私 问 服 管 存 设 证
用 问 传 绕 公 信 备 记 户 络 络 备 击 份 统
隧 仅 件 名 理 隧 传 码 份 泄 数 保 传 析 结

词汇列表

服务器网络 **联结网络** **解析服务器** **仅内存绕过器** **网络防火墙** **内存服务器** **网络泄漏**

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. 服务器网络
B. 联结网络
C. 解析服务器
D. 仅内存
E. 网络防火墙
F. 内存服务器
G. 网络泄漏
H. 绕过器

定义与配对字段
1. 每次断电都会清除所有数据的易失性内存服务器硬件。
2. 只把数据放在易失性内存中、断电即清空的服务器。
3. 分布在多地、协同转发用户流量的一组服务器。
4. 设在网络边界、过滤进出流量的防护系统。
5. 把所有服务器连接成统一网状结构的专有软件定义网络。
6. 让选定应用绕过 VPN 的分流隧道功能。
7. 负责把域名转换为地址的服务器。
8. 本应受保护的网络信息意外暴露在隧道之外。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的虚拟专用网络（VPN）概念和术语。把答案写在提供的输入框中。

1. 网器服络务 _____

2. 解器务服析 _____

3. 防网墙火络 _____

4. 漏泄网络 _____

5. 络联网结 _____

6. 内存仅 _____

7. 务器内服存 _____

8. 器过绕 _____

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	Surfshark 中的安全功能			
2	VPN 连接速度慢的迹象			
3	你知道的 VPN 协议			
4	加密所保护的内容			
5	公共 Wi-Fi 上的威胁			
6	以严格隐私法律闻名的国家			
7	设置强密码的方法			
8	你会安装 Surfshark 的设备			
9	可以向 Surfshark 客服提出的问题			
10	为增强安全而开启的设置			
11	Surfshark 可以对你的网络隐藏的内容			
12	VPN 泄漏的类型			
13	VPN 绝不应该存储的数据			
14	形容好用 VPN 应用的词语			
15	审计可以检查的内容			

检查点 8: VPN 与网络案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: 绕过校园和工作场所过滤



情景: 一名学生发现其大学校园 Wi-Fi 屏蔽了所有标准的 OpenVPN 和 WireGuard 端口。

讨论问题: Surfshark 的哪项功能可让这名学生在不被网络管理员察觉的情况下连接?

案例研究 2: 高风险新闻调查



情景: 一名调查记者在研究敏感的企业记录时，需要额外的防监控保护。

讨论问题: 与单服务器路由相比，Dynamic MultiHop 如何提供更出色的隐私保护?

检查点 9: 破解密码

网络工程师保护路由通道和客户端隧道。使用下面的汉字与数字对照表，在空白处写出对应的汉字，解密这条信息。

汉字转数字加密密钥

地=1 器=2 网=3 内=4 析=5 数=6 结=7 强=8 换=9 防=10

络=11 仅=12 务=13 存=14 火=15 联=16 私=17 绕=18 轮=19 全=20

解=21 隐=22 址=23 过=24 泄=25 漏=26 增=27 服=28 安=29 墙=30

16	7	3	11	19	9	1	23	27	8	22	17

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)

回顾有关虚拟专用网络（VPN）和隧道技术的最常见问题和解答。

Q1: 什么是 Surfshark CleanWeb?

CleanWeb 是一项集成安全功能，可拦截广告、跟踪器、恶意软件和网络钓鱼网站。

Q2: 什么是仅内存（RAM-only）服务器?

纯内存服务器在易失性内存上运行，这意味着服务器每次重启时，内存中的数据都会被清除。

Q3: Surfshark MultiHop 是什么?

MultiHop（Double VPN）将你的互联网连接通过两个不同的服务器位置进行路由和加密。

Q4: 伪装模式如何工作?

伪装模式会混淆 VPN 流量，使你的 ISP 无法判断你在使用 VPN。

Q5: Bypasser 功能是什么?

Bypasser 是 Surfshark 的分应用隧道工具，可让特定应用或网站绕过 VPN。

检查点 10: 基础 VPN 常见问题 (B 部分)

回顾有关虚拟专用网络（VPN）和隧道技术的最常见问题和解答。

Q6: Surfshark 有断网开关吗?

是的，如果 VPN 意外断开，终止开关会让你断开互联网。

Q7: Surfshark 使用什么加密标准?

Surfshark 使用 AES-256-GCM 和 ChaCha20，并在其新的 Dausos 协议上使用 AEGIS-256X2。

Q8: Surfshark 的无日志政策接受过审计吗?

是的，Deloitte 在 2023 年和 2025 年两次验证了 Surfshark 的无日志政策。

Q9: Surfshark Nexus 是什么?

Nexus 是一种先进的 SDN 架构，将所有服务器连接成统一网络，使路由更顺畅。

Q10: 什么是 IP 轮换器（IP Rotator）功能?

IP 轮换器会每隔几分钟自动更换你的 IP 地址，而不会断开你的 VPN 会话。

检查点 10: 高级 VPN 常见问题 (C 部分)

探索 VPN 隧道协议、移动客户端集成和企业部署的高级技术层面。

Q1: Dynamic MultiHop 与传统的双重 VPN 有何不同?

Dynamic MultiHop 让你可以自定义全球范围内入口和出口服务器的任意组合。

Q2: CleanWeb 2.0 可在浏览器扩展中使用吗?

是的，CleanWeb 2.0 可拦截 Chrome/Firefox 中的视频广告、Cookie 同意弹窗和提示横幅。

Q3: 安全套件中的 Alternative ID 是什么?

Alternative ID 会生成唯一的个人假名、电子邮件地址和电话掩码。

Q4: Surfshark 如何防止 DNS 泄漏?

Surfshark 通过每个节点上自己的私有 DNS 服务器路由所有域名请求。

Q5: Surfshark 在手机上支持 ChaCha20 加密吗?

是的，Android 和 iOS 上的 WireGuard 使用 ChaCha20-Poly1305，以获得出色的移动端效率。

检查点 10: 高级 VPN 常见问题 (D 部分)

探索 VPN 隧道协议、移动客户端集成和企业部署的高级技术层面。

Q6: Surfshark 中的 NoBorders 模式是什么?

NoBorders 会自动检测受限的网络环境并提供专用服务器。

Q7: 谁对 Surfshark 浏览器扩展进行了安全审计?

独立网络安全公司 Cure53 完成了对浏览器扩展和服务器系统的审计。

Q8: Surfshark 如何防范 IPv6 泄漏?

Surfshark 会安全地路由 IPv6 流量，或安全地加以限制，以防止任何未加密的泄漏。

Q9: Surfshark 的法律管辖地在哪里?

Surfshark 在荷兰法律下运营，遵守严格的 GDPR 欧洲隐私标准。

Q10: Surfshark 支持双重身份验证（2FA）吗?

是的，Surfshark One 还增加了 2FA 锁，因此只有你才能更改功能设置。

第 11 部分: 10 个现实中的 VPN 事实与洞察

回顾有关 VPN 加密速度、协议审计、移动连接和企业远程办公的真实事实。

1. VPN 洞察

1. Surfshark 表示其 4,500 多台服务器的整个网络都运行在无盘的易失性纯内存硬件上。

2. VPN 洞察

2. 四大会计师事务所之一的德勤在 2023 年和 2025 年 11 月再次验证了 Surfshark 的无日志政策。

3. VPN 洞察

3. 专有的 Nexus 架构将所有全球服务器连接成一个动态软件定义网络。

4. VPN 洞察

4. 轮换 IP 大约每五分钟更换一次你的 IP 地址，而不会断开 VPN 连接。

5. VPN 洞察

5. CleanWeb 2.0 直接在浏览器中拦截侵入式 Cookie 同意弹窗和视频广告。

6. VPN 洞察

6. Dynamic MultiHop 允许用户在 100 个国家之间创建自定义的双服务器加密路径。

7. VPN 洞察

7. 伪装模式会去除 VPN 头部特征，使流量与普通 HTTPS 无法区分。

8. VPN 洞察

8. Alternative ID 会生成一次性假名和邮箱掩码，保护用户免受数据库泄露影响。

9. VPN 洞察

9. Surfshark 在 WireGuard 协议上采用 AES-256-GCM 对称加密和 ChaCha20。

10. VPN 洞察

10. NoBorders 模式在受限网络上自动启用，以提供有弹性的隧道访问。

技术参考资料与来源

本学习指南和互动谜题根据全球技术标准、规范和监管框架编写。

学术与行业参考资料

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

答案: 检查点 1 – 单项选择

1 **集成内容拦截器** 广告与恶意软件防御 正确答案: B

教学提示

CleanWeb 是 Surfshark 的集成安全过滤器，可在网络层面拦截广告、跟踪器域名、网络钓鱼网站和恶意 URL 脚本。引用: CleanWeb 安全规格。

2 **100% 纯内存基础设施** 内存架构 正确答案: B

教学提示

Surfshark 运行仅 RAM 服务器，因此服务器内存中的数据会在服务器断电或重启时被清除。引用: Cure53 Infrastructure Audit。

3 **MultiHop 双重隧道** 多跳 VPN 正确答案: B

教学提示

MultiHop（Double VPN）通过位于不同国家的两个不同服务器节点加密流量，以防止流量关联攻击。引用: Surfshark MultiHop Guide。

4 **伪装模式混淆** 混淆 正确答案: B

教学提示

伪装模式会修改 OpenVPN 数据包头，将 VPN 流量伪装成标准 HTTPS 流量，从而绕过限制性防火墙的封锁。引用: Surfshark Stealth 白皮书。

5 **Bypasser 分应用隧道** 分割隧道 正确答案: B

教学提示

Bypasser 是 Surfshark 的分应用隧道工具，可让用户选择特定应用或网站，直接通过其常规 ISP 连接路由。引用：Surfshark Client Features。

答案: 检查点 2 – 判断题（正确或错误）

6 **易失性内存数据清除** 服务器安全 正确答案: 正确

教学提示

纯内存服务器不在永久性硬盘上存储任何数据；重启硬件会立即清除所有运行内存。引用: RAM Server Architecture。

7 **伪装模式 ISP 隐匿** 流量隐藏 正确答案: 正确

教学提示

伪装模式会剥离 OpenVPN 协议特征，使 ISP 无法检测到用户已连接到 VPN 隧道。引用: 深度包检测指南。

8 **CleanWeb 2.0 浏览器扩展** 浏览器扩展 正确答案: 正确

教学提示

CleanWeb 2.0 在浏览器扩展中运行，实时拦截 Cookie 同意弹窗、视频广告和恶意重定向脚本。引用: CleanWeb 2.0 发行说明。

9 **零连接日志留存** 无日志政策 正确答案: 错误

教学提示

Surfshark 坚持经独立审计的严格零日志政策，不记录 IP 地址、连接时间戳或带宽日志。引用: Deloitte No-Logs Audit。

10 **Nexus IP 动态轮换** Nexus 网络 正确答案: 正确

教学提示

Surfshark Nexus 软件定义网络每隔几分钟动态轮换用户 IP 地址，而不会中断当前的 VPN 连接。引用: Surfshark Nexus Architecture。

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

C 1. 服务器网络	D 2. 联结网络	G 3. 多跳	F 4. 仅内存
B 5. 绕过工具	A 6. 内存服务器	H 7. Nexus 网络	E 8. 轮换

检查点 3: 答案 – 关键术语

1 净网过滤	2 仅内存	3 多跳连接	4 伪装
5 绕过器	6 联结网络		

检查点 6 替代活动: 答案 – 词语配对

1 D – 仅内存	2 F – 内存服务器	3 A – 服务器网络	4 E – 网络防火墙
5 B – 联结网络	6 H – 绕过器	7 C – 解析服务器	8 G – 网络泄漏

教师讨论提示

关键术语:
检查学生能否用自己的话解释服务器网络、联结网络和多跳，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。

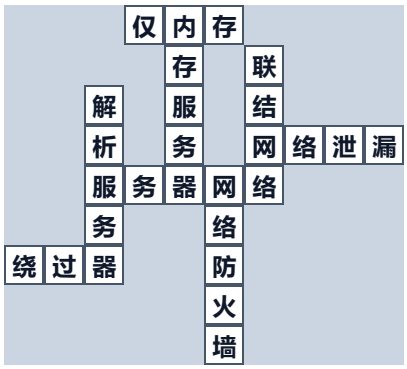
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

安	息	结	用	连	结	人	存	公	务	墙	统	击	议	隐
软	器	墙	全	人	服	安	传	网	协	系	私	过	务	器
安	务	份	私	问	公	份	信	险	络	户	软	名	务	数
传	服	绕	络	隐	域	浏	地	访	绕	泄	攻	传	录	安
设	存	名	器	名	服	析	证	漏	软	仅	漏	保	软	墙
密	内	理	问	保	务	风	网	管	认	软	绕	过	器	仅
件	攻	加	道	输	器	共	用	络	防	址	数	网	数	加
系	内	防	名	内	网	议	仅	隧	防	协	务	备	证	域
络	务	问	份	身	络	议	件	统	隐	火	身	身	设	管
网	输	隧	人	护	加	输	件	攻	接	传	墙	据	联	服
结	解	析	服	务	器	公	漏	览	加	绕	联	保	协	仅
联	私	过	服	身	务	备	析	统	加	道	数	网	内	过
风	服	议	络	务	攻	务	信	私	问	服	管	存	设	证
用	问	传	绕	公	信	备	记	户	络	络	备	击	份	统
隧	仅	件	名	理	隧	传	码	份	泄	数	保	传	析	结

填字游戏答案



填字游戏答案教师指南

横向

1 横向: 仅内存 每次断电都会清除所有数据的易失性内存服务器硬件 (3 字)

5 横向: 网络泄漏 本应受保护的网络信息意外暴露在隧道之外 (4 字)

6 横向: 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)

8 横向: 绕过器 让选定应用绕过 VPN 的分流隧道功能 (3 字)

纵向

2 纵向: 内存服务器 只把数据放在易失性内存中、断电即清空的服务器 (5 字)

3 纵向: 联结网络 把所有服务器连接成统一网状结构的专有软件定义网络 (4 字)

4 纵向: 解析服务器 负责把域名转换为地址的服务器 (5 字)

7 纵向: 网络防火墙 设在网络边界、过滤进出流量的防护系统 (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. 网器服络务 — **服务器网络**
2. 解器务服析 — **解析服务器**
3. 防网墙火络 — **网络防火墙**
4. 漏泄网络 — **网络泄漏**
5. 络联网结 — **联结网络**
6. 内存仅 — **仅内存**
7. 务器内服存 — **内存服务器**
8. 器过绕 — **绕过器**

秘密密码挑战答案

“联结网络轮换地址增强隐私”

案例研究答案

A 案例研究 1: 绕过校园和工作场所过滤

教师解答

评分标准与解答指南

- 情景分析: 一名学生发现其大学校园 Wi-Fi 阻止了所有标准的 OpenVPN 和 WireGuard 端口。
- 思考问题: 哪项 Surfshark 功能可让学生在不被网络管理员发现的情况下连接?
- 建议策略与方案: 启用伪装模式 (OpenVPN)，它会隐藏 VPN 元数据，使防火墙看到的是正常的 HTTPS 浏览行为。

B 案例研究 2: 高风险新闻调查

教师解答

评分标准与解答指南

- 情景分析: 一名调查记者在研究敏感的企业记录时，需要额外的防监控保护。
- 思考问题: 与单服务器路由相比，Dynamic MultiHop 如何提供更出色的隐私保护?
- 建议策略与方案: 动态 MultiHop 会通过两个国家的入口和出口服务器路由流量，因此没有任何单一服务器能够暴露用户。