姓名: _____ 日期: _____ 得分: _____

NordVPN 评测

对总部位于巴拿马的 NordVPN、专有 NordLynx 速度基准测试、无盘仅 RAM 服务器节点和基于 DNS 的威胁防护的技术分析。

NORDVPN 评测学习概览

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NordVPN 的技术评测。你将探索巴拿马司法管辖区、专有的 NordLynx 速度、无盘纯内存（RAM-only）服务器节点和 Threat Protection。

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/nordvpn/

你的 NordVPN 学习路线图

- 分析 NordVPN 评测的技术架构和加密标准。
- 配置客户端设置，防止 IP、DNS 和 WebRTC 流量泄漏。
- 将专有隧道协议与标准实现进行比较。

NORDVPN 评测说明

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NordLynx 和 Threat Protection。 最后完成附加活动: 快速思考。

NORDLYNX 性能与巴拿马司法管辖区（简介）

NordVPN 在法律上位于巴拿马，不属于“十四眼”联盟。它采用专有的 NordLynx 协议以获得顶级速度，使用无磁盘的仅内存服务器节点，并配备基于 DNS 的威胁防护套件来保护数据包。

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. NordVPN 基于 WireGuard 的专有协议叫什么名称?
   - A) NordLynx
   - B) Lightway
   - C) OpenWeb
   - D) Catapult Hydra

2. 为保护用户隐私，NordVPN 的法定总部位于哪个国家?
   - A) 巴拿马
   - B) 瑞士
   - C) 瑞典
   - D) 塞浦路斯

3. 哪个基于 DNS 的 NordVPN 工具（现已更名为诈骗与网络钓鱼防护）可以拦截广告?
   - A) Threat Protection
   - B) SafeConnect
   - C) AntiTracker
   - D) CleanWeb

4. 一个 NordVPN 账户允许多少台设备同时连接?
   - A) 十台设备
   - B) 五台设备
   - C) 不限
   - D) 两台设备

5. 哪种服务器类型将两个 VPN 节点串联以混淆源 IP?
   - A) 双重 VPN
   - B) Onion over VPN
   - C) 混淆服务器
   - D) 专用 IP

检查点 2: 判断正误挑战

6 问题 6

6. NordLynx 将快速的 WireGuard 协议与双重 NAT 转换系统结合在一起。

○ 正确 ○ 错误

7 问题 7

7. NordVPN 总部位于巴拿马，不属于全球“十四眼”情报联盟。

○ 正确 ○ 错误

8 问题 8

8. NordVPN 服务器运行在存储连接日志数据库的本地硬盘上。

○ 正确 ○ 错误

9 问题 9

9. 威胁防护功能完全在云端运行，不会在本地检查文件。

○ 正确 ○ 错误

10 问题 10

10. PwC 曾多次审计 NordVPN 的零日志政策，以验证其合规性。

○ 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. 基于 WireGuard 构建的专有协议称为 _____ 路由。
2. 为了在美国法律管辖之外运营，NordVPN 设在 _____ 司法辖区。
3. 为了实现高级路由安全，用户可以通过 _____ 模式串联服务器。
4. 恶意域名由内置的 _____ 引擎拦截。
5. NordVPN 选择在 _____ 基础设施上运行其 VPN 服务器。
6. 独立审计已验证 NordVPN 严格的 _____ 隐私承诺。

词汇词库

巴拿马　双重跳转　隧道传输　威胁防护　无盘内存　无日志　终止开关　NordLynx

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

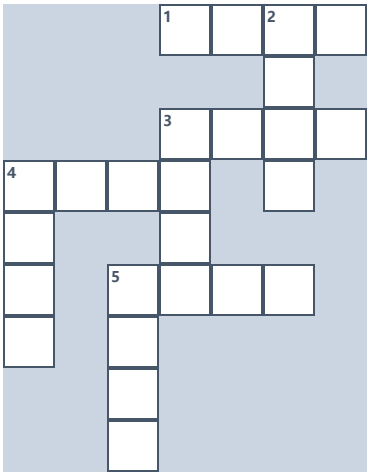
定义配对

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. NordLynx	**A**	中美洲的司法管辖区及总部所在地。
	2. 巴拿马	**B**	经审查的隐私政策，不存储任何活动历史。
	3. 双重 VPN	**C**	内置的广告拦截和恶意软件域名过滤工具。
	4. 威胁防护	**D**	串联路由流量的双服务器链。
	5. 无盘内存	**E**	在隧道中断时切断流量的故障安全拦截器。
	6. 零日志	**F**	不在磁盘上存储任何日志的易失性内存服务器硬件。
	7. Kill Switch	**G**	封装数据包载荷以跨越网络。
	8. 隧道传输	**H**	采用双重 NAT 的专有 WireGuard 实现。

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. 隧道中断时切断流量的故障保护拦截器 (4)
3. 规定数据如何被加密和交换密钥的一组规则 (4)
4. 对同一份数据连续进行两次加密保护 (4)
5. 带有双重 NAT 的、WireGuard 专有实现 (4)

纵向

2. 代码公开、可供任何人检查的连接协议 (4)
3. 对通过其中的所有数据进行加密的传输通道 (4)
4. 让流量依次经过串联的双重服务器路由 (4)
5. 封装数据包负载，以便跨越网络传输 (4)

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: 隧道中断时切断流量的故障保护拦截器 (4 字):

3 横向: 规定数据如何被加密和交换密钥的一组规则 (4 字):

4 横向: 对同一份数据连续进行两次加密保护 (4 字):

5 横向: 带有双重 NAT 的、WireGuard 专有实现 (4 字):

纵向

2 纵向: 代码公开、可供任何人检查的连接协议 (4 字):

3 纵向: 对通过其中的所有数据进行加密的传输通道 (4 字):

4 纵向: 让流量依次经过串联的双重服务器路由 (4 字):

5 纵向: 封装数据包负载，以便跨越网络传输 (4 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 址 人 安 信 录 用 私 开 公 终 输 务 火 击
攻 协 护 统 火 全 共 服 隧 安 管 名 击 私 转
服 密 器 安 身 私 访 输 身 道 户 风 户 统 域
务 加 数 理 跳 络 护 址 隧 问 传 访 跳 险 理
记 重 安 件 域 加 器 域 源 认 关 输 统 双 息
系 双 火 密 管 密 访 隧 保 份 设 认 统 双 软
险 加 人 传 输 协 用 议 道 地 数 网 数 加 击
重 议 域 重 协 议 双 共 名 协 务 件 认 址 服
关 访 身 证 协 软 系 隐 证 证 议 件 备 理 共
开 公 护 据 传 软 险 接 管 据 记 服 输 关 道
止 开 源 协 议 加 跳 记 息 名 私 转 服 证 双
终 务 设 源 加 系 据 隧 全 网 转 份 服 重 协
络 务 险 务 密 信 隐 访 服 备 件 认 跳 用 访
管 跳 传 信 隧 设 览 户 络 络 设 转 攻 身 系
共 双 软 域 道 管 人 理 码 身 止 数 息 管 源

词汇列表

加密协议 **开源协议** **加密隧道** **隧道协议** **双重加密** **终止开关** **隧道传输** **双重跳转**

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. 加密协议
B. 开源协议
C. 加密隧道
D. 隧道协议
E. 双重加密
F. 终止开关
G. 隧道传输
H. 双重跳转

定义与配对字段
1. 对同一份数据连续进行两次加密保护。
2. 隧道中断时切断流量的故障保护拦截器。
3. 封装数据包负载，以便跨越网络传输。
4. 规定数据如何被加密和交换密钥的一组规则。
5. 带有双重 NAT 的、WireGuard 专有实现。
6. 代码公开、可供任何人检查的连接协议。
7. 让流量依次经过串联的双重服务器路由。
8. 对通过其中的所有数据进行加密的传输通道。

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. 协 加 议 密
2. 加 隧 道 密
3. 密 双 加 重
4. 输 传 隧 道
5. 议 开 协 源
6. 协 议 隧 道
7. 开 终 关 止
8. 双 转 跳 重

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	你会向其推荐 NordVPN 的人			
2	VPN 绝不应该存储的数据			
3	形容好用 VPN 应用的词语			
4	NordVPN 可以对你的网络隐藏的内容			
5	终止开关（kill switch）能起到帮助的情形			
6	你会安装 NordVPN 的设备			
7	NordVPN 以外的 VPN 服务			
8	VPN 应用中的按钮或菜单			
9	选择 NordVPN 的原因			
10	你会开启 NordVPN 的场合			
11	你观看的流媒体服务			
12	你希望 NordVPN 提供服务器的国家			
13	你知道的 VPN 协议			
14	你在选择 NordVPN 时看重的功能			
15	VPN 连接速度慢的迹象			

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: 实施 NordLynx 架构



情景: 一家企业希望在移动客户端上实现高吞吐量，但要求动态分配本地 IP，并且不在服务器上存储连接历史。

讨论问题: 解释 NordLynx 的双重 NAT 系统如何解决标准 WireGuard IP 分配的隐私问题。

案例研究 2: 防范本地数据查扣



情景: 一家政府机构要求从位于托管机房的 NordVPN 服务器节点获取实体服务器硬盘，以调查用户流量。

讨论问题: 分析无盘纯内存服务器节点如何在断电时抵御实体数据提取。

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

传=1 护=2 网=3 加=4 户=5 密=6 全=7 接=8 保=9 客=10

重=11 输=12 据=13 协=14 议=15 止=16 终=17 码=18 安=19 跳=20

络=21 连=22 源=23 转=24 隧=25 开=26 道=27 关=28 数=29 双=30

25	27	14	15		9	2		10	5		29	13		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 NordLynx?

它是 NordVPN 基于 WireGuard 构建的专有协议，使用双重 NAT 系统，针对速度和隐私进行了优化。 [9]

Q2: NordVPN 总部在哪里?

NordVPN 总部位于巴拿马，该国有严格的隐私法律，且不属于“十四眼”联盟。

Q3: NordVPN 会保存连接日志吗?

不会，它执行严格的零日志政策，并已通过 PwC 和 Deloitte 审计独立验证。

Q4: 我可以连接多少台设备?

一个 NordVPN 订阅下，你最多可同时连接 10 台设备。

Q5: 它包含广告拦截吗?

是的，其威胁防护（Threat Protection）功能可拦截广告、跟踪脚本和恶意软件域名。

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: 什么是 Double VPN?

这项功能会将你的流量依次通过两台独立的 VPN 服务器路由，并加密两次。

Q7: NordVPN 的服务器是无盘的吗?

是的，NordVPN 选择了基于 RAM 的无盘服务器，因此服务器每次断电时存储的数据都会被清除。

Q8: 我可以在路由器上使用 NordVPN 吗?

是的，NordVPN 提供手动配置文件，可在兼容的路由器上设置隧道。

Q9: Onion Over VPN 是什么?

这项功能会将你的流量先路由到 NordVPN 的服务器，然后立即进入 Tor 洋葱网络。

Q10: 该应用有终止开关吗?

是的，它具有系统级和应用级终止开关，如果 VPN 断开，会阻止互联网访问。

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: NordLynx 中的双重 NAT 系统如何保护用户隐私?

WireGuard 通常需要在服务器上存储静态本地 IP。NordLynx 则动态分配临时本地 IP，不存储可识别身份的数据。

Q2: 巴拿马的司法管辖区对隐私有什么好处?

巴拿马没有针对 VPN 的数据留存法律，外国的数据请求必须通过巴拿马法律程序。 [2]

Q3: 威胁防护如何在本地扫描文件?

Threat Protection Pro 会在文件下载到你的设备时对其进行扫描，并隔离或删除任何含有恶意软件的文件。 [6]

Q4: NordLynx 使用哪些密码算法进行加密?

NordLynx 使用 ChaCha20 进行对称加密，使用 Poly1305 进行身份验证，使用 Curve25519 进行密钥交换。

Q5: NordVPN 支持混淆服务器吗?

是的，它提供混淆服务器，可伪装 VPN 流量，帮助其通过深度包检测（DPI）。

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: NordVPN 如何验证其零日志政策?

PwC Switzerland（2018、2020）和 Deloitte（2022–2025）审查了其系统，并在六次评估中确认了其无日志声明。 [4]

Q7: NordVPN 支持 Meshnet 吗?

是的，Meshnet 允许用户创建安全的本地网络，直接连接远程设备，而无需经过 VPN 服务器路由。

Q8: 该应用如何防止 WebRTC 和 DNS 泄漏?

它将你的 DNS 查询通过 NordVPN 自己的 DNS 服务器路由，使你的互联网服务商无法看到这些查询。

Q9: NordVPN 的服务器是托管在同一机房吗?

是的，NordVPN 正在增加其托管服务器的部署，拥有自己的物理硬件，同时租用数据中心空间。

Q10: 该应用在 macOS 上支持分流吗?

macOS 上不支持；NordVPN 在 Windows、Android 和 Android TV 上提供分流功能，其浏览器扩展还支持排除 URL。

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

NordVPN 由几位儿时好友于 2012 年推出，现归网络安全公司 Nord Security 所有。

2. VPN 洞察

在 VPN.com 的速度测试中，NordVPN 的就近服务器在其 NordLynx 协议的带动下，保持了超过 90% 的基准速度。 [8]

3. VPN 洞察

在 2018 年芬兰一个数据中心的一台服务器遭到入侵后，NordVPN 转向了无盘的基于内存的服务器。 [7]

4. VPN 洞察

NordVPN 在全球 225 个地点运营着数千台服务器（截至 2026 年 9 月）。

5. VPN 洞察

Meshnet 可直接连接用户设备；NordVPN 撤销了其 2025 年的停用计划，并将开源该功能。 [5]

6. VPN 洞察

NordVPN 的运营方 nordvpn S.A. 注册在巴拿马城，这使该服务受巴拿马法律管辖。 [2]

7. VPN 洞察

托管服务器由 NordVPN 拥有并管理，使其对硬件和升级拥有更多控制权。

8. VPN 洞察

NordVPN 提供适用于 Windows、macOS、Linux、Android、iOS、Apple TV 和主流网络浏览器的应用。

9. VPN 洞察

Deloitte 在 2022、2023、2024 和 2025 年审查了 NordVPN 的无日志声明，此前 PwC 曾在 2018 年和 2020 年进行审查。 [4]

10. VPN 洞察

即使 VPN 关闭，Threat Protection Pro 也能工作；在桌面端，基于 DNS 的版本需要开启 VPN。 [6]

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] NordVPN. (2026). NordLynx protocol for fast, secure VPN connections.
https://nordvpn.com/blog/nordlynx-protocol-wireguard/

[2] NordVPN. (n.d.). Privacy Policy - Nord Account.
https://nordvpn.com/privacy-policy/

[3] NordVPN. (2026). A leading no-log VPN for online privacy in 2026.
https://nordvpn.com/features/no-log-vpn/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] NordVPN. (2025). Meshnet stays.
https://nordvpn.com/blog/meshnet-stays/

[6] NordVPN Support. (n.d.). What is NordVPN's Scam, Phishing, and Malware protection?
https://support.nordvpn.com/hc/en-us/articles/19508765521425-What-is-Threat-Protection-Pro-and-Threat-Protection

[7] NordVPN. (2019). NordVPN safe after a third-party provider breach.
https://nordvpn.com/blog/official-response-datacenter-breach/

[8] VPN.com. (n.d.). NordVPN Review: Speed, Pricing & Features.
https://www.vpn.com/vpn/nordvpn/

[9] NordVPN. (2020). NordVPN Is Rolling Out NordLynx -- New Generation VPN Protocol That Makes VPN Connection Faster Than Ever. PR Newswire.
https://www.prnewswire.com/news-releases/nordvpn-is-rolling-out-nordlynx--new-generation-vpn-protocol-that-makes-vpn-connection-faster-than-ever-301046715.html

[10] NordVPN. (2024). NordVPN verifies its no-logs claim for the fourth time. PR Newswire.
https://www.prnewswire.com/news-releases/nordvpn-verifies-its-no-logs-claim-for-the-fourth-time-302031533.html

[11] Nord Security. (n.d.). libtelio: A library providing networking utilities for NordVPN VPN and meshnet functionality.
https://github.com/NordSecurity/libtelio

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

答案: 检查点 1 – 单项选择

1 问题 1 正确答案: A

教学提示

NordLynx 是 NordVPN 自己基于 WireGuard 构建的协议，并增加了双重 NAT 系统以保护隐私。

2 问题 2 正确答案: A

教学提示

NordVPN 的运营方 nordvpn S.A. 注册在巴拿马，该国没有 VPN 数据留存法律。

3 问题 3 正确答案: A

教学提示

Threat Protection（现标记为诈骗与网络钓鱼防护）通过 NordVPN 的 DNS 过滤广告和恶意域名。

4 问题 4 正确答案: A

教学提示

每个 NordVPN 套餐都可在单个账户下同时保护最多十台设备。

5 问题 5 正确答案: A

教学提示

Double VPN 让流量连续通过两台 VPN 服务器，并加密两次。

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

正确: NordLynx 将 WireGuard 的速度与自定义的双重 NAT 系统结合，因此不会存储任何用户 IP。

7 问题 7 正确答案: 正确

教学提示

正确: NordVPN 在巴拿马运营，该国不是“五眼”、“九眼”或“十四眼”联盟的成员。

8 问题 8 正确答案: 错误

教学提示

错误: NordVPN 使用无盘内存服务器，独立审计发现其未保留任何连接日志。

9 问题 9 正确答案: 错误

教学提示

错误: Threat Protection Pro 在设备本地扫描下载的文件并隔离恶意软件。

10 问题 10 正确答案: 正确

教学提示

正确: 在 Deloitte 接手之前，PwC Switzerland 于 2018 年和 2020 年审查了 NordVPN 的无日志声明。 [7]

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

H 1. NordLynx	A 2. 巴拿马	D 3. 双重 VPN	C 4. 威胁防护
F 5. 无盘内存	B 6. 零日志	E 7. Kill Switch	G 8. 隧道传输

检查点 3: 答案 – 关键术语

1 NordLynx	2 巴拿马	3 双重跳转	4 威胁防护
5 无盘内存	6 无日志		

检查点 6 替代活动: 答案 – 词语配对

1 E – 双重加密	2 F – 终止开关	3 G – 隧道传输	4 A – 加密协议
5 D – 隧道协议	6 B – 开源协议	7 H – 双重跳转	8 C – 加密隧道

教师讨论提示

关键术语:
检查学生能否用自己的话解释NordLynx、巴拿马和双重 VPN，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。

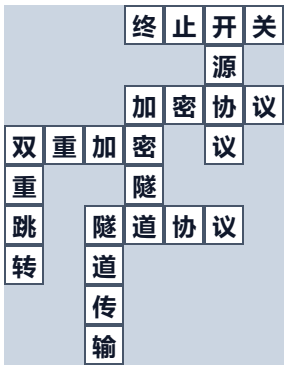
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	址	人	安	信	录	用	私	开	公	终	输	务	火	击
攻	协	护	统	火	全	共	服	隧	安	管	名	击	私	转
服	密	器	安	身	私	访	输	身	道	户	风	户	统	域
务	加	数	理	跳	络	护	址	隧	问	传	访	跳	险	理
记	重	安	件	域	加	器	域	源	认	关	输	统	双	息
系	双	火	密	管	密	访	隧	保	份	设	认	统	双	软
险	加	人	传	输	协	用	议	道	地	数	网	数	加	击
重	议	域	重	协	议	双	共	名	协	务	件	认	址	服
关	访	身	证	协	软	系	隐	证	证	议	件	备	理	共
开	公	护	据	传	软	险	接	管	据	记	服	输	关	道
止	开	源	协	议	加	跳	记	息	名	私	转	服	证	双
终	务	设	源	加	系	据	隧	全	网	转	份	服	重	协
络	务	险	务	密	信	隐	访	服	备	件	认	跳	用	访
管	跳	传	信	隧	设	览	户	络	络	设	转	攻	身	系
共	双	软	域	道	管	人	理	码	身	止	数	息	管	源

填字游戏答案



填字游戏答案教师指南

横向

1 横向: 终止开关 隧道中断时切断流量的故障保护拦截器 (4 字)

3 横向: 加密协议 规定数据如何被加密和交换密钥的一组规则 (4 字)

4 横向: 双重加密 对同一份数据连续进行两次加密保护 (4 字)

5 横向: 隧道协议 带有双重 NAT 的、WireGuard 专有实现 (4 字)

纵向

2 纵向: 开源协议 代码公开、可供任何人检查的连接协议 (4 字)

3 纵向: 加密隧道 对通过其中的所有数据进行加密的传输通道 (4 字)

4 纵向: 双重跳转 让流量依次经过串联的双重服务器路由 (4 字)

5 纵向: 隧道传输 封装数据包负载，以便跨越网络传输 (4 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. 协 加 议 密 — **加密协议**
2. 加 隧 道 密 — **加密隧道**
3. 密 双 加 重 — **双重加密**
4. 输 传 隧 道 — **隧道传输**
5. 议 开 协 源 — **开源协议**
6. 协 议 隧 道 — **隧道协议**
7. 开 终 关 止 — **终止开关**
8. 双 转 跳 重 — **双重跳转**

秘密密码挑战答案

“隧道协议保护客户数据连接”

案例研究答案

A 案例研究 1: 实施 NordLynx 架构

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家企业希望在移动客户端上实现高吞吐量，但要求动态分配本地 IP，且不在服务器上存储连接历史记录。
- 推荐策略与解决方案: 评分指引: 说明 NordLynx 会创建两个本地网络接口，为每个会话分配唯一的 IP，从而避免数据库存储客户端的静态 IP。

B 案例研究 2: 防范本地数据查扣

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一个政府机构要求从共置机房中的 NordVPN 服务器节点提取实体服务器硬盘，以调查用户流量。
- 推荐策略与解决方案: 评分指引: 分析要点：由于操作系统和关键配置完全在易失性 RAM 中运行，关闭服务器会立即清除所有数据。