姓名: _____ 日期: _____ 得分: _____

IPVanish 评测

对总部位于美国的 IPVanish VPN、基本自有的服务器的技术分析

IPVANISH 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IPVanish 的技术评测。你将探索自有物理基础设施、用于 P2P 种子下载的 SOCKS5 代理、WireGuard 性能和美国司法管辖的数据法规。

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/ipvanish/

你的 IPVanish 学习路线图

- 分析 IPVanish 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。

IPVANISH 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SOCKS5 代理和自有服务器基础设施。 最后完成附加活动: 快速思考。

自有基础设施与 SOCKS5 P2P 代理（简介）

IPVanish 的突出之处在于拥有并管理其大部分实体服务器网络，这有助于提升性能和安全性。它提供高速的 WireGuard 协议和用于 P2P 种子下载的 SOCKS5 代理，但受美国五眼联盟司法管辖。

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. 在 IPVanish 客户端应用中，哪种开源协议是高速的默认选项?
   - A) WireGuard
   - B) L2TP/IPSec
   - C) PPTP
   - D) Catapult Hydra

2. IPVanish 提供哪种服务器代理来协助 P2P 种子下载设置?
   - A) SOCKS5 代理
   - B) HTTP 代理
   - C) Tor 中继
   - D) Shadowsocks

3. 哪家公司在 2022 年对 IPVanish 进行了首次独立的无日志审计?
   - A) Leviathan Security Group
   - B) PwC
   - C) Deloitte
   - D) Cure53

4. IPVanish 的公司实体在哪个主要国家的司法管辖下运营?
   - A) 美国
   - B) 瑞士
   - C) 巴拿马
   - D) 英属维尔京群岛

5. IPVanish 高级套餐允许多少台设备同时连接?
   - A) 无限
   - B) 五
   - C) 十
   - D) 七

检查点 2: 判断正误挑战

6 问题 6

6. IPVanish 管理并拥有其大部分实体服务器基础设施。

○ 正确 ○ 错误

7 问题 7

7. SOCKS5 代理流量在传输过程中像标准 VPN 隧道一样被完全加密。

○ 正确 ○ 错误

8 问题 8

8. IPVanish 桌面客户端缺少系统级终止开关功能。

○ 正确 ○ 错误

9 问题 9

9. IPVanish 在美国运营，而美国是五眼情报联盟成员。

○ 正确 ○ 错误

10 问题 10

10. IPVanish 中的分应用隧道允许让应用流量在 VPN 隧道之外路由。

○ 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. 默认配置现代的 _____ 协议，可优化路由性能。
2. 点对点流量可以通过快速的 _____ 路由，以掩盖真实客户端位置。
3. 连接到地理位置较近的节点，可最大限度提高实际的 _____ 。
4. 为防止数据泄漏，用户应配置内置的 _____ 控制功能。
5. 独立的安全审计已认证该提供商的 _____ 承诺。
6. 与某些竞争对手不同，IPVanish 对账户不设任何实际的 _____ 。

词汇词库

服务器速度　服务器网络　设备上限　审计日志　套接字代理　终止开关　IP 地址　WireGuard

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

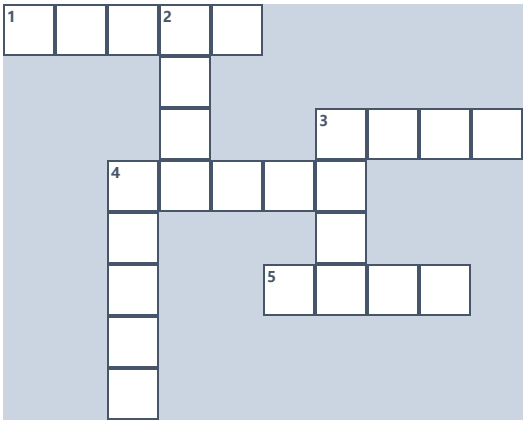
定义配对

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. WireGuard**	**A**	在 VPN 失效时阻止互联网流量的故障安全机制。
☐	**2. SOCKS5 代理**	**B**	以速度和现代密码学著称的开源协议。
☐	**3. 服务器速度**	**C**	限制活动设备会话数量的约束。
☐	**4. Kill Switch**	**D**	服务器节点在实际流量负载下的吞吐能力。
☐	**5. 已审计的日志**	**E**	分配给互联网上设备的唯一网络标识符。
☐	**6. 设备数量限制**	**F**	加密隧道系统的整体防护状况。
☐	**7. IP 地址**	**G**	经核实的记录，确认不追踪任何用户活动。
☐	**8. 安全**	**H**	用于隐藏 P2P 客户端位置的未加密代理路由系统。

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. 用于隐藏点对点客户端位置的非加密代理路由系统 (5)

3. 分配给互联网上设备的唯一网络标识符 (4)

4. 分布在多地、协同转发用户流量的一组服务器 (5)

5. 加密隧道系统整体的防护状况 (4)

纵向

2. 替用户转发请求、隐藏其真实位置的中转服务 (4)

3. 保护网络和系统免受攻击与未经授权访问的做法 (4)

4. 服务器节点在实际流量负载下的吞吐能力 (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: 用于隐藏点对点客户端位置的非加密代理路由系统 (5 字):

3 横向: 分配给互联网上设备的唯一网络标识符 (4 字):

4 横向: 分布在多地、协同转发用户流量的一组服务器 (5 字):

5 横向: 加密隧道系统整体的防护状况 (4 字):

纵向

2 纵向: 替用户转发请求、隐藏其真实位置的中转服务 (4 字):

3 纵向: 保护网络和系统免受攻击与未经授权访问的做法 (4 字):

4 纵向: 服务器节点在实际流量负载下的吞吐能力 (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 览 器 隐 记 输 字 理 务 防 攻 险 名 护
系 防 全 输 服 安 备 域 网 攻 隐 度 服 器 安
证 务 隐 接 传 证 户 份 户 络 系 址 服 数 备
速 服 络 护 地 人 访 接 速 份 安 管 浏 安 软
址 理 务 址 代 服 墙 限 系 套 息 全 击 防 密
设 代 访 息 身 务 件 服 墙 击 代 网 络 地 址
统 风 加 公 管 器 传 器 务 议 地 数 网 数 加
险 套 协 址 字 网 协 代 公 器 域 务 软 墙 址
限 服 接 证 认 络 名 统 击 护 速 认 认 统 设
上 管 公 输 保 据 理 系 风 连 备 度 数 浏 服
接 套 接 字 代 理 理 限 隧 加 速 浏 息 名 安
连 隐 度 服 认 务 软 录 击 据 共 全 网 全 度
身 服 名 络 务 风 务 户 隐 访 码 设 防 统 墙
器 接 备 速 理 户 软 道 用 络 络 护 软 险 证
击 公 套 统 址 设 公 备 码 证 上 数 息 备 录

词汇列表

服务器网络 **代理服务** **套接字代理** **连接上限** **服务器速度** **网络安全** **安全防护** **网络地址**

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. 代理服务
C. 套接字代理
D. 连接上限
E. 服务器速度
F. 网络安全
G. 安全防护
H. 网络地址

定义与配对字段
1. 替用户转发请求、隐藏其真实位置的中转服务。
2. 分配给互联网上设备的唯一网络标识符。
3. 保护网络和系统免受攻击与未经授权访问的做法。
4. 用于隐藏点对点客户端位置的非加密代理路由系统。
5. 分布在多地、协同转发用户流量的一组服务器。
6. 加密隧道系统整体的防护状况。
7. 同一账户允许同时建立的连接数量上限。
8. 服务器节点在实际流量负载下的吞吐能力。

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. 套理代字接 _____

3. 器服度速务 _____

4. 护防安全 _____

5. 务代服理 _____

6. 上限连接 _____

7. 安网全络 _____

8. 网址地络 _____

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	形容好用 VPN 应用的词语			
2	IPVanish 可以对你的网络隐藏的内容			
3	你会开启 IPVanish 的场合			
4	你知道的 VPN 协议			
5	可以向 IPVanish 客服提出的问题			
6	你希望 IPVanish 提供服务器的国家			
7	IPVanish 以外的 VPN 服务			
8	终止开关（kill switch）能起到帮助的情形			
9	选择 IPVanish 的原因			
10	VPN 连接速度慢的迹象			
11	你每天在网上做的事			
12	你会向其推荐 IPVanish 的人			
13	购买 VPN 前要检查的事项			
14	你在本练习单中学到的安全词汇			
15	你在选择 IPVanish 时看重的功能			

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: 媒体中心配置



情景: 一位客户想使用 IPVanish 保护其 Android Fire TV 媒体播放器，以便安全地观看流媒体，同时保持较快的吞吐量。

讨论问题: 为什么对于资源有限的流媒体硬件，WireGuard 协议比 OpenVPN 更受青睐?

案例研究 2: 种子下载网络代理



情景: 一名 P2P 上传者想通过 SOCKS5 配置隐藏自己的位置，同时避免完整数据加密带来的开销。

讨论问题: 比较使用 SOCKS5 代理与使用完整 IPVanish VPN 隧道在安全性和速度方面的取舍。

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

格=1 全=2 上=3 架=4 接=5 无=6 络=7 字=8 理=9 限=10

防=11 构=12 护=13 执=14 行=15 严=16 代=17 志=18 地=19 度=20

日=21 址=22 务=23 套=24 连=25 网=26 器=27 安=28 服=29 速=30

16	1		14	15		6	21	18		4	12

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: IPVanish 的默认协议是什么?

它默认通过高速的 WireGuard 进行路由。

Q2: IPVanish 拥有自己的服务器硬件吗?

是的，它拥有并管理其物理服务器网络的很大一部分。

Q3: IPVanish 总部在哪里?

它总部位于美国，受美国法律约束。

Q4: 可以同时连接多少台设备?

IPVanish 每个账户提供不限数量的并发设备连接。

Q5: 它会保存任何连接日志吗?

不会，它执行严格的零日志政策，并已通过独立审计验证。 [6]

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: IPVanish 提供代理服务吗?

是的，它为种子下载提供免费的 SOCKS5 代理。

Q7: 它包含断网开关吗?

是的，Windows、macOS、Android 和 iOS 上都提供 kill switch。

Q8: 我可以用 IPVanish 绕过地理限制吗?

是的，其全球服务器网络可以访问受限制的图书馆。

Q9: 它支持分应用隧道吗?

是的，提供分流隧道，包括在 Windows 和 Android 上。

Q10: 它使用哪些加密算法?

它使用 AES-256 和 ChaCha20 加密来保护连接。

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: SOCKS5 代理是如何配置的?

它在种子下载客户端中设置，用于隐藏用户 IP，且没有加密带来的开销。

Q2: 拥有服务器硬件如何提高安全性?

它降低了租用第三方服务器的风险，并让服务商能直接控制服务器配置。

Q3: 美国司法管辖区对隐私有哪些影响?

虽然美国法律不要求保留数据，但允许使用国家安全函和令状。

Q4: 断网开关如何防止 IP 泄漏?

如果 VPN 连接意外断开，它会阻止所有互联网适配器。

Q5: WireGuard 使用哪种加密?

WireGuard 使用 ChaCha20 对称密钥加密和 Poly1305 认证。 [7]

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: 零日志政策是如何验证的?

Leviathan Security Group 于 2022 年、Schellman 于 2025 年对其进行了审计；两者均未发现用户日志。 [3]

Q7: 它如何处理 IPv6 DNS 查询?

它会自动通过其私有名称服务器路由所有 DNS 和 IPv6 查询。

Q8: IPVanish 提供混淆功能吗?

是的，其 Scramble 功能可混淆 OpenVPN 流量以绕过防火墙。

Q9: 分应用隧道在移动设备上如何工作?

它允许选定的应用绕过 VPN 隧道并直接连接。

Q10: 它支持路由器配置吗?

是的，OpenVPN 和 WireGuard 配置可以手动加载到 DD-WRT 路由器上。 [1]

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

IPVanish 拥有其大部分服务器基础设施，而不是向第三方租用。 [3]

2. VPN 洞察

IPVanish 自 2012 年起运营，归 Ziff Davis 所有，Ziff Davis 前身为 J2 Global。 [2]

3. VPN 洞察

SOCKS5 代理会隐藏客户端的公网 IP 地址，但不会加密数据包。

4. VPN 洞察

WireGuard 是默认协议，应用中同时提供 OpenVPN 和 IKEv2/IPSec。 [2]

5. VPN 洞察

标准 OpenVPN Scramble 会在数据包头部添加一层 XOR 混淆以绕过防火墙。

6. VPN 洞察

无限同时连接政策允许用户同时保护家中所有设备。 [2]

7. VPN 洞察

Leviathan Security Group（2022 年）和 Schellman（2025 年）的审计验证了其无日志声明。 [3]

8. VPN 洞察

Android 应用支持始终开启的 VPN 设置，在隧道断开时阻止访问互联网。

9. VPN 洞察

OpenVPN 连接可以使用 UDP 以获得速度，或使用 TCP 以便稳定地穿过防火墙。

10. VPN 洞察

它提供 24/7 在线聊天支持，以及在固定工作日营业时间内的电话支持。 [5]

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] VPN.com. (2026). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

答案: 检查点 1 – 单项选择

1 **WireGuard 默认** WIREGUARD 正确答案: A

教学提示

WireGuard 默认配置为优化路由速度。引用: IPVanish Features。

2 **SOCKS5 代理** SOCKS5 代理 正确答案: A

教学提示

SOCKS5 代理可隐藏客户端位置，且没有加密开销。引用: IPVanish Support。

3 **问题 3** 正确答案: A

教学提示

Leviathan Security Group 于 2022 年对 IPVanish 进行了首次无日志审计；Schellman 于 2025 年随后进行了审计。 [3]

4 **美国司法管辖区** 美国 正确答案: A

教学提示

IPVanish 总部位于美国，受五眼联盟规则约束。引用来源: IPVanish Review。

5 **无限设备** 无限 正确答案: A

教学提示

IPVanish 允许不限数量的设备同时连接。引用来源: IPVanish Support。

答案: 检查点 2 – 判断题（正确或错误）

6 **服务器硬件** 拥有网络 正确答案: 正确

教学提示

IPVanish 拥有并管理其大部分实体服务器网络。引用来源: IPVanish Support。

7 **问题 7** 正确答案: 错误

教学提示

错误: SOCKS5 代理会隐藏你的 IP 地址，但不会加密数据。

8 **问题 8** 正确答案: 错误

教学提示

错误: IPVanish 在其桌面和移动应用中都包含终止开关。

9 **美国司法管辖区** 五眼联盟 美国 正确答案: 正确

教学提示

IPVanish 总部位于美国，受五眼联盟监控规则约束。引用来源: IPVanish Review。

10 **分应用隧道** 分割路由 正确答案: 正确

教学提示

分应用隧道让特定应用的流量在安全隧道之外路由。引用: IPVanish Support。

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

B 1. WireGuard	H 2. SOCKS5 代理	D 3. 服务器速度	A 4. Kill Switch
G 5. 已审计的日志	C 6. 设备数量限制	E 7. IP 地址	F 8. 安全

检查点 3: 答案 – 关键术语

1 WireGuard	2 套接字代理	3 服务器速度	4 终止开关
5 审计日志	6 设备上限		

检查点 6 替代活动: 答案 – 词语配对

1 B – 代理服务	2 H – 网络地址	3 F – 网络安全	4 C – 套接字代理
5 A – 服务器网络	6 G – 安全防护	7 D – 连接上限	8 E – 服务器速度

教师讨论提示

关键术语:
检查学生能否用自己的话解释WireGuard、SOCKS5 代理和服务器速度，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。

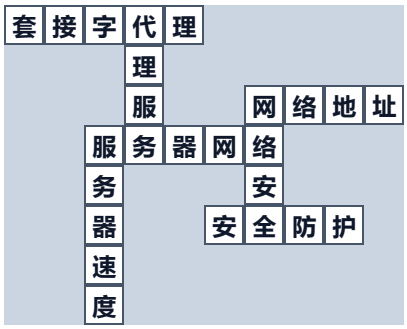
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

安	信	览	器	隐	记	输	字	理	务	防	攻	险	名	护
系	防	全	输	服	安	备	域	网	攻	隐	度	服	器	安
证	务	隐	接	传	证	户	份	户	络	系	址	服	数	备
速	服	络	护	地	人	访	接	速	份	安	管	浏	安	软
址	理	务	址	代	服	墙	限	系	套	息	全	击	防	密
设	代	访	息	身	务	件	服	墙	击	代	网	络	地	址
统	风	加	公	管	器	传	器	务	议	地	数	网	数	加
险	套	协	址	字	网	协	代	公	器	域	务	软	墙	址
限	服	接	证	认	络	名	统	击	护	速	认	认	统	设
上	管	公	输	保	据	理	系	风	连	备	度	数	浏	服
接	套	接	字	代	理	理	限	隧	加	速	浏	息	名	安
连	隐	度	服	认	务	软	录	击	据	共	全	网	全	度
身	服	名	络	务	风	务	户	隐	访	码	设	防	统	墙
器	接	备	速	理	户	软	道	用	络	络	护	软	险	证
击	公	套	统	址	设	公	备	码	证	上	数	息	备	录

填字游戏答案



填字游戏答案教师指南

横向

1 横向: 套接字代理 用于隐藏点对点客户端位置的非加密代理路由系统 (5 字)

3 横向: 网络地址 分配给互联网上设备的唯一网络标识符 (4 字)

4 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)

5 横向: 安全防护 加密隧道系统整体的防护状况 (4 字)

纵向

2 纵向: 代理服务 替用户转发请求、隐藏其真实位置的中转服务 (4 字)

3 纵向: 网络安全 保护网络和系统免受攻击与未经授权访问的做法 (4 字)

4 纵向: 服务器速度 服务器节点在实际流量负载下的吞吐能力 (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. 套理代字接 — **套接字代理**
3. 器服度速务 — **服务器速度**
4. 护防安全 — **安全防护**
5. 务代服理 — **代理服务**
6. 上限连接 — **连接上限**
7. 安网全络 — **网络安全**
8. 网址地络 — **网络地址**

秘密密码挑战答案

“严格执行无日志架构”

案例研究答案

A 案例研究 1: 媒体中心配置

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位客户想使用 IPVanish 保护其 Android Fire TV 媒体播放器，以便安全地观看流媒体，同时保持高吞吐量。
- 推荐策略与解决方案: 评分指引: 说明 WireGuard 的代码量更小，在内核空间中运行，并且占用的 CPU 周期更少，因此能在轻量硬件上最大限度地提升速度。

B 案例研究 2: 种子下载网络代理

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位 P2P 上传者想隐藏自己的位置，又不想承担完整数据加密的开销，于是使用 SOCKS5 配置。
- 推荐策略与解决方案: 评分指引: 指出 SOCKS5 隐藏 IP 地址但不加密流量，速度更快，但无法抵御 ISP 的数据包检查，几乎没有隐私保护。