姓名: _____ 日期: _____ 得分: _____

最安全 VPN 指南

对高安全 VPN 设计、仅 RAM 易失性内存服务器、零信任访问安全、私有加密 DNS 泄漏防御以及经审计的 WireGuard 配置的技术分析。

最安全 VPN 指南学习概览

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高安全性 VPN 的技术标准。你将探索纯内存（RAM-only）服务器硬件、零信任访问安全、私有加密 DNS 解析器和经审计的 WireGuard 配置。

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/most-secure-vpn/

你的最安全 VPN 学习路线图

- 分析最安全 VPN 指南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。

最安全 VPN 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）服务器硬件和零信任系统。 最后完成附加活动: 快速思考。

纯内存基础设施与零信任网络（简介）

真正安全的 VPN 依赖零信任框架、可防止磁盘被查扣而暴露日志的纯内存服务器、私有加密 DNS 解析器，以及 WireGuard 等经审计的协议。这些综合控制措施可保护高价值数字资产免受拦截威胁。

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. 哪种架构对确保现代 VPN 服务器的最高安全至关重要?
   - A) 纯内存服务器基础设施
   - B) 基于磁盘的存储
   - C) 动态 DNS 路由
   - D) 启用端口转发

2. 哪种协议被广泛推荐用于最安全、最现代的 VPN 配置?
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. 哪个安全框架要求无一例外地持续验证每个连接?
   - A) 零信任架构
   - B) 边界防火墙
   - C) 动态路由
   - D) 共享密钥

4. VPN 客户端 DNS 泄露防护的主要作用是什么?
   - A) 将所有 DNS 请求通过私有加密解析器路由
   - B) 混淆 IP 数据包
   - C) 在本地缓存 DNS 查询
   - D) 禁用名称服务器

5. 多跳路由如何提高 VPN 隧道的整体安全性?
   - A) 将数据依次通过两台独立服务器路由
   - B) 提高压缩速度
   - C) 使用低安全强度的密码算法加密数据
   - D) 绕过防火墙

检查点 2: 判断正误挑战

6 问题 6

6. 纯内存服务器将日志文件存储在临时内存中，重启后即被清除。

○ 正确 ○ 错误

7 问题 7

7. WireGuard 使用现代加密算法，不易受速度瓶颈影响。

○ 正确 ○ 错误

8 问题 8

8. VPN 断网保护的工作方式是在隧道中断时阻止所有网络流量。

○ 正确 ○ 错误

9 问题 9

9. 独立的第三方审计与验证安全承诺无关。

○ 正确 ○ 错误

10 问题 10

10. 零信任模型假定所有内部网络连接默认都是安全的。

○ 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. 管理员通过部署严格的 _____ 框架来加强安全。
2. 通过多个入口点路由数据包，需要安全的 _____ 配置。
3. 为防止被盗硬盘泄漏数据，我们采用 _____ 设计。
4. 通过配置原生的 _____ 功能，可缓解运营商劫持。
5. 为在连接失败时阻止流量，请启用 _____ 机制。
6. 要尽量减少存储的数据库日志，请选择完全 _____ 的提供商。

词汇词库

多跳连接　零信任　内存服务器　审计系统　隧道加密　网络隧道　域名保护　终止开关

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

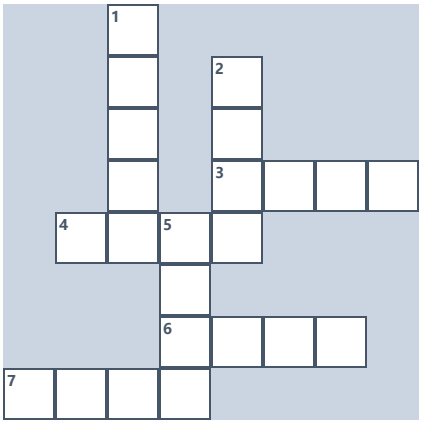
定义配对

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. 零信任	**A**	经独立检查的设置，确认不存储任何日志。
	2. 多跳	**B**	对数据载荷进行加密扰乱，以保护传输。
	3. 纯内存服务器	**C**	要求对所有用户持续进行身份验证的安全框架。
	4. DNS 防护	**D**	一套决定数据如何打包和发送的技术规则。
	5. Kill Switch	**E**	将两个服务器节点串联起来的级联 VPN 路由。
	6. 已审计的系统	**F**	使用易失性内存存储数据负载的服务器架构。
	7. 加密	**G**	强制使用私有 DNS 查询以保护名称服务器查询。
	8. 协议	**H**	在 VPN 失效时阻止流量的故障安全机制。

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

3. 决定数据如何打包和发送的一组技术规则 (4)

4. 在公共网络中为数据开辟的一条受保护的传输通路 (4)

6. 规定数据如何被加密和交换密钥的一组规则 (4)

7. 对数据负载进行加密屏蔽，以保障传输安全 (4)

纵向

1. 分布在多地、协同转发用户流量的一组服务器 (5)

2. 让部分应用走加密隧道、其余应用直接联网的路由方式 (4)

5. 对穿过隧道的数据进行加密保护 (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

3 横向: 决定数据如何打包和发送的一组技术规则 (4 字):

4 横向: 在公共网络中为数据开辟的一条受保护的传输通路 (4 字):

6 横向: 规定数据如何被加密和交换密钥的一组规则 (4 字):

7 横向: 对数据负载进行加密屏蔽，以保障传输安全 (4 字):

纵向

1 纵向: 分布在多地、协同转发用户流量的一组服务器 (5 字):

2 纵向: 让部分应用走加密隧道、其余应用直接联网的路由方式 (4 字):

5 纵向: 对穿过隧道的数据进行加密保护 (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 问 传 安 户 道 器 隐 道 理 分 备 服 议 风
份 域 保 攻 议 全 理 码 数 安 件 址 风 护 存
服 议 务 安 认 护 连 备 墙 据 用 证 用 攻 地
服 协 数 件 内 络 保 问 公 接 加 连 内 身 件
隧 密 安 系 地 服 务 地 览 火 流 密 攻 记 信
险 加 议 加 软 务 接 网 息 认 统 防 攻 览 击
身 加 传 设 管 器 器 名 络 问 数 网 全 据 风
记 名 地 录 域 网 览 理 址 隧 服 系 火 问 服
议 连 认 墙 域 络 击 险 保 火 道 火 击 软 设
协 传 理 保 据 设 攻 身 私 件 数 隧 码 备 流
道 内 存 服 务 器 公 加 内 隧 信 址 护 存 分
隧 码 墙 服 隧 系 览 险 据 输 全 网 存 流 证
服 域 络 服 道 身 服 户 护 接 码 软 隧 击 防
器 连 件 内 加 备 户 系 人 用 络 道 络 系 份
墙 险 理 记 密 击 地 软 传 件 密 墙 分 数 信

词汇列表

隧道加密 网络隧道 加密协议 隧道协议 服务器网络 数据加密 分流隧道 内存服务器

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. 隧道加密
B. 网络隧道
C. 加密协议
D. 隧道协议
E. 服务器网络
F. 数据加密
G. 分流隧道
H. 内存服务器

定义与配对字段
1. 分布在多地、协同转发用户流量的一组服务器。
2. 决定数据如何打包和发送的一组技术规则。
3. 在公共网络中为数据开辟的一条受保护的传输通路。
4. 使用易失性内存存储数据负载的服务器架构。
5. 让部分应用走加密隧道、其余应用直接联网的路由方式。
6. 规定数据如何被加密和交换密钥的一组规则。
7. 对数据负载进行加密屏蔽，以保障传输安全。
8. 对穿过隧道的数据进行加密保护。

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. 加 隧 密 道 _____
2. 加 协 议 密 _____
3. 器 服 络 网 务 _____
4. 道 隧 分 流 _____
5. 道 网 隧 络 _____
6. 协 议 隧 道 _____
7. 加 数 密 据 _____
8. 器 内 服 务 存 _____

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	你每天使用的锁或钥匙			
2	VPN 可以隐藏的内容			
3	使 VPN 安全的因素			
4	关于 VPN 的误解			
5	旅行时使用 VPN 的原因			
6	现实世界中的安全场所			
7	表示“受保护”的词语			
8	优质 VPN 服务商作出的承诺			
9	与隐私相关的词语			
10	审计或检查的类型			
11	你想记住的本练习单中的词语			
12	黑客想窃取的东西			
13	识别虚假 Wi-Fi 网络的方法			
14	你会使用 VPN 的场合			
15	你的网络服务商能看到的内容			

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: 加固企业基础设施



情景: 一家企业银行正在重新设计其远程访问拓扑。他们需要一种零信任架构，将所有客户端设备连接到安全服务器。

讨论问题: 在零信任 VPN 模型下，网络微隔离的主要好处是什么?

案例研究 2: 仅内存（RAM-Only）服务器防护



情景: 一家注重安全的 VPN 提供商正在升级其服务器，以防止服务器被实体扣押后暴露用户日志历史。

讨论问题: 解释纯内存（RAM-Only）硬件配置如何在服务器被实体扣押时防止取证数据提取。

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

全=1 网=2 分=3 价=4 高=5 络=6 用=7 字=8 产=9 器=10
加=11 据=12 护=13 内=14 服=15 存=16 专=17 议=18 隧=19 流=20
道=21 保=22 资=23 值=24 数=25 码=26 务=27 安=28 密=29 协=30

28	1	17	2		22	13		5	4	24		25	8	23	9

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: 是什么让 VPN 成为“最安全”的?

零信任、纯内存服务器和经审计协议的组合。

Q2: 什么是仅内存（RAM-Only）服务器?

在易失性内存中运行、设计为不在磁盘上存储任何日志的服务器。

Q3: 什么是零信任 VPN?

一种持续验证每个访问请求和连接的框架。

Q4: 为什么 WireGuard 被认为是安全的?

它的代码库小巧，易于审计，并使用现代密码算法。

Q5: 安全的 VPN 如何防止 DNS 泄漏?

通过将所有查询路由到私有的加密 DNS 解析器。

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: 安全的 VPN 需要审计吗?

是的，独立审计可验证无日志声明和代码安全性。

Q7: 断网开关起什么作用?

如果 VPN 连接断开，它会立即中断网络流量。

Q8: 安全的 VPN 使用什么加密?

AES-256 和 ChaCha20 是加密领域的行业标准。

Q9: 多跳路由安全吗?

是的，它串联两台或更多服务器，以防止流量分析。

Q10: 离岸司法管辖区有什么帮助?

它可能会限制适用的法律，但并不提供绝对豁免。

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: 仅内存（RAM-Only）服务器如何防止数据被扣押的风险?

因为它们在 RAM 中运行，拔掉电源会清除内存中保存的数据。

Q2: 零信任如何取代标准边界安全?

它把每个客户端都视为不可信，要求持续进行身份验证。

Q3: WireGuard 的代码库为什么更容易审计?

它的 Linux 代码不到 4,000 行，远少于典型的 VPN 软件栈。 [4]

Q4: DNSSEC 如何保护 DNS 查询?

它对 DNS 记录进行签名，使解析器能够检测伪造或被篡改的响应。

Q5: 多跳如何使流量关联更加困难?

通过将传入和传出的 IP 分隔在不同的托管服务商上。

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: 五眼联盟司法管辖区对 VPN 为什么有风险?

成员国共享情报，并可能通过法律命令索取用户数据。

Q7: 断网开关如何在内核层面实现?

它使用系统防火墙规则（如 iptables 或 WFP）来阻止出站流量。

Q8: VPN 握手中的前向保密是什么?

它会生成唯一的会话密钥，使过去的会话无法被解密。

Q9: 安全的 VPN 如何缓解 WebRTC 泄漏?

通过阻止 WebRTC 请求，或让其通过隧道路由。

Q10: 独立审计如何确保隐私合规?

审计人员会进行渗透测试并检查服务器配置。

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

纯内存服务器在启动时将操作系统加载到内存中，因此重启后磁盘上不会留下任何内容。

2. VPN 洞察

WireGuard 使用 Noise 框架，搭配 Curve25519、ChaCha20、Poly1305、BLAKE2s 和 HKDF。 [3]

3. VPN 洞察

零信任按资源授予访问权限，不基于网络位置给予任何隐式信任（NIST SP 800-207）。 [1]

4. VPN 洞察

五眼情报联盟包括美国、英国、加拿大、澳大利亚和新西兰。

5. VPN 洞察

当浏览器通过 STUN 查询泄露客户端真实公网 IP 地址时，就会发生 WebRTC 泄露。

6. VPN 洞察

完美前向保密（PFS）可确保长期密钥泄露不会暴露过去的会话密钥。 [3]

7. VPN 洞察

总部位于柏林的安全公司 Cure53 已发布对多家 VPN 提供商的审计报告。

8. VPN 洞察

DNS 泄漏是指 DNS 查询绕过 VPN 隧道，转而发送到本地 ISP 的名称服务器。

9. VPN 洞察

易失性 RAM 芯片需要持续供电才能保存数据，断电后内容会丢失。

10. VPN 洞察

企业零信任系统在允许连接到安全资源之前，会强制执行设备状态检查。 [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

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

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

[4] 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/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

答案: 检查点 1 – 单项选择

1 **纯内存服务器** 纯内存 正确答案: A

教学提示

纯内存服务器不在磁盘上存储日志，重启后数据即被清除。引用: Most Secure VPN。

2 **问题 2** 正确答案: A

教学提示

WireGuard 将小巧、可审计的代码库与现代加密算法相结合。

3 **零信任模型** 零信任 正确答案: A

教学提示

零信任模型在授予访问权限前会持续验证设备合规性。引用来源: Most Secure VPN。

4 **DNS 防护** DNS 防护 正确答案: A

教学提示

DNS 泄漏防护会将查询请求通过私有解析器路由。引用: Most Secure VPN。

5 **多跳隧道** 多跳 正确答案: A

教学提示

多跳路由将两个独立的服务器节点串联起来。引用: Most Secure VPN。

答案: 检查点 2 – 判断题（正确或错误）

6 **纯内存服务器** 纯内存 正确答案: 正确

教学提示

纯内存服务器硬件不向磁盘写入任何数据，重启后即被清除。引用: Most Secure VPN。

7 **WireGuard 速度** WIREGUARD 正确答案: 正确

教学提示

WireGuard 使用可避免处理瓶颈的现代加密技术。引用: Most Secure VPN。

8 **Kill Switch** 故障安全开关 正确答案: 正确

教学提示

如果 VPN 连接中断，断网保护会阻止所有流量。引用: Most Secure VPN。

9 **第三方审计** 审计至关重要 正确答案: 错误

教学提示

第三方审计对于验证企业的隐私声明至关重要。引用: Most Secure VPN。

10 **问题 10** 正确答案: 错误

教学提示

零信任不会基于网络位置给予任何隐式信任。

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. 零信任	E 2. 多跳	F 3. 纯内存服务器	G 4. DNS 防护
H 5. Kill Switch	A 6. 已审计的系统	B 7. 加密	D 8. 协议

检查点 3: 答案 – 关键术语

1 零信任	2 多跳连接	3 内存服务器	4 域名保护
5 终止开关	6 审计系统		

检查点 6 替代活动: 答案 – 词语配对

1 E – 服务器网络	2 D – 隧道协议	3 B – 网络隧道	4 H – 内存服务器
5 G – 分流隧道	6 C – 加密协议	7 F – 数据加密	8 A – 隧道加密

教师讨论提示

关键术语:
检查学生能否用自己的话解释零信任、多跳和纯内存服务器，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。

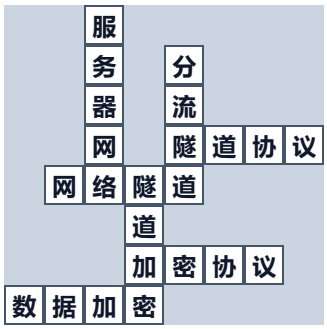
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

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

填字游戏答案



填字游戏答案教师指南

横向

3 横向: 隧道协议 决定数据如何打包和发送的一组技术规则 (4 字)

4 横向: 网络隧道 在公共网络中为数据开辟的一条受保护的传输通路 (4 字)

6 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)

7 横向: 数据加密 对数据负载进行加密屏蔽，以保障传输安全 (4 字)

纵向

1 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)

2 纵向: 分流隧道 让部分应用走加密隧道、其余应用直接联网的路由方式 (4 字)

5 纵向: 隧道加密 对穿过隧道的数据进行加密保护 (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. 加隧密道 — **隧道加密**
2. 加协议密 — **加密协议**
3. 器服络网务 — **服务器网络**
4. 道隧分流 — **分流隧道**
5. 道网隧络 — **网络隧道**
6. 协议隧道 — **隧道协议**
7. 加数密据 — **数据加密**
8. 器内服务存 — **内存服务器**

秘密密码挑战答案

“安全专网保护高价值数字资产”

案例研究答案

A 案例研究 1: 加固企业基础设施

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家企业银行正在重新设计其远程访问拓扑。他们需要一个将所有客户端设备与安全服务器相连的零信任架构。
- 推荐策略与解决方案: 评分指引: 说明微分段将访问限制在特定资源，从而在设备被入侵时防止威胁横向移动。

B 案例研究 2: 仅内存（RAM-Only）服务器防护

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家注重安全的 VPN 提供商正在升级其服务器，以防止服务器被实体查封而暴露用户的日志历史。
- 推荐策略与解决方案: 评分指引: 详述纯内存（RAM-Only）服务器没有物理磁盘存储。断电会自动清除易失性内存中的所有临时数据。