姓名: _____ 日期: _____ 得分: _____

ExpressVPN 安全

评估 ExpressVPN 的安全基础设施，包括自研开源 Lightway 协议、纯内存 TrustedServer 技术、独立安全审计和 Network Lock kill switch。

EXPRESSVPN 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ExpressVPN 的安全功能。你将探索开源协议、纯内存（RAM-only）服务器节点、加密算法和 Network Lock 终止开关（kill switch）。

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/expressvpn/security/

你的 ExpressVPN 安全学习路线图

- 分析 ExpressVPN 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。

EXPRESSVPN 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。将所学知识应用于开源协议和仅内存（RAM-only）服务器节点。 最后完成附加活动: 快速思考。

纯内存服务器阵列与开源连接协议

ExpressVPN 采用纯内存 TrustedServer 技术来防止本地日志，并结合其自研开源 Lightway 协议和 Internet Kill Switch，提供端到端的用户数据安全。

(简介)

ExpressVPN 采用纯内存 TrustedServer 技术来防止本地日志，并结合其自研开源 Lightway 协议和 Internet Kill Switch，提供端到端的用户数据安全。

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. ExpressVPN 的自定义开源协议是什么?

- A) Lightway
- B) WireGuard
- C) OpenVPN
- D) Chameleon

2. 哪种服务器技术只在易失性 RAM 中运行?

- A) TrustedServer
- B) RAM-Core
- C) SecureRAM
- D) NoSpy 服务器

3. 如果 VPN 连接意外断开会发生什么?

- A) 终止开关阻断流量
- B) 流量泄露给 ISP
- C) 系统重启
- D) 数据变为未加密状态

4. ExpressVPN 为保护隐私注册在哪里?

- A) 英属维尔京群岛
- B) 瑞士
- C) 巴拿马
- D) 罗马尼亚

5. 默认使用哪种对称加密算法?

- A) AES-256-GCM
- B) Blowfish
- C) DES-64
- D) RC4

检查点 2: 判断正误挑战

6 问题 6

6. TrustedServer 技术将服务器日志存储在硬盘上。

○ 正确 ○ 错误

7 问题 7

7. ExpressVPN 已接受过第三方安全审计。

○ 正确 ○ 错误

8 问题 8

8. Lightway 协议构建于 OpenVPN 代码库之上。

○ 正确 ○ 错误

9 问题 9

9. 终止开关在桌面应用上默认开启。

○ 正确 ○ 错误

10 问题 10

10. ExpressVPN 在每台服务器上都运行私有 DNS。

○ 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. ExpressVPN 自主设计的高速协议是 _____ 。
2. 为防止保留数据，服务器网络依赖仅使用内存的 _____ 节点。
3. ExpressVPN 的终止开关以前叫做 _____ 。
4. ExpressVPN 依据英属维尔京 _____ 的法律注册。
5. 数据负载通过强大的对称密码 AES-256 进行保护，这种方式称为 _____ 。
6. 零日志政策已由顶尖公司独立验证，属于 _____ 。

词汇词库

独立审计　对称加密　光速协议　可信服务器　群岛　数据泄漏　网络锁　DNS

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

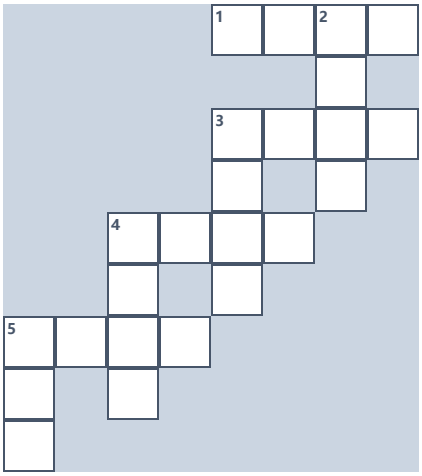
定义配对

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. Lightway	**A**	提供强隐私保护的英属维尔京群岛司法管辖区
	2. TrustedServer	**B**	私有 IP、DNS 或 WebRTC 数据的意外暴露
	3. 锁	**C**	域名系统解析器在每个服务器节点上私下运行
	4. 群岛	**D**	经第三方安全公司独立验证
	5. AES-256	**E**	防止在磁盘上存储数据的纯内存服务器架构
	6. 已审计	**F**	Network Lock（终止开关的旧名称）的最后一个单词
	7. 泄漏	**G**	ExpressVPN 的轻量级开源连接协议
	8. DNS	**H**	保护数据传输的对称加密标准

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. 加解密双方使用同一密钥、用于保护数据传输的标准，例如 AES-256 (4)

3. 规定如何封装并加密隧道内数据的一组规则 (4)

4. 用密码算法把数据变成他人无法读取的形式 (4)

5. 本应受保护的网络信息意外暴露在隧道之外 (4)

纵向

2. 规定数据如何被加密和交换密钥的一组规则 (4)

3. 对穿过隧道的数据进行加密保护 (4)

4. 私有 IP、DNS 或 WebRTC 数据的意外暴露 (4)

5. 终止开关的旧名称（英文原名为 Network Lock）(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

1 横向: 加解密双方使用同一密钥、用于保护数据传输的标准，例如 AES-256 (4 字):

3 横向: 规定如何封装并加密隧道内数据的一组规则 (4 字):

4 横向: 用密码算法把数据变成他人无法读取的形式 (4 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):

纵向

2 纵向: 规定数据如何被加密和交换密钥的一组规则 (4 字):

3 纵向: 对穿过隧道的数据进行加密保护 (4 字):

4 纵向: 私有 IP、DNS 或 WebRTC 数据的意外暴露 (4 字):

5 纵向: 终止开关的旧名称（英文原名为 Network Lock） (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 问 输 安 户 道 器 隐 浏 理 锁 管 务 防 险
风 域 保 击 议 全 传 码 网 安 件 域 风 隐 漏
服 密 务 安 认 隐 接 管 认 络 户 身 用 击 址
服 加 数 设 泄 络 保 问 公 访 泄 连 泄 身 设
隧 据 安 统 地 隧 务 址 记 火 称 漏 攻 录 信
攻 数 议 密 件 道 接 对 息 认 软 火 攻 记 击
身 加 输 备 管 协 器 协 称 问 数 网 全 据 风
录 协 址 锁 名 议 记 传 域 加 服 统 火 地 服
漏 接 认 墙 域 系 险 护 墙 墙 密 系 软 备 传
泄 理 保 据 备 击 身 私 设 数 道 服 管 称 共
据 加 密 协 议 加 泄 道 信 域 隐 漏 码 墙 网
数 服 统 览 隧 险 据 公 全 网 漏 证 服 络 名
络 服 身 服 道 户 护 接 码 软 系 火 锁 器 接
件 泄 备 户 加 统 人 用 络 络 统 风 认 攻 传
录 击 址 件 密 输 设 密 认 对 数 信 设 记 浏

词汇列表

隧道协议 **加密协议** **网络锁** **隧道加密** **对称加密** **数据加密** **数据泄漏** **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. 隧道协议
B. 加密协议
C. 网络锁
D. 隧道加密
E. 对称加密
F. 数据加密
G. 数据泄漏
H. 网络泄漏

定义与配对字段
1. 私有 IP、DNS 或 WebRTC 数据的意外暴露。
2. 对穿过隧道的数据进行加密保护。
3. 本应受保护的网络信息意外暴露在隧道之外。
4. 规定如何封装并加密隧道内数据的一组规则。
5. 终止开关的旧名称（英文原名为 Network Lock）。
6. 加解密双方使用同一密钥、用于保护数据传输的标准，例如 AES-256。
7. 规定数据如何被加密和交换密钥的一组规则。
8. 用密码算法把数据变成他人无法读取的形式。

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 隧 议 道 _____

2. 锁 络 网 _____

3. 密 对 加 称 _____

4. 漏 泄 数 据 _____

5. 议 加 协 密 _____

6. 加 密 隧 道 _____

7. 加 数 密 据 _____

8. 网 漏 泄 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	你在选择 ExpressVPN 时看重的功能			
2	公共 Wi-Fi 上的威胁			
3	VPN 泄漏的类型			
4	设置强密码的方法			
5	VPN 应用中的按钮或菜单			
6	你每天在网上做的事			
7	你会向其推荐 ExpressVPN 的人			
8	以严格隐私法律闻名的国家			
9	你知道的 VPN 协议			
10	审计可以检查的内容			
11	ExpressVPN 中的安全功能			
12	购买 VPN 前要检查的事项			
13	为增强安全而开启的设置			
14	加密所保护的内容			
15	ExpressVPN 可以对你的网络隐藏的内容			

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: 落实仅内存保护



情景: 一家政府机构扣押了一台 ExpressVPN 服务器，以提取用户日志和连接历史。

讨论问题: 他们会在服务器上找到什么信息，为什么?

案例研究 2: 不稳定的 Wi-Fi 连接隧道



情景: 一名远程办公者使用的酒店公共 Wi-Fi 每隔几分钟就会断线，而他正在编辑文档。

讨论问题: 断线期间，ExpressVPN 如何保护他们的数据不泄露?

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

安=1 务=2 密=3 络=4 信=5 码=6 每=7 加=8 全=9 志=10

泄=11 议=12 清=13 日=14 据=15 漏=16 用=17 器=18 道=19 数=20

户=21 网=22 称=23 除=24 隧=25 服=26 可=27 锁=28 对=29 协=30

27	5	26	2	18		7	14		13	24		17	21	14	10

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: ExpressVPN 使用什么加密?

ExpressVPN 默认使用 AES-256-GCM 对称加密。

Q2: 什么是 Lightway 协议?

Lightway 是 ExpressVPN 为速度、安全和稳定而打造的自研协议。

Q3: ExpressVPN 会记录我的搜索历史吗?

不会，ExpressVPN 执行经过独立审计的严格零日志政策。

Q4: 什么是互联网断网开关?

它是 ExpressVPN 的原生 Kill Switch，在连接断开时阻止互联网流量。

Q5: Lightway 协议是开源的吗?

是的，Lightway 协议的核心代码是开源的，并托管在 GitHub 上。 [9]

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: ExpressVPN 运行私有 DNS 吗?

是的，ExpressVPN 在每台服务器上运行自己的私有加密 DNS。 [7]

Q7: TrustedServer 技术是什么?

这是一种服务器配置，操作系统和应用完全在易失性的 RAM 内存中运行。

Q8: ExpressVPN 接受过审计吗?

是的，ExpressVPN 已接受 PwC、Cure53 和 F-Secure 等公司的审计。 [1]

Q9: ExpressVPN 能防范 DNS 和 IPv6 泄漏吗?

是的，Internet Kill Switch 会阻止隧道之外的 IPv4、IPv6 和 DNS 流量。

Q10: ExpressVPN 位于何处?

ExpressVPN 注册于英属维尔京群岛 (BVI)。

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: 仅内存架构如何增强安全性?

数据不会写入硬盘，内存中的数据在服务器断电时就会被清除。

Q2: 为什么 BVI 司法管辖区对隐私很重要?

ExpressVPN 总部位于英属维尔京群岛 (BVI)，因此数据方面的法律要求须遵守 BVI 法律。

Q3: ExpressVPN 支持完美前向保密吗?

是的，Lightway 使用动态密钥，并定期清除和重新生成。

Q4: Network Lock 如何防止 IP 泄漏?

每当 VPN 连接断开时，它会在系统层面阻止所有流量。

Q5: Lightway 能抵御量子攻击吗?

是的，Lightway 采用 NIST ML-KEM 标准提供后量子保护。

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: 政府机构能拦截 Lightway 流量吗?

他们可以拦截，但由于 AES-256/ChaCha20 加密，无法解密。

Q7: 私有 DNS 如何保护用户的搜索记录?

它在加密隧道内处理所有 DNS 查询，防止 ISP 监控。

Q8: Lightway Turbo 用于什么?

它使用多通道隧道一次发送更多数据，以获得更快的速度。

Q9: Lightway 相比 WireGuard 有什么优势?

Lightway 专为快速处理网络切换（如从 Wi-Fi 切换到移动网络）而打造，不会掉线。

Q10: 服务器软件多久重新安装一次?

借助 TrustedServer，每次重启时都会从安全的只读镜像重新加载整个软件栈。

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

Lightway 使用 AES-256-GCM，在低功耗设备上则使用 ChaCha20/Poly1305。 [6]

2. VPN 洞察

TrustedServer 技术旨在让所有服务器操作都在 RAM 中运行。 [4]

3. VPN 洞察

英属维尔京群岛（BVI）是公司注册的司法管辖区。 [8]

4. VPN 洞察

Lightway 已从 C 语言重写为 Rust，并经 Cure53 和 Praetorian 审计。 [3]

5. VPN 洞察

如果 VPN 断开，Internet Kill Switch 会在系统层面阻止流量。 [5]

6. VPN 洞察

所有 DNS 查询都通过私有加密 DNS 服务器解析。 [7]

7. VPN 洞察

ExpressVPN 已发布了 20 多份独立的第三方审计报告。 [1]

8. VPN 洞察

该服务不记录 IP 地址、浏览历史或流量元数据。

9. VPN 洞察

通过动态会话密钥轮换来维持完美前向保密。 [1]

10. VPN 洞察

Lightway 协议同时支持 UDP 和 TCP 传输层。

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] ExpressVPN. (n.d.). ExpressVPN Trust Center.
https://www.expressvpn.com/trust

[2] ExpressVPN. (n.d.). Lightway: A VPN Protocol by ExpressVPN.
https://www.expressvpn.com/lightway

[3] ExpressVPN. (2025). Lightway's Rust rewrite undergoes two security audits, by Cure53 and Praetorian.
https://www.expressvpn.com/blog/lightway-audits-cure53-praetorian/

[4] ExpressVPN. (n.d.). ExpressVPN TrustedServer Technology.
https://www.expressvpn.com/features/trustedserver

[5] ExpressVPN. (n.d.). VPN Kill Switch: What It Is & How ExpressVPN Keeps You Safe.
https://www.expressvpn.com/features/network-lock

[6] ExpressVPN. (n.d.). How Secure Is VPN Encryption?
https://www.expressvpn.com/what-is-vpn/vpn-encryption

[7] ExpressVPN. (n.d.). Get a VPN With Private DNS.
https://www.expressvpn.com/features/dns

[8] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[9] ExpressVPN. (n.d.). Lightway Rust Open Source Workspace [GitHub repository].
https://github.com/expressvpn/lightway

[10] Cure53. (2024). Audit-Report ExpressVPN Lightway Protocol 10.-11.2024.
https://cure53.de/pentest-report_expressvpn-lightway_2024.pdf

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

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

答案: 检查点 1 – 单项选择

1 问题 1 正确答案: A

教学提示

ExpressVPN 的自定义开源协议是什么? → Lightway

2 问题 2 正确答案: A

教学提示

哪种服务器技术只在易失性 RAM 中运行? → TrustedServer

3 问题 3 正确答案: A

教学提示

如果 VPN 连接意外断开会发生什么? → A) 终止开关阻断流量

4 问题 4 正确答案: A

教学提示

ExpressVPN 为保护隐私注册在哪里? → 英属维尔京群岛

5 问题 5 正确答案: A

教学提示

默认使用哪种对称加密算法? → AES-256-GCM

答案: 检查点 2 – 判断题（正确或错误）

6 **问题 6** 正确答案: 错误

教学提示

TrustedServer 技术将服务器日志存储在硬盘上。

7 **问题 7** 正确答案: 正确

教学提示

ExpressVPN 已接受过第三方安全审计。

8 **问题 8** 正确答案: 错误

教学提示

Lightway 协议构建于 OpenVPN 代码库之上。

9 **问题 9** 正确答案: 正确

教学提示

终止开关在桌面应用上默认开启。

10 **问题 10** 正确答案: 正确

教学提示

ExpressVPN 在每台服务器上都运行私有 DNS。

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. Lightway	E 2. TrustedServer	F 3. 锁	A 4. 群岛
H 5. AES-256	D 6. 已审计	B 7. 泄漏	C 8. DNS

检查点 3: 答案 – 关键术语

1 光速协议	2 可信服务器	3 网络锁	4 群岛
5 对称加密	6 独立审计		

检查点 6 替代活动: 答案 – 词语配对

1 G – 数据泄漏	2 D – 隧道加密	3 H – 网络泄漏	4 A – 隧道协议
5 C – 网络锁	6 E – 对称加密	7 B – 加密协议	8 F – 数据加密

教师讨论提示

关键术语:
检查学生能否用自己的话解释Lightway、TrustedServer和锁，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。

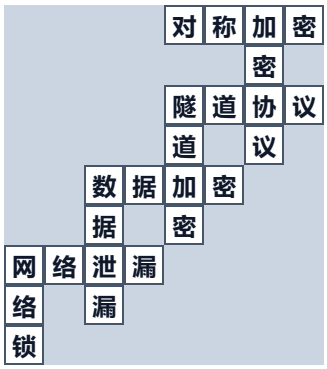
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

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

填字游戏答案



填字游戏答案教师指南

横向

1 横向: 对称加密 加解密双方使用同一密钥、用于保护数据传输的标准，例如 AES-256 (4 字)

3 横向: 隧道协议 规定如何封装并加密隧道内数据的一组规则 (4 字)

4 横向: 数据加密 用密码算法把数据变成他人无法读取的形式 (4 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)

纵向

2 纵向: 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)

3 纵向: 隧道加密 对穿过隧道的数据进行加密保护 (4 字)

4 纵向: 数据泄漏 私有 IP、DNS 或 WebRTC 数据的意外暴露 (4 字)

5 纵向: 网络锁 终止开关的旧名称（英文原名为 Network Lock） (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. 协 隧 议 道 — **隧道协议**
2. 锁 络 网 — **网络锁**
3. 密 对 加 称 — **对称加密**
4. 漏 泄 数 据 — **数据泄漏**
5. 议 加 协 密 — **加密协议**
6. 加 密 隧 道 — **隧道加密**
7. 加 数 密 据 — **数据加密**
8. 网 漏 泄 络 — **网络泄漏**

秘密密码挑战答案

“可信服务器每日清除用户日志”

案例研究答案

A 案例研究 1: 落实仅内存保护 教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一个政府机构查封了一台 ExpressVPN 服务器，以提取用户日志和连接历史。
- 推荐策略与解决方案: 什么都没有。ExpressVPN 的 TrustedServer 技术完全在 RAM 中运行，因此断电时所有数据都会被立即清除。

B 案例研究 2: 不稳定的 Wi-Fi 连接隧道 教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位远程办公者使用的酒店公共 Wi-Fi 每隔几分钟就会断线，而他们正在编辑文档。
- 推荐策略与解决方案: 互联网 Kill Switch 会自动阻止所有互联网流量，直到 VPN 隧道重新建立。