姓名: _____ 日期: _____ 得分: _____

零信任架构与安全

持续验证、网络微隔离、身份与访问管理、最小权限和安全态势检查。

零信任安全学习概览

受保护
数据加密
256 位 AES 标准

合规的
全球标准
GDPR 与 CCPA 框架

零信任
访问策略
多重身份验证

欢迎！ 本活动手册将带你了解零信任架构与安全。你将探索持续验证、网络微隔离、身份访问管理（IAM）、最小权限和会话审计。

练习单检查点

- [ ] **第 1-4 部分: 掌握网络安全和威胁防范。**
- [ ] **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 网络安全指南

URL: https://www.vpn.com/cybersecurity/zero-trust-cyber-security/

你的零信任策略学习路线图

- 了解持续验证的核心原则。
- 实施网络微分段和最小权限访问。
- 配置设备安全态势检查和活动会话审计。

零信任安全指南说明

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。将所学知识应用于零信任架构。 最后完成附加活动: 快速思考。

零信任架构与安全（简介）

零信任安全以严格的“永不信任，始终验证”策略取代旧的网络边界模型。实施微分段、身份与访问管理（IAM）、最小权限和安全状态检查，可阻止威胁的横向移动。

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. 零信任安全的核心原则是什么?
   - A. 永不信任，始终验证每一个访问请求，无论其来源
   - B. 假定企业防火墙内的所有流量都是安全的
   - C. 为提高速度而不加密存储数据库文件
   - D. 仅使用 SPF 记录强制执行电子邮件认证

2. 什么是网络微分段?
   - A. 将网络划分为小型隔离区域以遏制横向移动
   - B. 在数据传输期间加密网卡
   - C. 将所有本地服务器连接到单个公共 IP 地址
   - D. 监控浏览器会话中的用户击键

3. 什么是最小权限原则?
   - A. 将用户访问权限限制在工作所必需的范围内
   - B. 默认授予每个用户所有系统权限
   - C. 允许匿名登录企业数据库服务器
   - D. 配置不设密码的公共 Wi-Fi 路由器

4. 什么是身份与访问管理（IAM）?
   - A. 管理数字身份和控制系统权限的框架
   - B. 扫描本地文件目录的防病毒工具
   - C. 使用物理隔离介质的备份存储系统
   - D. 一种拒绝伪造域名的电子邮件网关协议

5. 持续身份验证是什么意思?
   - A. 在活动会话期间反复验证用户身份和设备状态
   - B. 每 10 分钟更改一次主密码
   - C. 使用多种算法对数据库记录进行哈希处理
   - D. 使用 TLS 密钥加密网络传输数据包

检查点 2: 判断正误挑战

6 问题 6

6. 零信任假定企业防火墙内的所有流量都是安全的。

○ 正确 ○ 错误

7 问题 7

7. 微隔离限制了攻击者在内部服务器之间横向移动的能力。

○ 正确 ○ 错误

8 问题 8

8. 最小权限默认授予对所有数据库文件的访问权限。

○ 正确 ○ 错误

9 问题 9

9. 持续验证会在整个登录会话期间验证设备健康状况和凭据。

○ 正确 ○ 错误

10 问题 10

10. 实施零信任可以降低企业登录凭据被盗的影响。

○ 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. 要求在每个访问点提供凭证称为持续 _____ 。
2. 把企业网络划分为很小的区域称为微 _____ 。
3. 配置数字身份和访问控制使用 _____ 系统。
4. 限制用户的访问许可，遵循最小 _____ 原则。
5. 评估已连接设备的健康状况需要扫描设备 _____ 。
6. 记录并审查活跃会话属于安全 _____ 。

词汇词库

持续验证　防火墙　访问审计　路由器　权限　身份管理　网络分段　状态

在此写下你的答案:

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

检查点 4: 安全概念配对

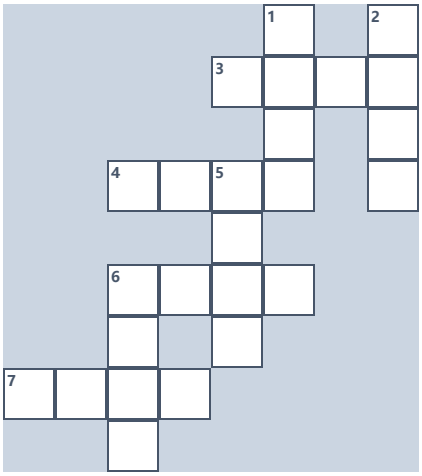
定义配对

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. 验证	**A**	管理用户凭据的访问。（C）
	2. 分段	**B**	最小访问权限原则。（D）
	3. IAM	**C**	路由网络数据包流量。
	4. 权限	**D**	外部网络屏障防护。
	5. 安全状态	**E**	审查已记录的访问会话。
	6. 审计	**F**	划分内部网络区域。
	7. 防火墙	**G**	始终检查用户凭据。
	8. 路由器	**H**	评估设备健康状态。

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. 审查已记录的访问会话 (4)

4. 最少访问权限原则 (4)

6. 管理用户凭证与访问权限 (4)

7. 始终检查用户凭证 (4)

纵向

1. 用户被允许访问哪些资源的授权范围 (4)

2. 按时间顺序记录谁在何时做了什么的日志 (4)

5. 为不同用户分配、调整和回收各项操作权限 (4)

6. 确认用户确实是其所声称的那个人 (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: 审查已记录的访问会话 (4 字):

4 横向: 最少访问权限原则 (4 字):

6 横向: 管理用户凭证与访问权限 (4 字):

7 横向: 始终检查用户凭证 (4 字):

纵向

1 纵向: 用户被允许访问哪些资源的授权范围 (4 字):

2 纵向: 按时间顺序记录谁在何时做了什么的日志 (4 字):

5 纵向: 为不同用户分配、调整和回收各项操作权限 (4 字):

6 纵向: 确认用户确实是其所声称的那个人 (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 道 安 息 续 用 连 续 人 小 公 务 墙 统
击 议 隐 软 墙 全 人 服 访 安 传 协 系 私 志
务 限 器 安 份 私 问 公 份 问 信 险 户 软 名
务 权 数 传 日 络 隐 域 浏 地 审 访 日 攻 传
录 小 安 设 名 持 器 名 权 证 计 计 软 限 保
软 最 墙 密 理 续 问 权 保 风 管 认 软 限 件
攻 加 道 输 共 验 用 防 限 址 数 网 数 加 系
最 防 名 最 议 证 限 隧 协 管 务 备 证 域 务
限 问 份 身 议 件 统 隐 身 身 理 设 管 输 隧
权 人 护 加 输 件 攻 接 传 据 持 服 公 计 览
问 身 份 验 证 加 日 持 保 协 私 志 服 身 审
访 务 备 权 身 统 加 道 数 网 志 风 服 计 议
络 务 攻 务 份 信 私 问 服 管 设 证 日 用 问
传 日 公 信 管 备 记 户 络 络 备 志 击 份 统
隧 限 件 名 理 理 隧 传 码 份 审 数 保 传 权

词汇列表

持续验证 **身份验证** **身份管理** **权限管理** **最小权限** **访问权限** **访问审计** **审计日志**

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. 持续验证
B. 身份验证
C. 身份管理
D. 权限管理
E. 最小权限
F. 访问权限
G. 访问审计
H. 审计日志

定义与配对字段
1. 审查已记录的访问会话。
2. 用户被允许访问哪些资源的授权范围。
3. 为不同用户分配、调整和回收各项操作权限。
4. 确认用户确实是其所声称的那个人。
5. 按时间顺序记录谁在何时做了什么的日志。
6. 最少访问权限原则。
7. 管理用户凭证与访问权限。
8. 始终检查用户凭证。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的网络安全概念和术语。把答案写在提供的输入框中。

1. 验 持 证 续
2. 身 管 理 份
3. 限 最 权 小
4. 计 审 访 问
5. 证 身 验 份
6. 管 理 权 限
7. 权 访 限 问
8. 审 志 日 计

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	你绝不应分享的信息			
2	你今天就可以开始的安全习惯			
3	设备上被检查的内容			
4	会被记录的内容			
5	与网络安全相关的词语			
6	零信任会检查的内容			
7	日常生活中出示身份证件的地方			
8	证明确实是你本人的方法			
9	数据泄露后要做的事			
10	电脑被感染的迹象			
11	更新软件的原因			
12	公司内的访问级别			
13	你知道的安全工具			
14	网络可以划分成的区域			
15	关于信任的谚语			

检查点 8: 网络安全案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: 过渡到零信任网络架构



情景: 一家大型企业目前使用扁平化的内部网络，本地网络上的任何设备都可以访问所有公司服务器和数据库。

讨论问题: 设计一个网络微隔离策略来限制横向移动。

案例研究 2: 部署最小权限访问控制



情景: 审计日志显示，临时数据库用户和低级别员工拥有关键会计数据库的全局读写权限。

讨论问题: 审计并限制数据库 IAM 权限，以落实最小权限原则。

检查点 9: 破解密码

网络安全专业人员保护网络资产免受网络威胁行为者的攻击。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

限=1 安=2 访=3 信=4 全=5 架=6 最=7 身=8 证=9 日=10

零=11 任=12 志=13 权=14 管=15 络=16 持=17 份=18 构=19 网=20

小=21 审=22 问=23 理=24 续=25 验=26 终=27 计=28 数=29 始=30

30	27	26	9		2	5		11	4	12	6	19

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: 基础网络安全常见问题 (A 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q1: 什么是零信任?

零信任是一种安全框架，假定威胁既存在于网络边界之外，也存在于其内部，要求对每个请求进行验证。 [1]

Q2: 零信任的核心规则是什么?

永不信任，始终验证。

Q3: 什么是微分段?

将网络划分为小型、安全的逻辑网段，以控制流量并遏制入侵。

Q4: 什么是最小权限?

只授予用户完成其具体工作任务所需的最低访问权限。 [2]

Q5: IAM 代表什么?

身份与访问管理。

检查点 10: 基础网络安全常见问题 (B 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q6: 设备合规检查有什么帮助?

它会在允许访问之前，验证设备已打补丁、正在运行杀毒软件且处于安全状态。

Q7: 什么是横向移动?

攻击者从最初被入侵的节点出发，在网络中逐步移动到更高价值系统的过程。

Q8: 零信任会取代防火墙吗?

不会，它反而通过增加以身份为中心的检查和内部分段防火墙来增强这些措施。

Q9: 什么是持续身份验证?

在整个活动登录会话期间持续验证用户身份，而不仅仅是在最初登录时。

Q10: 为什么扁平网络很危险?

在扁平网络中，只要有一个节点被攻陷，攻击者就能轻易访问网络上的任何数据库。

检查点 10: 高级安全常见问题 (C 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q1: 零信任如何应对边界模型?

它取代了过时的“城堡与护城河”模型，将防御从边界网络转移到具体的用户身份和资源上。

Q2: 什么是策略决策点（PDP）?

根据安全规则评估授权请求，以决定是否授予访问权限的系统组件。

Q3: 什么是策略执行点 (PEP)?

根据 PDP 的决定，在物理上允许或阻止连接请求的系统节点（如网关或代理）。

Q4: 基于角色的访问控制 (RBAC) 如何支持零信任?

RBAC 将权限归入特定角色，有助于防止用户继承过多的管理权限。

Q5: 什么是情境化访问控制?

利用地理位置、设备状态和登录时间等辅助线索评估登录请求，以判断风险。

检查点 10: 高级安全常见问题 (D 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q6: 微分段与标准 VLAN 有何不同?

VLAN 在第 2 层将网络划分为较大的逻辑网段，而微隔离则使用软件策略来隔离单个工作负载。

Q7: 什么是即时 (JIT) 访问?

临时授予提升的管理权限，并在任务完成后自动撤销。

Q8: 如何在零信任框架中保护 API 安全?

通过要求使用经过加密签名的 OAuth 令牌，并在每个 API 网关审计请求签名。

Q9: 什么是零信任网络访问 (ZTNA) 客户端?

一种软件代理，向特定应用而非原始网络子网建立安全的加密出站连接。

Q10: 日志审计如何协助零信任?

持续记录日志让自动化安全分析工具能够检测异常并立即暂停恶意登录。

第 11 部分: 10 个现实中的网络安全事实与洞察

回顾有关安全漏洞、防御机制和合规标准的真实事实。

1. 安全洞察

零信任架构以以身份为中心的验证规则取代传统的“城堡护城河”模型。

2. 安全洞察

网络微分段通过将工作负载隔离到小型受保护区域，缩小恶意软件可触及的范围。

3. 安全洞察

零信任侧重于保护资产、服务和账户等资源，而不是网络分段。 [1]

4. 安全洞察

最小权限访问策略可降低内部威胁导致核心数据库数据外流的风险。

5. 安全洞察

设备状态验证会实时检查操作系统补丁级别和杀毒软件的运行状态。

6. 安全洞察

零信任网络访问（ZTNA）代理可以取代或补充企业 VPN，以限制用户访问范围。

7. 安全洞察

即时（JIT）管理权限委派可降低域控制器上的凭据被盗风险。

8. 安全洞察

持续验证会记录并审计会话行为，暂停表现出异常脚本执行模式的用户。

9. 安全洞察

一旦管理员凭据泄露，传统的边界防御就无法阻止横向攻击。

10. 安全洞察

NIST 特别出版物 800-207（2020 年）给出了零信任架构的抽象定义及部署模型。 [1]

技术参考资料与来源

本学习指南和互动谜题根据全球 NIST、OWASP 以及数据隐私合规标准编写。

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] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

答案: 检查点 1 – 单项选择

1 问题 1 正确答案: A

教学提示

零信任安全的核心原则是什么？ → 永不信任，始终验证每一个访问请求，无论其来源

2 问题 2 正确答案: A

教学提示

什么是网络微分段？ → 将网络划分为小型隔离区域以遏制横向移动

3 问题 3 正确答案: A

教学提示

什么是最小权限原则？ → 将用户访问权限限制在工作所必需的范围内

4 问题 4 正确答案: A

教学提示

什么是身份与访问管理（IAM）？ → 管理数字身份和控制系统权限的框架

5 问题 5 正确答案: A

教学提示

持续身份验证是什么意思？ → 在活动会话期间反复验证用户身份和设备状态

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

错误: 零信任不会基于网络位置（无论在内部还是外部）给予任何隐式信任。

7 问题 7 正确答案: 正确

教学提示

正确: 小型隔离区域限制了入侵者在服务器之间的移动范围。

8 问题 8 正确答案: 错误

教学提示

错误: 最小权限只授予每个角色所需的最低访问权限。

9 问题 9 正确答案: 正确

教学提示

持续验证会在整个登录会话期间验证设备健康状况和凭据。

10 问题 10 正确答案: 正确

教学提示

实施零信任可以降低企业登录凭据被盗的影响。

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. 验证	F 2. 分段	A 3. IAM	B 4. 权限
H 5. 安全状态	E 6. 审计	D 7. 防火墙	C 8. 路由器

检查点 3: 答案 – 关键术语

1 持续验证	2 网络分段	3 身份管理	4 权限
5 状态	6 访问审计		

检查点 6 替代活动: 答案 – 词语配对

1 G – 访问审计	2 F – 访问权限	3 D – 权限管理	4 B – 身份验证
5 H – 审计日志	6 E – 最小权限	7 C – 身份管理	8 A – 持续验证

教师讨论提示

关键术语:
检查学生能否用自己的话解释验证、分段和IAM，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。

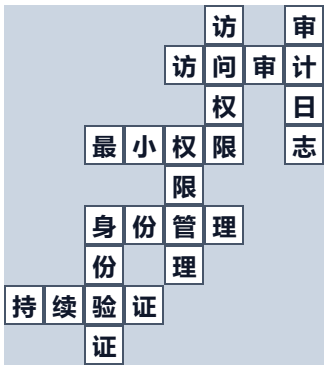
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	址	道	安	息	续	用	连	续	人	小	公	务	墙	统
击	议	隐	软	墙	全	人	服	访	安	传	协	系	私	志
务	限	器	安	份	私	问	公	份	问	信	险	户	软	名
务	权	数	传	日	络	隐	域	浏	地	审	访	日	攻	传
录	小	安	设	名	持	器	名	权	证	计	计	软	限	保
软	最	墙	密	理	续	问	权	保	风	管	认	软	限	件
攻	加	道	输	共	验	用	防	限	址	数	网	数	加	系
最	防	名	最	议	证	限	隧	协	管	务	备	证	域	务
限	问	份	身	议	件	统	隐	身	身	理	设	管	输	隧
权	人	护	加	输	件	攻	接	传	据	持	服	公	计	览
问	身	份	验	证	加	日	持	保	协	私	志	服	身	审
访	务	备	权	身	统	加	道	数	网	志	风	服	计	议
络	务	攻	务	份	信	私	问	服	管	设	证	日	用	问
传	日	公	信	管	备	记	户	络	络	备	志	击	份	统
隧	限	件	名	理	理	隧	传	码	份	审	数	保	传	权

填字游戏答案



填字游戏答案教师指南

横向

3 横向: 访问审计 审查已记录的访问会话 (4 字)

4 横向: 最小权限 最少访问权限原则 (4 字)

6 横向: 身份管理 管理用户凭证与访问权限 (4 字)

7 横向: 持续验证 始终检查用户凭证 (4 字)

纵向

1 纵向: 访问权限 用户被允许访问哪些资源的授权范围 (4 字)

2 纵向: 审计日志 按时间顺序记录谁在何时做了什么的日志 (4 字)

5 纵向: 权限管理 为不同用户分配、调整和回收各项操作权限 (4 字)

6 纵向: 身份验证 确认用户确实是其所声称的那个人 (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. 验持证续 → **持续验证**
2. 身管理份 → **身份管理**
3. 限最权小 → **最小权限**
4. 计审访问 → **访问审计**
5. 证身验份 → **身份验证**
6. 管理权限 → **权限管理**
7. 权访限问 → **访问权限**
8. 审志日计 → **审计日志**

秘密密码挑战答案

“始终验证安全零信任架构”

案例研究答案

A 案例研究 1: 过渡到零信任网络架构

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家大型企业目前使用扁平的内部网络，本地网络上的任何设备都可以访问所有企业服务器和数据库。
- 推荐策略与解决方案: 将扁平网络划分为相互隔离的部门区域。安装内部防火墙来控制区域之间的流量，并要求所有访问都进行连接令牌验证。

B 案例研究 2: 部署最小权限访问控制

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 审计日志显示，临时数据库用户和低级别员工拥有关键会计数据库的全局读写权限。
- 推荐策略与解决方案: 撤销所有全局管理权限。实施基于角色的访问控制（RBAC）以匹配确切的工作角色，并建立每周自动化的权限审查。