姓名: _____ 日期: _____ 得分: _____

企业 VPN

实施零信任网络访问、专用网关节点和集中式企业管理控制。

企业 VPN 网络学习概览

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企业 VPN 网络。你将探索零信任架构、专用静态 IP 网关、管理员控制台、配置部署和站点到站点 IPsec 隧道。

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/best-vpn-for-business/enterprise/

你的企业 VPN 网络学习路线图

- 实施零信任网络访问（ZTNA）框架。
- 为白名单过滤器配置专用服务器网关 IP 地址。
- 管理集中的企业管理面板和用户席位列表。
- 审计网络访问日志和用户连接历史。
- 配置单点登录（SSO）和多因素认证规则。
- 设置分支到分支的站点到站点 IPsec 隧道。

企业 VPN 网络说明

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和站点到站点 IPsec。 最后完成附加活动: 快速思考。

零信任架构与专用网关（简介）

企业 VPN 通过过渡到零信任网络访问 (ZTNA) 框架并对专用静态 IP 网关设置白名单来保护企业资产。IT 经理利用集中式管理控制台来编排站点到站点 IPsec 隧道和单点登录 (SSO) 链接。

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. 哪种安全模型正在取代传统的企业 VPN?
   - A) 零信任
   - B) 多跳
   - C) 点对点
   - D) 单一网关

2. 限制数据库仅供公司服务器访问需要哪项功能?
   - A) 专用 IP
   - B) 动态路由
   - C) 分应用隧道
   - D) DNS 代理

3. 哪种协议是企业站点到站点隧道的标准?
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. 哪个中央工具允许管理员管理员工席位?
   - A) 管理控制台
   - B) 注册表项
   - C) 路由器固件
   - D) 系统日志

5. 哪种身份验证标准允许通过 Okta 或 Microsoft Entra ID 登录?
   - A) 单点登录
   - B) 共享密钥
   - C) EPP 身份验证
   - D) WEP 密钥

检查点 2: 判断正误挑战

6 问题 6

6. 零信任网络访问只有在持续验证设备可信度之后才授予网络准入。

○ 正确 ○ 错误

7 问题 7

7. 专用 IP 网关会让员工流量与随机的公共消费者用户混在一起路由。

○ 正确 ○ 错误

8 问题 8

8. 集中式管理控制台让 IT 管理员能够立即撤销单个员工的席位。

○ 正确 ○ 错误

9 问题 9

9. IPsec 是一种轻量级协议，不支持站点到站点的网络隧道。

○ 正确 ○ 错误

10 问题 10

10. 单点登录（SSO）借助企业身份提供商实现安全的员工身份验证。

○ 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. 现代安全架构要求对每一次 _____ 都进行验证，取代了传统隧道。
2. 为了限制数据库访问，企业会配置一个 _____ 网关地址。
3. 分支机构通过站点到站点的 _____ 隧道安全相连。
4. 管理员为员工统一配置账户保护策略，以加强 _____ 。
5. 集成 Okta 后，员工可以通过企业 _____ 进行身份验证。
6. 为保护登录，企业门户强制要求采用 _____ 。

词汇词库

单点登录　登录安全　多重验证　管理控制台　零信任　网络访问　专用IP　IPsec

在此写下你的答案:

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

检查点 4: 关键概念配对

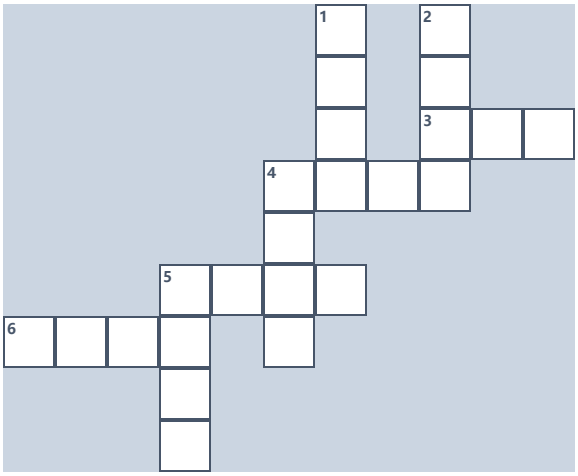
定义配对

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**	分配员工 VPN 访问许可。
	2. 专用 IP	**B**	Okta 和 Entra ID 的身份关联。
	3. IPSEC	**C**	需要额外令牌的登录安全措施。
	4. 管理控制台	**D**	静态白名单网关地址。
	5. 单点登录	**E**	站点到站点隧道标准。
	6. 多重验证	**F**	网络入口路由节点。
	7. 网关	**G**	中央 IT 管理员席位门户。
	8. 供应	**H**	持续信任验证框架。

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. 用于确认身份的一次性数字 (3)

4. 确认用户身份后才允许进入的步骤 (4)

5. 保护网络及其数据不受攻击 (4)

6. 连接多个办公地点的网络 (4)

纵向

1. 一次验证即可使用多个应用的方式 (4)

2. 需要两种以上证明才能登录的安全措施 (4)

4. 保护账户入口不被冒用 (4)

5. 用户进入内部资源的过程 (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: 用于确认身份的一次性数字 (3 字):

4 横向: 确认用户身份后才允许进入的步骤 (4 字):

5 横向: 保护网络及其数据不受攻击 (4 字):

6 横向: 连接多个办公地点的网络 (4 字):

纵向

1 纵向: 一次验证即可使用多个应用的方式 (4 字):

2 纵向: 需要两种以上证明才能登录的安全措施 (4 字):

4 纵向: 保护账户入口不被冒用 (4 字):

5 纵向: 用户进入内部资源的过程 (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 地 公 安 信 览 器 隐 记 输 站 理 务 防 攻
险 名 护 系 防 全 输 服 多 安 备 域 攻 隐 重
服 络 器 安 证 隐 接 传 证 重 户 份 户 系 址
服 网 数 备 多 络 护 地 人 访 验 接 多 份 管
浏 点 安 软 址 登 务 址 登 墙 单 证 系 验 息
击 站 防 密 设 录 访 网 息 身 件 墙 击 登 统
风 加 公 管 传 验 器 议 络 地 数 网 数 加 险
验 协 址 站 协 证 登 公 域 访 务 软 墙 址 服
录 接 证 认 名 统 击 护 认 认 问 统 设 管 公
登 输 保 据 理 系 风 连 备 数 浏 服 理 单 隧
点 登 录 安 全 加 多 浏 息 名 隐 重 服 认 验
单 务 软 录 网 击 据 共 全 网 重 身 服 证 名
络 务 风 务 络 户 隐 访 码 设 统 墙 码 器 接
备 多 理 户 安 软 道 用 络 络 软 险 证 击 公
验 统 址 设 全 公 备 码 证 点 数 息 备 录 记

词汇列表

登录验证 **登录安全** **网络安全** **网络访问** **站点网络** **单点登录** **多重验证** **验证码**

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. 登录验证
B. 登录安全
C. 网络安全
D. 网络访问
E. 站点网络
F. 单点登录
G. 多重验证
H. 验证码

定义与配对字段
1. 保护账户入口不被冒用。
2. 需要两种以上证明才能登录的安全措施。
3. 用于确认身份的一次性数字。
4. 一次验证即可使用多个应用的方式。
5. 保护网络及其数据不受攻击。
6. 确认用户身份后才允许进入的步骤。
7. 连接多个办公地点的网络。
8. 用户进入内部资源的过程。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出本练习单的关键概念。把答案写在提供的输入框中。

1. 验 登 证 录 _____

2. 网 安 全 络 _____

3. 络 站 网 点 _____

4. 证 验 多 重 _____

5. 全 登 安 录 _____

6. 访 问 网 络 _____

7. 登 单 录 点 _____

8. 码 证 验 _____

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	公司每天使用的工具			
2	VPN 可以隐藏的内容			
3	IT 部门中的角色			
4	描述零信任的词语			
5	安全登录的方法			
6	为员工提供 VPN 的原因			
7	发生安全漏洞后要做的事			
8	旅行时使用 VPN 的原因			
9	安全远程办公的规则			
10	公司必须保护的数据			
11	可能中断视频会议的因素			
12	可以使用 VPN 的设备			
13	你知道的办公软件			
14	员工办公的地点			
15	员工可能拥有的设备			

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: 零信任迁移



情景: 一家企业希望通过持续验证设备合规证书、防火墙状态和用户位置来保护其本地服务器，而不是信任网络内部的任何人。

讨论问题: IT 安全总监应实施什么框架来实现这一目标?

案例研究 2: 网关限制



情景: 一家公司在云端托管私有财务数据库。他们希望阻止公共互联网访问管理面板，只允许来自经过验证的公司终端的登录。

讨论问题: 数据库管理员应在云防火墙上设置什么网络配置?

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

信=1 登=2 多=3 联=4 每=5 设=6 点=7 访=8 任=9 加=10

网=11 全=12 安=13 台=14 问=15 码=16 络=17 证=18 验=19 数=20

务=21 服=22 备=23 密=24 录=25 站=26 重=27 零=28 据=29 单=30

28	1	9	19		18	5	14	4		11	6	23

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: 什么是企业 VPN?

专为企业设计的安全网络隧道，让远程工作者可通过集中管理访问公司网络。

Q2: 零信任与传统 VPN 有何不同?

传统 VPN 信任隧道内的任何人，而零信任会持续验证每台设备和每个用户连接。

Q3: 企业 VPN 中的专用 IP 是什么?

仅为你的企业预留的静态 IP 地址，让你可以将其加入白名单以安全访问云数据库。

Q4: 单点登录 (SSO) 对商业 VPN 为什么重要?

单点登录（SSO）允许员工使用企业凭据（如 Okta 或 Microsoft Entra ID）安全登录。

Q5: 什么是站点到站点 VPN?

通过公共互联网使用 IPsec 连接两个实体办公室（如分公司和总部）的隧道。

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: 管理控制台的功能是什么?

供 IT 管理员使用的仪表板，用于添加或移除员工席位、分配网关并监控活动连接。

Q7: MFA 如何保护商业 VPN?

通过要求提供二次验证码（如验证器应用令牌），以防止他人使用被泄露的密码未经授权进入。

Q8: 我可以审计员工的连接历史吗?

是的，企业 VPN 会记录连接时间戳、时长和分配的 IP，用于合规审计。

Q9: ZTNA 是什么?

零信任网络访问是一种安全模型，只授予对特定应用的访问权限，而不是整个网络。

Q10: 网关节点的作用是什么?

它们充当远程流量的安全入口，将数据直接路由到企业私有服务器。

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: IPsec 如何保护站点到站点的企业通信?

IPsec 使用封装安全有效载荷（ESP）在网络层加密流量，以确保数据的机密性和完整性。

Q2: 为什么传统的基于边界的安全模式对远程办公人员不再有效?

因为员工会从多个地点和设备访问数据，使得单一的网络防火墙边界已经过时。

Q3: IT 经理如何实现自动化配置?

通过在身份提供商（Okta）与 VPN 管理控制台之间映射 SCIM 协议，以同步用户目录。

Q4: 在企业环境中使用分应用隧道有什么好处?

它将本地 SaaS 流量（如 Microsoft 365）放在 VPN 隧道之外路由，为私有数据库保留公司网关带宽。

Q5: 设备合规检查如何验证终端安全?

VPN 客户端在连接前会扫描设备，验证防火墙已启用、杀毒软件正在运行且操作系统补丁为最新。

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: NAT 穿透在企业 VPN 部署中起什么作用?

NAT-T 将 IPsec 数据包封装在 UDP 中，使其能够穿过家用路由器和防火墙而不会断开连接。

Q7: 企业如何避免网关带宽瓶颈?

通过部署多个区域网关节点，并使用负载均衡器在它们之间平衡传入的用户流量。

Q8: 为什么静态 IP 白名单比动态白名单更受青睐?

静态白名单可阻止未经授权的外部 IP 尝试连接握手，从而大幅减少攻击面。

Q9: 基于证书的身份验证在企业 VPN 中起什么作用?

它验证安装在公司管理设备上的唯一数字证书，从而阻止未受管理的个人电脑。

Q10: ZTNA 如何降低横向移动风险?

通过将用户会话隔离到特定的授权资源，防止黑客在某个节点被攻破时在网络中横向移动。

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

零信任架构会持续验证每台尝试网络连接的设备的安全状态。

2. VPN 洞察

专用 IP 网关允许企业通过对静态地址设置白名单来锁定云数据库。

3. VPN 洞察

IPsec 是配置安全的站点到站点办公网络隧道的行业标准协议。

4. VPN 洞察

管理控制台让 IT 部门可以配置、管理和审计员工的 VPN 访问席位。

5. VPN 洞察

单点登录（SSO）将 VPN 访问与 Okta 和 Entra ID 等企业身份提供商集成。

6. VPN 洞察

多重身份验证可阻止使用被盗密码密钥发起的未授权连接尝试。

7. VPN 洞察

分应用隧道通过把公共 SaaS 流量排除在加密隧道之外来优化企业带宽。

8. VPN 洞察

设备状态检查会在授予访问企业服务器的权限之前，验证本地安全设置。

9. VPN 洞察

SCIM 目录同步可自动执行员工入职和离职的访问控制。

10. VPN 洞察

零信任网络访问将用户访问限制在特定的授权应用上，防止在网络内横向移动。

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). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

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

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

答案: 检查点 1 – 单项选择

1 **零信任** ZTNA 模型 正确答案: A

教学提示

零信任模型在允许进入网络前会持续验证设备合规性。引用来源: NIST Zero Trust。

2 **专用 IP** 静态 IP 正确答案: A

教学提示

专用 IP 地址允许对网关设置白名单，以阻止公共流量。引用: Dedicated IP Guide。

3 **IPsec 标准** IPSEC 隧道 正确答案: A

教学提示

IPsec 是用于分支机构站点到站点隧道的标准协议。引用来源: IPsec Tunneling。

4 **IT 分配** 管理控制台 正确答案: A

教学提示

集中式管理仪表板让 IT 管理员能够分配席位许可。引用: CISA 指南。

5 **问题 5** 正确答案: A

教学提示

哪种身份验证标准允许通过 Okta 或 Microsoft Entra ID 登录？ → 单点登录

答案: 检查点 2 – 判断题（正确或错误）

6 **零信任** ZTNA 检查 正确答案: 正确

教学提示

零信任模型在允许进入网络前会持续验证设备合规性。引用来源: NIST Zero Trust。

7 **问题 7** 正确答案: 错误

教学提示

专用 IP 是为单个企业保留的，因此其流量不会与其他用户混在一起。

8 **IT 分配** IT 管理员席位 正确答案: 正确

教学提示

集中式管理仪表板让 IT 管理员能够分配席位许可。引用: CISA 指南。

9 **IPsec 标准** 站点到站点 正确答案: 错误

教学提示

IPsec 是用于分支机构站点到站点隧道的标准协议。引用来源: IPsec Tunneling。

10 **Okta SSO 链接** SSO 登录 正确答案: 正确

教学提示

单点登录（SSO）将 VPN 登录与 Okta 等企业目录集成。引用: Okta SSO。

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. 零信任	D 2. 专用 IP	E 3. IPSEC	G 4. 管理控制台
B 5. 单点登录	C 6. 多重验证	F 7. 网关	A 8. 供应

检查点 3: 答案 – 关键术语

1 网络访问	2 专用IP	3 IPsec	4 登录安全
5 单点登录	6 多重验证		

检查点 6 替代活动: 答案 – 词语配对

1 B – 登录安全	2 G – 多重验证	3 H – 验证码	4 F – 单点登录
5 C – 网络安全	6 A – 登录验证	7 E – 站点网络	8 D – 网络访问

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、专用 IP和IPSEC，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。

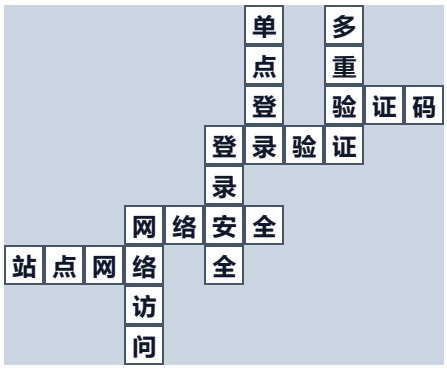
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	地	公	安	信	览	器	隐	记	输	站	理	务	防	攻
险	名	护	系	防	全	输	服	多	安	备	域	攻	隐	重
服	络	器	安	证	隐	接	传	证	重	户	份	户	系	址
服	网	数	备	多	络	护	地	人	访	验	接	多	份	管
浏	点	安	软	址	登	务	址	登	墙	单	证	系	验	息
击	站	防	密	设	录	访	网	息	身	件	墙	击	登	统
风	加	公	管	传	验	器	议	络	地	数	网	数	加	险
验	协	址	站	协	证	登	公	域	访	务	软	墙	址	服
录	接	证	认	名	统	击	护	认	认	问	统	设	管	公
登	输	保	据	理	系	风	连	备	数	浏	服	理	单	隧
点	登	录	安	全	加	多	浏	息	名	隐	重	服	认	验
单	务	软	录	网	击	据	共	全	网	重	身	服	证	名
络	务	风	务	络	户	隐	访	码	设	统	墙	码	器	接
备	多	理	户	安	软	道	用	络	络	软	险	证	击	公
验	统	址	设	全	公	备	码	证	点	数	息	备	录	记

填字游戏答案



填字游戏答案教师指南

横向

3 横向: 验证码 用于确认身份的一次性数字 (3 字)

4 横向: 登录验证 确认用户身份后才允许进入的步骤 (4 字)

5 横向: 网络安全 保护网络及其数据不受攻击 (4 字)

6 横向: 站点网络 连接多个办公地点的网络 (4 字)

纵向

1 纵向: 单点登录 一次验证即可使用多个应用的方式 (4 字)

2 纵向: 多重验证 需要两种以上证明才能登录的安全措施 (4 字)

4 纵向: 登录安全 保护账户入口不被冒用 (4 字)

5 纵向: 网络访问 用户进入内部资源的过程 (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 登 证 录 — **登录验证**
2. 网 安 全 络 — **网络安全**
3. 络 站 网 点 — **站点网络**
4. 证 验 多 重 — **多重验证**
5. 全 登 安 录 — **登录安全**
6. 访 问 网 络 — **网络访问**
7. 登 单 录 点 — **单点登录**
8. 码 证 验 — **验证码**

秘密密码挑战答案

“零信任验证每台联网设备”

案例研究答案

A 案例研究 1: 零信任迁移

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家企业想通过持续验证设备合规证书、防火墙状态和用户位置来保护本地服务器，而不是信任网络内部的任何人。
- 推荐策略与解决方案: 主管应迁移到零信任网络访问（ZTNA）模式，该模式会持续执行基于上下文的安全检查。

B 案例研究 2: 网关限制

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家公司在云端托管私有的财务数据库。他们想阻止对管理面板的所有公共互联网访问，仅允许来自经过验证的公司终端的登录。
- 推荐策略与解决方案: 管理员应在企业 VPN 上配置专用 IP 网关，并将此静态地址加入云数据库防火墙的白名单。