नाम: _____ दिनांक: _____ अंक: _____

एंटरप्राइज़ VPN

Zero Trust नेटवर्क एक्सेस, समर्पित गेटवे नोड और केंद्रीकृत कॉर्पोरेट एडमिन नियंत्रण लागू करना।

एंटरप्राइज़ VPN नेटवर्क सीखने का अवलोकन

शिक्षार्थी
छात्र का दर्जा
नेटवर्क डिफ़ेंडर ट्रैक

सुरक्षित
कनेक्शन की स्थिति
डेटा पैकेट की ढाल बनाना

सक्रिय
लीक सुरक्षा
DNS और IPv6 लीक सुरक्षा

स्वागत है! यह गतिविधि पैकेट आपको एंटरप्राइज़ VPN नेटवर्क से परिचित कराता है। आप Zero Trust आर्किटेक्चर, समर्पित स्टैटिक IP गेटवे, एडमिनिस्ट्रेटर कंसोल, प्रोविज़निंग और साइट-टू-साइट IPsec टनल का अध्ययन करेंगे।

वर्कशीट चेकपॉइंट

- [ ] **भाग 1-4: VPN और नेटवर्क सुरक्षा कॉन्फ़िगरेशन में महारत हासिल करें।**
- [ ] **भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।**
- [ ] **भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।**
- [ ] **भाग 10: बुनियादी और उन्नत FAQ पेज देखें।**
- [ ] **भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।**
- [ ] **अतिरिक्त: झटपट सोचें चुनौती।**

VPN.com सर्वश्रेष्ठ VPN गाइड खोलें

URL: https://www.vpn.com/hi/vpn/business-enterprise-ke-liye-best-vpn/

आपका एंटरप्राइज़ VPN नेटवर्क लर्निंग रोडमैप

- Zero Trust Network Access (ZTNA) फ़्रेमवर्क लागू करें।
- व्हाइटलिस्ट फ़िल्टर के लिए समर्पित सर्वर गेटवे IP पते कॉन्फ़िगर करें।
- केंद्रीकृत कॉर्पोरेट एडमिन पैनल और उपयोगकर्ता सीट सूचियाँ प्रबंधित करें।
- नेटवर्क एक्सेस लॉग और उपयोगकर्ता कनेक्शन इतिहास का ऑडिट करें।
- Single Sign-On (SSO) और बहु-कारक प्रमाणीकरण नियम कॉन्फ़िगर करें।
- ब्रांच-टू-ब्रांच साइट-टू-साइट IPsec टनल सेट करें।

एंटरप्राइज़ VPN नेटवर्क निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को Zero Trust और साइट-टू-साइट IPsec पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

ज़ीरो ट्रस्ट आर्किटेक्चर और समर्पित गेटवे (परिचय)

एंटरप्राइज़ VPN, Zero Trust Network Access (ZTNA) फ़्रेमवर्क अपनाकर और डेडिकेटेड स्थिर IP गेटवे को व्हाइटलिस्ट करके कॉर्पोरेट संपत्तियों को सुरक्षित करते हैं। IT मैनेजर साइट-टू-साइट IPsec टनल और सिंगल साइन-ऑन (SSO) लिंक को समन्वित करने के लिए केंद्रीकृत एडमिन कंसोल का उपयोग करते हैं।

प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही उत्तर चुनें या लिखें।

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. कौन-सा सुरक्षा मॉडल पुराने एंटरप्राइज़ VPN की जगह ले रहा है?
   - A) Zero Trust
   - B) Multi-hop
   - C) पीयर-टू-पीयर
   - D) एकल गेटवे

2. डेटाबेस एक्सेस को कंपनी के सर्वरों तक सीमित करने के लिए कौन-सी सुविधा ज़रूरी है?
   - A) डेडिकेटेड IP
   - B) डायनेमिक रूटिंग
   - C) स्प्लिट टनल
   - D) DNS प्रॉक्सी

3. कॉर्पोरेट साइट-टू-साइट टनल के लिए मानक प्रोटोकॉल कौन-सा है?
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. कर्मचारियों की सीटें प्रबंधित करने के लिए प्रशासकों को कौन-सा केंद्रीय टूल मिलता है?
   - A) एडमिन कंसोल
   - B) रजिस्ट्री कुंजी
   - C) राउटर फ़र्मवेयर
   - D) सिस्टम लॉग

5. कौन-सा ऑथेंटिकेशन मानक Okta या Microsoft Entra ID के ज़रिए लॉग इन करने देता है?
   - A) Single Sign-On
   - B) साझा गुप्त कुंजी
   - C) EPP ऑथेंटिकेशन
   - D) WEP कुंजी

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. Zero Trust Network Access निरंतर डिवाइस भरोसे की पुष्टि के बाद ही नेटवर्क में प्रवेश देता है।

○ सही ○ गलत

7 प्रश्न 7

7. डेडिकेटेड IP गेटवे कर्मचारियों का ट्रैफ़िक अनजान सार्वजनिक उपभोक्ता उपयोगकर्ताओं के साथ-साथ रूट करते हैं।

○ सही ○ गलत

8 प्रश्न 8

8. केंद्रीकृत एडमिन कंसोल IT मैनेजरों को किसी भी कर्मचारी की सीट तुरंत रद्द करने देते हैं।

○ सही ○ गलत

9 प्रश्न 9

9. IPsec एक हल्का प्रोटोकॉल है जो साइट-टू-साइट नेटवर्क टनल को सपोर्ट नहीं करता।

○ सही ○ गलत

10 प्रश्न 10

10. सिंगल साइन-ऑन कॉर्पोरेट आइडेंटिटी प्रदाताओं से कर्मचारियों का सुरक्षित प्रमाणीकरण संभव बनाता है।

○ सही ○ गलत

चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. आधुनिक सुरक्षा आर्किटेक्चर में कर्मचारियों का _____ पुराने टनल की जगह पहचान-आधारित नियमों से तय होता है।

2. डेटाबेस तक पहुंच सीमित करने के लिए कंपनियां सख्त _____ नीतियां लागू करती हैं।

3. शाखा कार्यालयों के बीच भेजा जाने वाला डेटा सुरक्षित रखने के लिए _____ ज़रूरी है।

4. आईटी प्रशासक कर्मचारियों के उपयोगकर्ता लाइसेंस केंद्रीय _____ में आवंटित करते हैं।

5. Okta इंटीग्रेशन से कर्मचारी कॉर्पोरेट _____ के ज़रिए प्रमाणित हो सकते हैं।

6. लॉगिन सुरक्षित रखने के लिए एंटरप्राइज़ पोर्टल बहु-स्तरीय _____ अनिवार्य करते हैं।

शब्दावली शब्द-बैंक

अनुपालन | एक्सेस नियंत्रण | एडमिन कंसोल | एन्क्रिप्शन | प्रमाणीकरण | रिमोट एक्सेस | सिंगल साइन-ऑन | IPSEC

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: प्रमुख अवधारणा मिलान

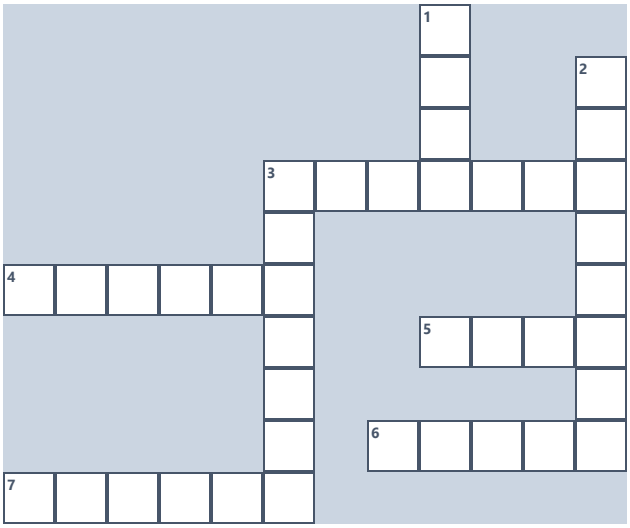
परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

☐	**1. ज़ीरो ट्रस्ट**	**A**	कर्मचारियों के VPN एक्सेस लाइसेंस आवंटित करना।
☐	**2. डेडिकेटेड IP**	**B**	Okta और Entra ID की पहचान लिंक।
☐	**3. IPSEC**	**C**	अतिरिक्त टोकन माँगने वाली लॉगिन सुरक्षा।
☐	**4. एडमिन कंसोल**	**D**	स्टैटिक व्हाइटलिस्ट गेटवे पता।
☐	**5. सिंगल साइन-ऑन**	**E**	साइट-टू-साइट टनल का मानक।
☐	**6. मल्टी-फ़ैक्टर**	**F**	नेटवर्क में प्रवेश का रूटिंग नोड।
☐	**7. गेटवे**	**G**	केंद्रीय IT मैनेजर सीट पोर्टल।
☐	**8. प्रावधान**	**H**	निरंतर विश्वास सत्यापन फ़्रेमवर्क।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।



बाएँ से दाएँ

3. आईटी प्रबंधक का केंद्रीय सीट-पोर्टल (7)

4. दूर बैठे कर्मचारी का कंपनी नेटवर्क और संसाधनों तक सुरक्षित रूप से पहुंचना (6)

5. फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना। (4)

6. निजी उपयोगकर्ता जानकारी के प्रबंधन के लिए GDPR या CCPA जैसे नियामक मानक पूरे करना (5)

7. यह जांचने की प्रक्रिया कि लॉगिन करने वाला उपयोगकर्ता वास्तव में वही है जो वह होने का दावा करता है (6)

ऊपर से नीचे

1. कर्मचारियों के VPN एक्सेस लाइसेंस सौंपना (4)

2. Okta और Entra ID से पहचान का जुड़ाव (8)

3. यह तय करने की व्यवस्था कि कौन सा उपयोगकर्ता किस संसाधन तक पहुंच सकता है (7)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं।

बाएँ से दाएँ

3 बाएँ से दाएँ: आईटी प्रबंधक का केंद्रीय सीट-पोर्टल (7 अक्षर):

4 बाएँ से दाएँ: दूर बैठे कर्मचारी का कंपनी नेटवर्क और संसाधनों तक सुरक्षित रूप से पहुंचना (6 अक्षर):

5 बाएँ से दाएँ: फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना। (4 अक्षर):

6 बाएँ से दाएँ: निजी उपयोगकर्ता जानकारी के प्रबंधन के लिए GDPR या CCPA जैसे नियामक मानक पूरे करना (5 अक्षर):

7 बाएँ से दाएँ: यह जांचने की प्रक्रिया कि लॉगिन करने वाला उपयोगकर्ता वास्तव में वही है जो वह होने का दावा करता है (6 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: कर्मचारियों के VPN एक्सेस लाइसेंस सौंपना (4 अक्षर):

2 ऊपर से नीचे: Okta और Entra ID से पहचान का जुड़ाव (8 अक्षर):

3 ऊपर से नीचे: यह तय करने की व्यवस्था कि कौन सा उपयोगकर्ता किस संसाधन तक पहुंच सकता है (7 अक्षर):

चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

ड	रे	स	ख	नि	फ	ढ	मा	ना	का	रे	दे	सि	मी	क
पि	ता	न	ति	ज	श	भ	ऊ	रि	अ	ऊ	ए	रि	वि	श
य	वि	ल	व	वा	पा	ल	च	से	मो	कि	य	घ	प	के
की	व	पा	ण	र	क	णी	मा	प्र	सि	ट	री	त	की	कि
सि	ना	नु	ने	पा	सिं	ते	ण	ए	ता	सा	ए	मी	न	नी
ण	ऋ	अ	ले	घ	ग	ति	ए	जि	ला	ए	जी	क्से	ले	ड
त्र	ल	द	जे	घ	ल	के	च	ड	से	न	दे	री	स	ए
यं	पी	उ	अ	जे	सा	मि	घ	व	मि	आ	प्श	च	मी	च
नि	ट	थ	फ	ग	इ	ना	सी	का	ज	न	फ	न्क्रि	नी	जी
स	ता	ठ	से	लि	न	ट	आ	इ	से	रा	कं	के	ए	री
क्से	पा	वा	सि	य	ऑ	नि	पि	ने	ख	न	के	सो	वे	ऊ
ए	ड	नी	दे	दि	न	भ	आ	नि	ट	जे	वे	वे	ल	ष
ण	प	कि	से	य	ह	ह	ते	वं	रा	द	सा	सी	थ	जे
इ	मे	ला	ढ	पे	ऋ	वे	आ	नी	वे	उ	थ	ह	जे	त
य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा	दा	पी	व

शब्दावली शब्द-सूची

एडमिनकंसोल सिंगलसाइनऑन आवंटन अनुपालन एन्क्रिप्शन एक्सेसनियंत्रण रिमोटएक्सेस प्रमाणीकरण

चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

शब्दावली के शब्द

- **A. एडमिनकंसोल**
- **B. सिंगलसाइनऑन**
- **C. आवंटन**
- **D. अनुपालन**
- **E. एन्क्रिप्शन**
- **F. एक्सेसनियंत्रण**
- **G. रिमोटएक्सेस**
- **H. प्रमाणीकरण**

परिभाषाएँ और मिलान फ़ील्ड

1. Okta और Entra ID से पहचान का जुड़ाव। ____
2. दूर बैठे कर्मचारी का कंपनी नेटवर्क और संसाधनों तक सुरक्षित रूप से पहुंचना। ____
3. यह जांचने की प्रक्रिया कि लॉगिन करने वाला उपयोगकर्ता वास्तव में वही है जो वह होने का दावा करता है। ____
4. यह तय करने की व्यवस्था कि कौन सा उपयोगकर्ता किस संसाधन तक पहुंच सकता है। ____
5. कर्मचारियों के VPN एक्सेस लाइसेंस सौंपना। ____
6. आईटी प्रबंधक का केंद्रीय सीट-पोर्टल। ____
7. फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना। ____
8. निजी उपयोगकर्ता जानकारी के प्रबंधन के लिए GDPR या CCPA जैसे नियामक मानक पूरे करना। ____

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर इस वर्कशीट की प्रमुख अवधारणाएँ पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. **न सो ए कं ल मि ड** _____

2. **आ ट न वं** _____

3. **न ए प्श क्रि** _____

4. **स ए ट क्से रि मो** _____

5. **इ न ग न सा सिं ऑ ल** _____

6. **ल अ पा न नु** _____

7. **ए त्र यं ण क्से नि स** _____

8. **णी ण प्र र क मा** _____

अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

1	ऐसे टूल जिन्हें कोई कंपनी रोज़ इस्तेमाल करती है			
2	ऐसी चीज़ें जिन्हें VPN छिपा सकता है			
3	IT विभाग की भूमिकाएँ			
4	Zero Trust का वर्णन करने वाले शब्द			
5	सुरक्षित रूप से लॉग इन करने के तरीके			
6	कर्मचारियों को VPN देने के कारण			
7	सुरक्षा उल्लंघन के बाद की जाने वाली चीज़ें			
8	यात्रा के दौरान VPN इस्तेमाल करने के कारण			
9	सुरक्षित रिमोट वर्क के नियम			
10	ऐसा डेटा जिसे कंपनी को सुरक्षित रखना होता है			
11	वीडियो मीटिंग में बाधा डालने वाली चीज़ें			
12	ऐसे डिवाइस जो VPN इस्तेमाल कर सकते हैं			
13	आपके जाने-पहचाने ऑफ़िस प्रोग्राम			
14	ऐसी जगहें जहाँ से कर्मचारी काम करते हैं			
15	ऐसे डिवाइस जो किसी कर्मचारी के पास हो सकते हैं			

चेकपॉइंट 8: VPN और नेटवर्क केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

केस स्टडी 1: ज़ीरो ट्रस्ट माइग्रेशन

👷

परिदृश्य: एक उद्यम नेटवर्क के अंदर किसी पर भी भरोसा करने के बजाय डिवाइस अनुपालन सर्टिफ़िकेट, फ़ायरवॉल स्थिति और उपयोगकर्ता की लोकेशन को लगातार सत्यापित करके अपने स्थानीय सर्वर सुरक्षित करना चाहता है।

चर्चा प्रश्न: इसे हासिल करने के लिए IT सुरक्षा निदेशक को कौन-सा फ़्रेमवर्क लागू करना चाहिए?

केस स्टडी 2: गेटवे प्रतिबंध

👷

परिदृश्य: एक कंपनी क्लाउड में निजी वित्तीय डेटाबेस होस्ट करती है। वह एडमिन पैनल तक सारी सार्वजनिक इंटरनेट पहुँच ब्लॉक करना चाहती है और लॉगिन केवल सत्यापित कंपनी एंडपॉइंट से ही अनुमत करना चाहती है।

चर्चा प्रश्न: डेटाबेस एडमिनिस्ट्रेटर को क्लाउड फ़ायरवॉल पर कौन-सी नेटवर्क कॉन्फ़िगरेशन सेट करनी चाहिए?

चेकपॉइंट 9: कूट संदेश को डिकोड करें

नेटवर्क इंजीनियर रूटिंग चैनलों और क्लाइंट टनल को सुरक्षित करता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके संदेश को डिक्रिप्ट करें और खाली स्थानों में मेल खाते अक्षर लिखें।

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12

क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24

ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36

म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48

ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60

्=61

20	60	48	39	54		23	61	39	44	61	23		45	39

25	47	41	46	3	44		33	39	14	28	46

डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग A)

वर्चुअल प्राइवेट नेटवर्क (VPN) और टनलिंग से जुड़े सबसे आम सवाल और जवाब देखें।

Q1: एंटरप्राइज़ VPN क्या है?

व्यवसायों के लिए बनाई गई सुरक्षित नेटवर्क टनल, जो दूरस्थ कर्मचारियों को केंद्रीकृत प्रबंधन के साथ कॉर्पोरेट नेटवर्क तक पहुँचने देती है।

Q2: Zero Trust पारंपरिक VPN से कैसे अलग है?

पारंपरिक VPN टनल के अंदर हर किसी पर भरोसा करते हैं, जबकि Zero Trust हर डिवाइस और उपयोगकर्ता कनेक्शन को लगातार सत्यापित करता है।

Q3: बिज़नेस VPN में Dedicated IP क्या है?

केवल आपके व्यवसाय के लिए आरक्षित स्थिर IP पता, जिसे आप सुरक्षित क्लाउड डेटाबेस एक्सेस के लिए व्हाइटलिस्ट कर सकते हैं।

Q4: बिज़नेस VPN के लिए SSO क्यों महत्वपूर्ण है?

सिंगल साइन-ऑन कर्मचारियों को सुरक्षित लॉगिन के लिए अपने कॉर्पोरेट क्रेडेंशियल (जैसे Okta या Microsoft Entra ID) का उपयोग करने देता है।

Q5: साइट-टू-साइट VPN क्या है?

टनल जो IPsec का उपयोग करके सार्वजनिक इंटरनेट पर दो भौतिक कार्यालयों (जैसे शाखा कार्यालय और मुख्यालय) को जोड़ती है।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

वर्चुअल प्राइवेट नेटवर्क (VPN) और टनलिंग से जुड़े सबसे आम सवाल और जवाब देखें।

Q6: एडमिन कंसोल का कार्य क्या है?

IT प्रशासकों के लिए डैशबोर्ड, जिससे वे कर्मचारी सीटें जोड़ या हटा सकते हैं, गेटवे असाइन कर सकते हैं और सक्रिय कनेक्शन की निगरानी कर सकते हैं।

Q7: MFA बिज़नेस VPN को कैसे सुरक्षित करता है?

दूसरा कोड (जैसे ऑथेंटिकेटर ऐप टोकन) माँगकर, ताकि समझौता हुए पासवर्ड से अनधिकृत प्रवेश रोका जा सके।

Q8: क्या मैं कर्मचारियों का कनेक्शन इतिहास ऑडिट कर सकता हूँ?

हाँ, एंटरप्राइज़ VPN अनुपालन ऑडिट के लिए कनेक्शन के टाइमस्टैम्प, अवधि और असाइन किए गए IP लॉग करते हैं।

Q9: ZTNA क्या है?

Zero Trust Network Access, एक सुरक्षा मॉडल जो पूरे नेटवर्क के बजाय केवल विशिष्ट ऐप्लिकेशन तक पहुँच देता है।

Q10: गेटवे नोड की भूमिका क्या है?

वे दूरस्थ ट्रैफ़िक के लिए सुरक्षित प्रवेश बिंदु का काम करते हैं और डेटा को सीधे निजी कॉर्पोरेट सर्वरों तक भेजते हैं।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

VPN टनलिंग प्रोटोकॉल, मोबाइल क्लाइंट एकीकरण और एंटरप्राइज़ तैनाती के उन्नत तकनीकी पहलुओं को जानें।

Q1: IPsec साइट-टू-साइट कॉर्पोरेट संचार की रक्षा कैसे करता है?

IPsec, डेटा की गोपनीयता और अखंडता सुनिश्चित करने के लिए Encapsulating Security Payload (ESP) का उपयोग करके नेटवर्क लेयर पर ट्रैफ़िक को एन्क्रिप्ट करता है।

Q2: रिमोट कर्मचारियों के लिए पुरानी परिधि-आधारित सुरक्षा क्यों विफल हो रही है?

क्योंकि कर्मचारी कई स्थानों और डिवाइसों से डेटा एक्सेस करते हैं, जिससे एकल नेटवर्क फ़ायरवॉल परिधि अप्रचलित हो जाती है।

Q3: IT प्रबंधक स्वचालित प्रोविज़निंग कैसे लागू करते हैं?

उपयोगकर्ता डायरेक्टरी सिंक्रनाइज़ करने के लिए पहचान प्रदाताओं (Okta) और VPN एडमिन कंसोल के बीच SCIM प्रोटोकॉल मैप करके।

Q4: कॉर्पोरेट वातावरण में स्प्लिट टनलिंग का क्या लाभ है?

यह स्थानीय SaaS ट्रैफ़िक (जैसे Microsoft 365) को VPN टनल के बाहर रूट करता है, जिससे कॉर्पोरेट गेटवे की बैंडविड्थ निजी डेटाबेस के लिए बची रहती है।

Q5: डिवाइस पोस्चर चेक एंडपॉइंट सुरक्षा को कैसे मान्य करते हैं?

VPN क्लाइंट कनेक्ट करने से पहले डिवाइस को स्कैन करता है, ताकि पुष्टि हो कि फ़ायरवॉल सक्रिय है, एंटीवायरस चल रहा है और OS पैच अद्यतन हैं।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

VPN टनलिंग प्रोटोकॉल, मोबाइल क्लाइंट एकीकरण और एंटरप्राइज़ तैनाती के उन्नत तकनीकी पहलुओं को जानें।

Q6: बिज़नेस VPN सेटअप में NAT ट्रैवर्सल की क्या भूमिका है?

NAT-T, IPsec पैकेट को UDP में एनकैप्सुलेट करता है, ताकि वे कनेक्शन टूटे बिना होम राउटर और फ़ायरवॉल से गुज़र सकें।

Q7: व्यवसाय गेटवे बैंडविड्थ की रुकावट को कैसे रोकते हैं?

कई क्षेत्रीय गेटवे नोड तैनात करके और लोड बैलेंसर से आने वाले उपयोगकर्ता ट्रैफ़िक को उनके बीच बाँटकर।

Q8: डायनामिक की तुलना में स्टैटिक IP व्हाइटलिस्ट को प्राथमिकता क्यों दी जाती है?

स्टैटिक व्हाइटलिस्ट अनधिकृत बाहरी IP को कनेक्शन हैंडशेक की कोशिश करने से रोकती हैं, जिससे हमले की सतह काफ़ी घटती है।

Q9: एंटरप्राइज़ VPN में सर्टिफ़िकेट-आधारित प्रमाणीकरण की क्या भूमिका है?

यह कंपनी द्वारा प्रबंधित डिवाइस पर इंस्टॉल अनूठे डिजिटल सर्टिफ़िकेट को सत्यापित करता है और अप्रबंधित निजी कंप्यूटर को ब्लॉक करता है।

Q10: ZTNA लेटरल मूवमेंट के जोखिम को कैसे घटाता है?

उपयोगकर्ता सत्रों को केवल अधिकृत संसाधनों तक सीमित करके, ताकि कोई एक नोड भंग होने पर हैकर नेटवर्क में आगे न बढ़ सकें।

भाग 11: 10 वास्तविक VPN तथ्य और अंतर्दृष्टियाँ

VPN एन्क्रिप्शन की गति, प्रोटोकॉल ऑडिट, मोबाइल कनेक्टिविटी और एंटरप्राइज़ रिमोट वर्क से जुड़े वास्तविक तथ्य देखें।

1. VPN इनसाइट

ज़ीरो ट्रस्ट आर्किटेक्चर नेटवर्क कनेक्शन का प्रयास करने वाले हर डिवाइस की सुरक्षा स्थिति को लगातार सत्यापित करते हैं।

2. VPN इनसाइट

डेडिकेटेड IP गेटवे स्थिर पतों को व्हाइटलिस्ट करके व्यवसायों को क्लाउड डेटाबेस सुरक्षित करने देते हैं।

3. VPN इनसाइट

IPsec सुरक्षित साइट-टू-साइट कार्यालय नेटवर्क टनल कॉन्फ़िगर करने के लिए उद्योग का मानक प्रोटोकॉल है।

4. VPN इनसाइट

एडमिन कंसोल IT विभागों को कर्मचारियों की VPN पहुँच सीटें उपलब्ध कराने, प्रबंधित करने और उनका ऑडिट करने देते हैं।

5. VPN इनसाइट

सिंगल साइन-ऑन VPN एक्सेस को Okta और Entra ID जैसे कॉर्पोरेट आइडेंटिटी प्रदाताओं से जोड़ता है।

6. VPN इनसाइट

मल्टी-फ़ैक्टर ऑथेंटिकेशन चुराई गई पासवर्ड कुंजियों से आने वाले अनधिकृत कनेक्शन प्रयासों को रोकता है।

7. VPN इनसाइट

स्प्लिट टनलिंग सार्वजनिक SaaS ट्रैफ़िक को एन्क्रिप्टेड टनल से बाहर रखकर कॉर्पोरेट बैंडविड्थ अनुकूलित करती है।

8. VPN इनसाइट

डिवाइस पोस्चर जाँच कॉर्पोरेट सर्वरों तक पहुँच देने से पहले स्थानीय सुरक्षा सेटिंग सत्यापित करती है।

9. VPN इनसाइट

SCIM डायरेक्टरी सिंक्रोनाइज़ेशन कर्मचारियों के ऑनबोर्डिंग और ऑफ़बोर्डिंग के एक्सेस नियंत्रण को स्वचालित करता है।

10. VPN इनसाइट

Zero Trust Network Access उपयोगकर्ता की पहुँच को विशिष्ट अधिकृत ऐप्लिकेशन तक सीमित करता है, जिससे नेटवर्क में पार्श्व गति रुकती है।

तकनीकी संदर्भ और स्रोत

यह अध्ययन गाइड और इंटरैक्टिव पहेलियाँ वैश्विक तकनीकी मानकों, विनिर्देशों और नियामक ढाँचों से तैयार की गई हैं।

शैक्षणिक और उद्योग संदर्भ

[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/

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 **ज़ीरो ट्रस्ट** ZTNA मॉडल **सही उत्तर: A**

शिक्षण नोट

ज़ीरो ट्रस्ट मॉडल नेटवर्क में प्रवेश से पहले डिवाइस अनुपालन को लगातार सत्यापित करते हैं। उद्धरण: NIST Zero Trust।

2 **डेडिकेटेड IP** स्टैटिक IP **सही उत्तर: A**

शिक्षण नोट

डेडिकेटेड IP पते गेटवे को व्हाइटलिस्ट करने की सुविधा देते हैं, जिससे सार्वजनिक ट्रैफ़िक ब्लॉक किया जा सकता है। उद्धरण: Dedicated IP Guide।

3 **IPsec मानक** IPSEC टनल **सही उत्तर: A**

शिक्षण नोट

IPsec शाखा साइट-टू-साइट टनल के लिए उपयोग किया जाने वाला मानक प्रोटोकॉल है। उद्धरण: IPsec Tunneling।

4 **IT आवंटन** एडमिन कंसोल **सही उत्तर: A**

शिक्षण नोट

केंद्रीकृत एडमिन डैशबोर्ड IT मैनेजरों को सीट लाइसेंस आवंटित करने देते हैं। उद्धरण: CISA Guidelines।

5 **प्रश्न 5** **सही उत्तर: A**

शिक्षण नोट

कौन-सा ऑथेंटिकेशन मानक Okta या Microsoft Entra ID के ज़रिए लॉग इन करने देता है? → Single Sign-On

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **ज़ीरो ट्रस्ट** ZTNA जाँच — **सही उत्तर: सही**

शिक्षण नोट

ज़ीरो ट्रस्ट मॉडल नेटवर्क में प्रवेश से पहले डिवाइस अनुपालन को लगातार सत्यापित करते हैं। उद्धरण: NIST Zero Trust।

7 **प्रश्न 7** — **सही उत्तर: गलत**

शिक्षण नोट

Dedicated IP एक व्यवसाय के लिए आरक्षित होते हैं, इसलिए उसका ट्रैफ़िक अन्य उपयोगकर्ताओं के ट्रैफ़िक में नहीं मिलता।

8 **IT आवंटन** IT एडमिन सीट — **सही उत्तर: सही**

शिक्षण नोट

केंद्रीकृत एडमिन डैशबोर्ड IT मैनेजरों को सीट लाइसेंस आवंटित करने देते हैं। उद्धरण: CISA Guidelines।

9 **IPsec मानक** साइट-टू-साइट — **सही उत्तर: गलत**

शिक्षण नोट

IPsec शाखा साइट-टू-साइट टनल के लिए उपयोग किया जाने वाला मानक प्रोटोकॉल है। उद्धरण: IPsec Tunneling।

10 **Okta SSO लिंक** SSO लॉगिन — **सही उत्तर: सही**

शिक्षण नोट

सिंगल साइन-ऑन VPN लॉगिन को Okta जैसी कॉर्पोरेट डायरेक्टरी से जोड़ता है। उद्धरण: Okta SSO।

शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।

चेकपॉइंट 4: उत्तर – अवधारणा मिलान

H 1. ज़ीरो ट्रस्ट	D 2. डेडिकेटेड IP	E 3. IPSEC	G 4. एडमिन कंसोल
B 5. सिंगल साइन-ऑन	C 6. मल्टी-फ़ैक्टर	F 7. गेटवे	A 8. प्रावधान

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 रिमोट एक्सेस	2 एक्सेस नियंत्रण	3 एन्क्रिप्शन	4 एडमिन कंसोल
5 सिंगल साइन-ऑन	6 प्रमाणीकरण		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 B – सिंगलसाइनऑन	2 G – रिमोटएक्सेस	3 H – प्रमाणीकरण	4 F – एक्सेसनियंत्रण
5 C – आवंटन	6 A – एडमिनकंसोल	7 E – एन्क्रिप्शन	8 D – अनुपालन

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी ज़ीरो ट्रस्ट, डेडिकेटेड IP और IPSEC को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

केस स्टडी:
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

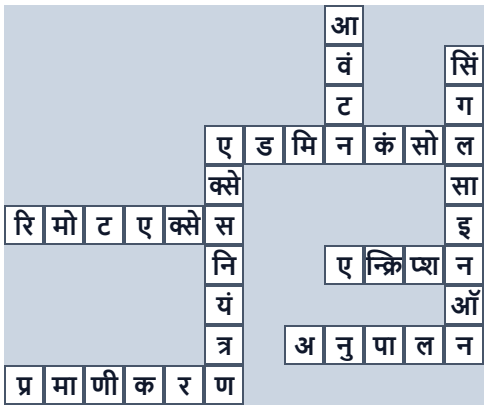
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

ड	रे	स	ख	नि	फ	ढ	मा	ना	का	रे	दे	सि	मी	क
पि	ता	न	ति	ज	श	भ	ऊ	रि	अ	ऊ	ए	रि	वि	श
य	वि	ल	व	वा	पा	ल	च	से	मो	कि	य	घ	प	के
की	व	पा	ण	र	क	णी	मा	प्र	सि	ट	री	त	की	कि
सि	ना	नु	ने	पा	सिं	ते	ण	ए	ता	सा	ए	मी	न	नी
ण	ऋ	अ	ले	घ	ग	ति	ए	जि	ला	ए	जी	क्से	ले	ड
त्र	ल	द	जे	घ	ल	के	च	ड	से	न	दे	री	स	ए
यं	पी	उ	अ	जे	सा	मि	घ	व	मि	आ	प्श	च	मी	च
नि	ट	थ	फ	ग	इ	ना	सी	का	ज	न	फ	क्रि	नी	जी
स	ता	ठ	से	लि	न	ट	आ	इ	से	रा	कं	के	ए	री
क्से	पा	वा	सि	य	ऑ	नि	पि	ने	ख	न	के	सो	वे	ऊ
ए	ड	नी	दे	दि	न	भ	आ	नि	ट	जे	वे	वे	ल	ष
ण	प	कि	से	य	ह	ह	ते	वं	रा	द	सा	सी	थ	जे
इ	मे	ला	ढ	पे	ऋ	वे	आ	नी	वे	उ	थ	ह	जे	त
य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा	दा	पी	व

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

3 बाएँ से दाएँ: एडमिनकंसोल आईटी प्रबंधक का केंद्रीय सीट-पोर्टल (7 अक्षर)

4 बाएँ से दाएँ: रिमोटएक्सेस दूर बैठे कर्मचारी का कंपनी नेटवर्क और संसाधनों तक सुरक्षित रूप से पहुंचना (6 अक्षर)

5 बाएँ से दाएँ: एन्क्रिप्शन फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना। (4 अक्षर)

6 बाएँ से दाएँ: अनुपालन निजी उपयोगकर्ता जानकारी के प्रबंधन के लिए GDPR या CCPA जैसे नियामक मानक पूरे करना (5 अक्षर)

7 बाएँ से दाएँ: प्रमाणीकरण यह जांचने की प्रक्रिया कि लॉगिन करने वाला उपयोगकर्ता वास्तव में वही है जो वह होने का दावा करता है (6 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: आवंटन कर्मचारियों के VPN एक्सेस लाइसेंस सौंपना (4 अक्षर)

2 ऊपर से नीचे: सिंगलसाइनऑन Okta और Entra ID से पहचान का जुड़ाव (8 अक्षर)

3 ऊपर से नीचे: एक्सेसनियंत्रण यह तय करने की व्यवस्था कि कौन सा उपयोगकर्ता किस संसाधन तक पहुंच सकता है (7 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

शब्द अनस्क्रैम्बल कुंजी

1. न सो ए कं ल मि ड — **एडमिनकंसोल**
2. आ ट न वं — **आवंटन**
3. न ए प्श क्रि — **एन्क्रिप्शन**
4. स ए ट क्से रि मो — **रिमोटएक्सेस**
5. इ न ग न सा सिं ऑ ल — **सिंगलसाइनऑन**
6. ल अ पा न नु — **अनुपालन**
7. ए त्र यं ण क्से नि स — **एक्सेसनियंत्रण**
8. णी ण प्र र क मा — **प्रमाणीकरण**

गुप्त कूट चुनौती कुंजी

"ज़ीरो ट्रस्ट हर डिवाइस परखता"

केस स्टडी के उत्तर

A केस स्टडी 1: ज़ीरो ट्रस्ट माइग्रेशन

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक एंटरप्राइज़ अपने स्थानीय सर्वर को सुरक्षित करना चाहता है। वह नेटवर्क के भीतर के किसी भी व्यक्ति पर भरोसा करने के बजाय डिवाइस अनुपालन प्रमाणपत्र, फ़ायरवॉल की स्थिति और उपयोगकर्ता के स्थान को लगातार सत्यापित करना चाहता है।
- अनुशंसित रणनीति और समाधान: डायरेक्टर को Zero Trust Network Access (ZTNA) मॉडल अपनाना चाहिए, जो संदर्भ पर आधारित सुरक्षा जाँचें लगातार लागू करता है।

B केस स्टडी 2: गेटवे प्रतिबंध

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक कंपनी क्लाउड में निजी वित्तीय डेटाबेस होस्ट करती है। वह एडमिन पैनल तक सार्वजनिक इंटरनेट की सारी पहुँच रोकना चाहती है और लॉगिन केवल सत्यापित कंपनी एंडपॉइंट से अनुमत करना चाहती है।
- अनुशंसित रणनीति और समाधान: एडमिनिस्ट्रेटर को एंटरप्राइज़ VPN पर Dedicated IP गेटवे कॉन्फ़िगर करना चाहिए और इस स्थिर पते को क्लाउड डेटाबेस फ़ायरवॉल पर व्हाइटलिस्ट करना चाहिए।