ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

VPN ที่ดีที่สุดสำหรับธุรกิจ

การรีวิวเชิงปฏิบัติด้านความปลอดภัย ความสามารถในการขยายขนาด และการบริหารจัดการส่วนกลางของ VPN สำหรับธุรกิจ

ภาพรวมการเรียนรู้ VPN ที่ดีที่สุดสำหรับธุรกิจ

ผู้เรียน

สถานะนักเรียน

สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย

สถานะการเชื่อมต่อ

การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน

การป้องกันการรั่วไหล

การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับBusiness VPN และเครือข่ายเข้าถึงระยะไกล คุณจะได้สำรวจสถาปัตยกรรม Zero Trust อุโมงค์ IPsec แบบไซต์ต่อไซต์ เฟรมเวิร์ก SASE การเข้าสู่ระบบแบบหลายปัจจัย และการตรวจสอบความปลอดภัยของอุปกรณ์ปลายทาง

จุดตรวจสอบของใบงาน

- [ ] **ส่วนที่ 1-4: เรียนรู้การกำหนดค่า VPN และความปลอดภัยเครือข่ายให้เชี่ยวชาญ**
- [ ] **ส่วนที่ 5-7: แก้ปริศนาอักษรไขว้และค้นหาคำ**
- [ ] **ส่วนที่ 8-9: แก้กรณีศึกษาและภารกิจถอดรหัส**
- [ ] **ส่วนที่ 10: ทบทวนหน้า FAQ ระดับพื้นฐานและระดับสูง**
- [ ] **ส่วนที่ 11: สำรวจข้อเท็จจริงน่าสนใจในโลกจริง 10 ข้อ**
- [ ] **เสริม: ความท้าทายคิดเร็ว**

เปิดคู่มือ VPN ที่ดีที่สุดของ VPN.com

URL: https://www.vpn.com/th/vpn/vpn-di-thi-sut-samrap-thurakit/

เส้นทางการเรียนรู้ VPN สำหรับธุรกิจของคุณ

- ระบุผู้ให้บริการ VPN ธุรกิจอันดับต้นๆ และฟีเจอร์เฉพาะสำหรับทีม
- วิเคราะห์ความแตกต่างระหว่างความเป็นส่วนตัวของ VPN สำหรับผู้บริโภคกับการควบคุมการดูแลระบบสำหรับธุรกิจ
- จำแนกความแตกต่างระหว่าง VPN สำหรับการเข้าถึงระยะไกลกับอุโมงค์ Site-to-Site ขององค์กร

คำแนะนำคู่มือ VPN สำหรับธุรกิจ

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การตั้งค่าการเข้าถึงระยะไกลระดับองค์กร ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การเข้าถึงระยะไกลระดับองค์กรและขอบเครือข่ายที่ปลอดภัย (บทนำ)

การรักษาความปลอดภัยการเข้าถึงระยะไกลขององค์กรต้องเปลี่ยนจากโมเดล VPN แบบอิงขอบเขตเครือข่ายแบบเดิมไปสู่สถาปัตยกรรม Zero Trust การบังคับใช้การยืนยันตัวตนหลายปัจจัย (MFA) ที่แข็งแกร่งและกรอบงาน Secure Access Service Edge (SASE) ช่วยปกป้องทรัพย์สินสำคัญจากอุปกรณ์ปลายทางที่ถูกบุกรุก

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. 1. VPN ธุรกิจประเภทใดที่เชื่อมเครือข่ายสำนักงานทั้งหมดเข้าด้วยกัน?
   - A. Site-to-Site VPN
   - B. VPN สำหรับการเข้าถึงระยะไกล
   - C. VPN สำหรับผู้บริโภค
   - D. Smart DNS

2. 2. ตัวเลือกใดที่ได้รับการเน้นว่าดีที่สุดโดยรวมสำหรับทีมธุรกิจ?
   - A. NordLayer
   - B. Surfshark
   - C. Proton VPN
   - D. Private Internet Access

3. 3. ที่อยู่ IP แบบคงที่เฉพาะช่วยป้องกันอะไรให้ทีมธุรกิจ?
   - A. การขึ้นบัญชีดำที่อยู่ IP
   - B. ความเร็วของเราเตอร์ลดลง
   - C. การบีบอัดข้อมูล
   - D. การอัปเดตไคลเอนต์

4. 4. ผู้ให้บริการรายใดที่ได้รับการเน้นว่าดีที่สุดสำหรับโครงสร้างพื้นฐานเฉพาะ?
   - A. Proton VPN
   - B. NordLayer
   - C. Surfshark
   - D. Private Internet Access

5. 5. ฟีเจอร์ใดที่มีแดชบอร์ดผู้ดูแลระบบแบบรวมศูนย์สำหรับจัดการผู้ใช้?
   - A. การควบคุมของผู้ดูแลระบบ
   - B. การส่งต่อพอร์ต
   - C. การจำลองเราเตอร์
   - D. Split tunneling

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. VPN สำหรับเข้าถึงระยะไกลช่วยให้พนักงานแต่ละคนเชื่อมต่อได้จากทุกที่

จริง เท็จ

7 คำถาม 7

7. VPN สำหรับผู้บริโภคปกป้องทั้งองค์กรภายใต้แผงผู้ดูแลระบบเดียว

จริง เท็จ

8 คำถาม 8

8. IP เฉพาะช่วยแยกทราฟฟิกของบริษัทออกจากทราฟฟิกสาธารณะ

จริง เท็จ

9 คำถาม 9

9. Private Internet Access ถูกเน้นว่าเหมาะที่สุดสำหรับองค์กรขนาดใหญ่

จริง เท็จ

10 คำถาม 10

10. SASE รวมการกำหนดเส้นทาง WAN เข้ากับเฟรมเวิร์กความปลอดภัยที่ส่งผ่านคลาวด์

จริง เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. ผู้ให้บริการอันดับหนึ่งโดยรวมสำหรับทีมธุรกิจคือ _____
2. การเชื่อมต่อสำนักงานสาขาหลายแห่งของบริษัทเข้าด้วยกันใช้ _____
3. เพื่อป้องกันไม่ให้ที่อยู่ถูกขึ้นบัญชีดำ ทีมงานใช้ _____
4. ผู้ดูแลระบบจัดการสิทธิ์ของอุปกรณ์ผ่าน _____ ส่วนกลาง
5. การเพิ่มที่นั่งแบบไดนามิกเพื่อรองรับทีมที่เติบโตคือคุณสมบัติที่ _____
6. การผ่านมาตรฐานด้านกฎระเบียบและการตรวจสอบข้อมูลต้องอาศัย _____

คลังคำศัพท์

เกตเวย์ ขยายได้ ไซต์ทูไซต์ แดชบอร์ด นอร์ดเลเยอร์ ปฏิบัติตามกฎ เส้นทาง ไอพีคงที่

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดสำคัญ

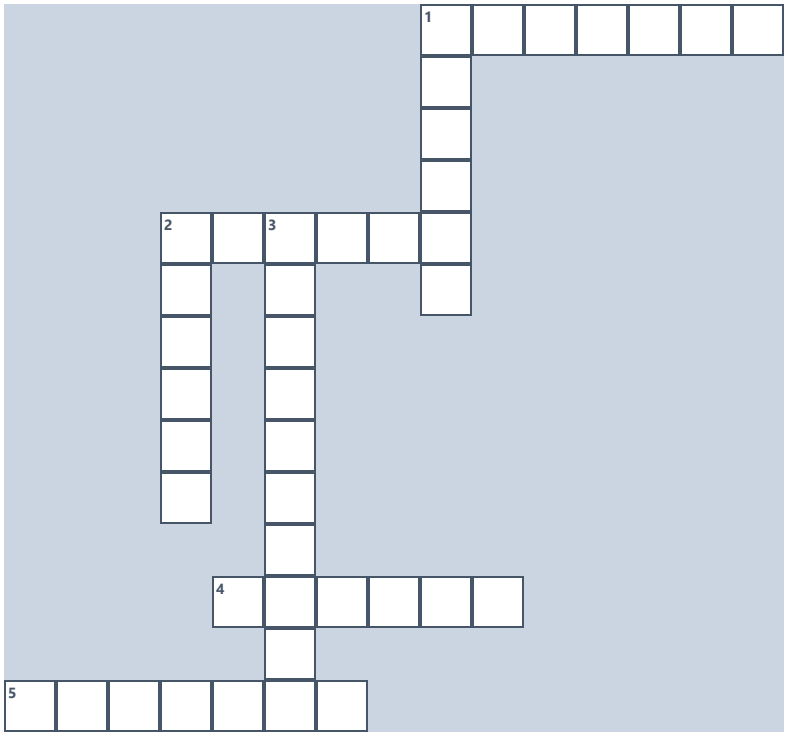
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. NORDLAYER**	**A**	การเติบโตของทีมแบบหลายที่นั่งที่ปรับเปลี่ยนได้
☐	**2. ไซต์ถึงไซต์**	**B**	ตัวเลือกธุรกิจที่ดีที่สุดโดยรวม
☐	**3. IP แบบคงที่**	**C**	การควบคุมทราฟฟิกแบบ Split tunneling
☐	**4. แดชบอร์ด**	**D**	การตรวจสอบมาตรฐานตามกฎระเบียบ
☐	**5. ความสามารถในการขยายระบบ**	**E**	โหนดจุดเข้าสำหรับการยืนยันตัวตนจากระยะไกล
☐	**6. การปฏิบัติตามข้อกำหนด**	**F**	ที่อยู่เฉพาะที่ไม่อยู่ในบัญชีดำ
☐	**7. การกำหนดเส้นทาง**	**G**	อุโมงค์เชื่อมต่อเครือข่ายสำนักงาน
☐	**8. เกตเวย์**	**H**	คอนโซลควบคุมผู้ดูแลระบบส่วนกลาง

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

1. อุโมงค์เชื่อมเครือข่ายสำนักงานเข้าด้วยกัน (7)

2. การควบคุมทราฟฟิกแบบ Split Tunneling (6)

4. การเพิ่มจำนวนที่นั่งของทีมอย่างยืดหยุ่น (6)

5. คอนโซลควบคุมของผู้ดูแลระบบส่วนกลาง (7)

แนวตั้ง

1. ที่อยู่เฉพาะที่ไม่ถูกขึ้นบัญชีดำ (6)

2. โหนดทางเข้าระยะไกลที่ใช้ยืนยันตัวตน (6)

3. ตัวเลือกที่ดีที่สุดโดยรวมสำหรับธุรกิจ (10)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

1 แนวนอน: อุโมงค์เชื่อมเครือข่ายสำนักงานเข้าด้วยกัน (7 ตัวอักษร):

2 แนวนอน: การควบคุมทราฟฟิกแบบ Split Tunneling (6 ตัวอักษร):

4 แนวนอน: การเพิ่มจำนวนที่นั่งของทีมอย่างยืดหยุ่น (6 ตัวอักษร):

5 แนวนอน: คอนโซลควบคุมของผู้ดูแลระบบส่วนกลาง (7 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ที่อยู่เฉพาะที่ไม่ถูกขึ้นบัญชีดำ (6 ตัวอักษร):

2 แนวตั้ง: โหนดทางเข้าระยะไกลที่ใช้ยืนยันตัวตน (6 ตัวอักษร):

3 แนวตั้ง: ตัวเลือกที่ดีที่สุดโดยรวมสำหรับธุรกิจ (10 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช	มี	ด้	ฟ	บ	า	า	ไ	ห	นี	า	ม	กี	จ	า
า	รี	ไ	ต	ว	ย	ง	อ	ไ	ก	ค	จ	น	ตี	ว
ร	ตี	ย	ว	า	ล	ล	พี	ด	ช	า	อ	ย	ช	ฟ
ฏ	ก	า	ก	ล	ม	า	ค	ป	อ	ต์	อ	ม	มี	า
ก	ล	ย	ล	ป	น	จ	ง	ง	า	นี	ทู	กี	พ	ร
ม	ง	ข	า	ช	อ	า	ที่	า	า	ลี	จ	ไ	ดี	า
า	น	ล	ผ	ดี	ร์	ช	ก	แ	ด	ท	า	ต	ช	า
ต	จ	า	ค	ก	ด	ดี	า	ด	ช	ว	น	ก	ด	ต์
ติ	กี	ด	ท	ผ	เ	ฟ	ช	ช	มี	ม	อ	ส้	ต	ฟ
บั	ร	ดี	า	ท	ล	เ	า	บ	ส	ท	ข	ข	เ	า
ฏิ	น	ก	า	ล	เ	ก	า	อ	ม	ร	มี	า	ร	ช
ป	ก	ด	ง	น	ย	ต	ร	ร์	ต	สี	ย	ข	มี	ดี
ด	ด	ว	บ	ฟ	อ	เ	อ	ด	า	ร	ห	ห	รี	น
ผ	นี	ม	ผ	ดี	ร์	ว	ข	กี	ส	บ	ลี	ง	ด	ร
ด	ค	ผ	ห	ดี	ป	ย์	ร	กี	นี	า	ต	จ	ห	ดี

รายการคำศัพท์

นอร์ดเลเยอร์ ไซต์ทูไซต์ ไอพีคงที่ แดชบอร์ดเกตเวย์ ขยายได้ ปฏิบัติตามกฎ เส้นทาง

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. นอร์ดเลเยอร์

B. ไซต์ทูไซต์

C. ไอพีคงที่

D. แดชบอร์ด

E. ขยายได้

F. ปฏิบัติตามกฎ

G. เส้นทาง

H. เกตเวย์

คำนิยามและช่องจับคู่

1. การควบคุมทราฟฟิกแบบ Split Tunneling
2. คอนโซลควบคุมของผู้ดูแลระบบส่วนกลาง
3. โหนดทางเข้าระยะไกลที่ใช้ยืนยันตัวตน
4. ที่อยู่เฉพาะที่ไม่ถูกขึ้นบัญชีดำ
5. มาตรฐานการตรวจสอบตามข้อกำหนดด้านกฎระเบียบ
6. อุโมงค์เชื่อมเครือข่ายสำนักงานเข้าด้วยกัน
7. ตัวเลือกที่ดีที่สุดโดยรวมสำหรับธุรกิจ
8. การเพิ่มจำนวนที่นั่งของทีมอย่างยืดหยุ่น

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดสำคัญของใบงานนี้ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. อ เ ล เ อ น ย ร์ ด ร์
2. ที่ ไ พึ ง ค อ
3. ข า ย ต้ ไ ย
4. ง ท น า เ ส้
5. ไ ต์ ทู ต์ ไ ซ ซ
6. ร์ ช อ แ บ ด ด
7. า ป ก ฎ ม ติ ฏิ ต บั
8. ต ย์ เ ว เ ก

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	คำมั่นสัญญาที่ผู้ให้บริการ **VPN** ที่ดีให้ไว้			
2	สิ่งที่อาจรบกวนการประชุมทางวิดีโอ			
3	กฎสำหรับการทำงานจากระยะไกลอย่างปลอดภัย			
4	โปรแกรมสำนักงานที่คุณรู้จัก			
5	สิ่งที่ผู้ให้บริการอินเทอร์เน็ตของคุณมองเห็นได้			
6	เหตุผลที่ควรให้พนักงานใช้ **VPN**			
7	สิ่งที่ **VPN** ปกป้องคุณไม่ได้			
8	สถานที่ที่พนักงานทำงาน			
9	เครื่องมือที่บริษัทใช้ทุกวัน			
10	วิธีเข้าสู่ระบบอย่างปลอดภัย			
11	ข้อมูลที่บริษัทต้องปกป้อง			
12	บทบาทในแผนก **IT**			
13	อุปกรณ์ที่พนักงานอาจมี			
14	สิ่งที่ต้องทำหลังเกิดการละเมิดความปลอดภัย			
15	คำที่อธิบาย **Zero Trust**			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN และเครือข่าย

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: IP สาธารณะที่ใช้ร่วมกันถูกขึ้นบัญชีดำ



สถานการณ์: ทีมขายเข้าถึงฐานข้อมูลขององค์กรโดยใช้ VPN สำหรับผู้บริโภค แต่ถูกล็อกไม่ให้เข้าได้เพราะ IP ขาออกที่ใช้ร่วมกันถูกระบบตรวจจับการฉ้อโกงขึ้นบัญชีดำ

คำถามอภิปราย: จงเสนอการตั้งค่าโครงสร้างพื้นฐาน VPN ระดับธุรกิจเพื่อแก้ไขการล็อกนี้

กรณีศึกษาที่ 2: การเชื่อมต่อสำนักงานองค์กร



สถานการณ์: บริษัทขนาดใหญ่ที่มีสำนักงานในมิวนิกและบอสตันต้องการแชร์เซิร์ฟเวอร์ไฟล์ภายในอย่างปลอดภัยโดยไม่ส่งทราฟฟิกผ่านพื้นที่เว็บสาธารณะ

คำถามอภิปราย: เลือกโทโพโลยี VPN ธุรกิจที่เหมาะสม

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

วิศวกรเครือข่ายรักษาความปลอดภัยของช่องทางกำหนดเส้นทางและอุโมงค์ของไคลเอนต์ ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความ โดยเขียนตัวอักษรที่ตรงกันลงในช่องว่าง

คีย์เข้ารหัสตัวอักษรเป็นตัวเลข

ก=1 ข=2 ฃ=3 ค=4 ฅ=5 ฆ=6 ง=7 จ=8 ฉ=9 ช=10 ซ=11 ฌ=12
ญ=13 ฎ=14 ฏ=15 ฐ=16 ฑ=17 ฒ=18 ณ=19 ด=20 ต=21 ถ=22 ท=23 ธ=24
น=25 บ=26 ป=27 ผ=28 ฝ=29 พ=30 ฟ=31 ภ=32 ม=33 ย=34 ร=35 ฤ=36
ล=37 ฦ=38 ว=39 ศ=40 ษ=41 ส=42 ห=43 ฬ=44 อ=45 ฮ=46 ะ=47 ั=48
า=49 ำ=50 ิ=51 ี=52 ึ=53 ื=54 ุ=55 ู=56 เ=57 แ=58 โ=59 ใ=60
ไ=61 ็=62 ่=63 ้=64 ๊=65 ๋=66 ์=67

11	52	59	35	23	35	48	42	21	67		27	1	27	64	45	7

57	4	35	54	45	2	63	49	34		45	7	4	67	1	35

ข้อความที่ถอดรหัสแล้ว:

คำใบ้: ตัวเลขแต่ละตัวแทนตำแหน่งของตัวอักษรนั้นในตัวอักษรไทย (เช่น 1 = ก, 2 = ข, 67 = ์)

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q1: VPN สำหรับธุรกิจคืออะไร?

การเชื่อมต่อเครือข่ายที่ปลอดภัยซึ่งช่วยให้พนักงานระยะไกลและสำนักงานเข้าถึงข้อมูลส่วนตัวขององค์กรได้อย่างปลอดภัย

Q2: VPN สำหรับผู้บริโภคกับ VPN สำหรับธุรกิจต่างกันอย่างไร?

VPN สำหรับผู้บริโภคซ่อนการท่องเว็บส่วนบุคคล ส่วน VPN สำหรับธุรกิจปกป้องระบบองค์กรด้วยคอนโซลผู้ดูแลระบบส่วนกลาง

Q3: Site-to-Site VPN คืออะไร?

อุโมงค์ที่เชื่อมเครือข่ายสำนักงานจริงทั้งหมดเข้าด้วยกันผ่านเว็บ

Q4: Remote Access VPN คืออะไร?

อุโมงค์ที่ให้พนักงานระยะไกลแต่ละคนเชื่อมต่อกับเครือข่ายของบริษัทได้อย่างปลอดภัย

Q5: IP คงที่เฉพาะ (dedicated static IP) มีประโยชน์อย่างไร?

แยกทราฟฟิกขององค์กรออกจากกลุ่มสาธารณะและหลีกเลี่ยงการขึ้นบัญชีดำ IP ที่ใช้ร่วมกัน

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q6: ผู้ให้บริการรายใดดีที่สุดสำหรับธุรกิจขนาดเล็ก?

Private Internet Access (PIA) ขึ้นชื่อเรื่องราคาที่เหมาะกับทีมขนาดเล็กและการตั้งค่าที่ง่าย

Q7: VPN สำหรับธุรกิจตัวใดได้รับการจัดอันดับที่ 1 โดยรวม?

NordLayer ได้คะแนน 92/100 จาก VPN.com ด้านฟีเจอร์และเครื่องมือผู้ดูแลระบบ

Q8: การขยายขนาดสำหรับทีม (team scalability) ใน VPN คืออะไร?

ความสามารถในการเพิ่มที่นั่งผู้ใช้ ใบอนุญาต และเกตเวย์ได้แบบไดนามิกเมื่อบริษัทเติบโต

Q9: ทำไมการจัดการแบบรวมศูนย์จึงสำคัญยิ่ง?

ช่วยให้ผู้ดูแลระบบบังคับใช้นโยบายความปลอดภัยและเพิกถอนการเข้าถึงของพนักงานได้ในแดชบอร์ดเดียว

Q10: SASE คืออะไร?

Secure Access Service Edge ซึ่งรวมการกำหนดเส้นทาง WAN เข้ากับบริการความปลอดภัยที่ส่งมอบผ่านคลาวด์

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q1: split tunneling รักษาความปลอดภัยของทีมได้อย่างไร?

เก็บทราฟฟิก SaaS ส่วนตัวไว้ภายในอุโมงค์ที่ปลอดภัย ขณะกำหนดเส้นทางการเข้าถึงเว็บสาธารณะในเครื่อง

Q2: Proton VPN มีอะไรให้ธุรกิจบ้าง?

โครงสร้างพื้นฐานเซิร์ฟเวอร์เฉพาะ ได้คะแนน 88/100 จาก VPN.com (มีฐานในสวิตเซอร์แลนด์)

Q3: มาตรฐานการปฏิบัติตามข้อกำหนดใดที่กำหนดให้ใช้ VPN?

PCI DSS กำหนดให้ใช้การเข้ารหัสที่แข็งแรงบนเครือข่ายสาธารณะ ส่วน HIPAA และ GDPR คาดหวังให้ใช้เป็นมาตรการป้องกัน

Q4: เรียกใช้ VPN สำหรับธุรกิจบนเราเตอร์ได้หรือไม่?

ได้ การตั้งค่าอุโมงค์ VPN บนเราเตอร์ช่วยปกป้องอุปกรณ์ทั้งหมดในสำนักงานโดยอัตโนมัติ

Q5: การยืนยันตัวตนแบบหลายปัจจัยคืออะไร?

การกำหนดให้ใช้ข้อมูลรับรองหลายอย่าง (เช่น สมาร์ทการ์ดหรือรหัส SMS) เพื่อยืนยันตัวตนการล็อกอิน

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q6: ทำไม IP address ที่ใช้ร่วมกันจึงถูกขึ้นบัญชีดำ?

เพราะผู้ใช้นับพันคนใช้ร่วมกัน ซึ่งบางคนอาจกระทำการที่เป็นอันตราย

Q7: เกตเวย์พิสูจน์ตัวตนผู้ใช้อย่างไร?

ด้วยการตรวจสอบใบรับรองไคลเอนต์ รหัสผ่าน และรหัสหลายปัจจัยกับ active directory

Q8: Surfshark มีอะไรให้ทีมบ้าง?

ตัวเลือกยอดเยี่ยมของ VPN.com สำหรับชุดความปลอดภัย ได้คะแนน 84/100 พร้อมเซิร์ฟเวอร์ที่ใช้ RAM เท่านั้น

Q9: คุณตรวจสอบการเชื่อมต่อ VPN ของธุรกิจอย่างไร?

ด้วยการตรวจสอบล็อกการเชื่อมต่อ ตัวชี้วัดการใช้ข้อมูล และประวัติการเข้าสู่ระบบในคอนโซลผู้ดูแลระบบ

Q10: การควบคุมการเข้าถึงแบบ Zero Trust คืออะไร?

แนวคิดที่ถือว่าทุกอุปกรณ์ไม่น่าเชื่อถือ และต้องมีการตรวจสอบสำหรับทุกเซสชัน

ส่วนที่ 11: ข้อเท็จจริง VPN ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับความเร็วการเข้ารหัส VPN การตรวจสอบโปรโตคอล การเชื่อมต่อบนมือถือ และการทำงานระยะไกลขององค์กร

1. ข้อมูลเชิงลึกเรื่อง VPN

VPN สำหรับธุรกิจเข้ารหัสทราฟฟิกและปกป้องระบบของบริษัทจากการดักข้อมูลบนเครือข่ายสาธารณะ

2. ข้อมูลเชิงลึกเรื่อง VPN

VPN แบบไซต์ต่อไซต์เชื่อมเครือข่ายสาขาทั้งหมดเข้าด้วยกันอย่างปลอดภัยโดยไม่เปิดเผยโฮสต์ภายใน

3. ข้อมูลเชิงลึกเรื่อง VPN

VPN สำหรับผู้บริโภคซ่อนการท่องเว็บส่วนบุคคล ขณะที่ VPN สำหรับธุรกิจปกป้องเกตเวย์ทรัพยากรขององค์กร

4. ข้อมูลเชิงลึกเรื่อง VPN

VPN.com ให้คะแนน NordLayer 92/100 เป็น VPN ธุรกิจโดยรวมที่ดีที่สุด

5. ข้อมูลเชิงลึกเรื่อง VPN

VPN.com ให้คะแนน Proton VPN 88/100 และจัดให้ดีที่สุดสำหรับโครงสร้างพื้นฐานเฉพาะ

6. ข้อมูลเชิงลึกเรื่อง VPN

VPN.com ให้คะแนน Private Internet Access 76/100 และจัดอันดับว่าดีที่สุดสำหรับทีมธุรกิจขนาดเล็ก

7. ข้อมูลเชิงลึกด้าน VPN

แดชบอร์ดผู้ดูแลระบบส่วนกลางช่วยให้เจ้าหน้าที่ความปลอดภัยจัดการสิทธิ์ผู้ใช้และกฎการเข้าถึงได้

8. ข้อมูลเชิงลึกด้าน VPN

IP แบบคงที่เฉพาะช่วยป้องกันไม่ให้ทีมถูกบล็อกจากระบบตรวจจับการฉ้อโกงที่ใช้ IP ร่วมกัน

9. ข้อมูลเชิงลึกด้าน VPN

GDPR ระบุให้การเข้ารหัสเป็นมาตรการที่เหมาะสมในการปกป้องข้อมูลส่วนบุคคล

10. ข้อมูลเชิงลึกเรื่อง VPN

สถาปัตยกรรมซีโร่ทรัสต์ตรวจสอบเอนด์พอยต์ระยะไกลทั้งหมดโดยไม่คำนึงถึงตำแหน่งหรือข้อมูลรับรอง

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานทางเทคนิค ข้อกำหนดเฉพาะ และกรอบการกำกับดูแลระดับโลก

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[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/

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **โทโพโลยีอุโมงค์** ไซต์ถึงไซต์ — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

VPN แบบไซต์ต่อไซต์เชื่อมต่อสำนักงานสาขาระยะไกลทั้งหมดเข้าด้วยกันอย่างปลอดภัย การอ้างอิง: NIST Zero Trust.

2 **คำถาม 2** — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

VPN.com ให้คะแนน NordLayer 92/100 และจัดอันดับให้ดีที่สุดโดยรวมสำหรับทีมธุรกิจ

3 **การอนุญาต IP (Whitelisting)** IP เฉพาะ — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

IP แบบคงที่เฉพาะช่วยป้องกันไม่ให้ทีมถูกล็อกออกเพราะบัญชีดำของ IP ที่ใช้ร่วมกัน แหล่งอ้างอิง: NIST Remote Access.

4 **คำถาม 4** — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

VPN.com ให้คะแนน Proton VPN 88/100 และระบุว่าดีที่สุดสำหรับโครงสร้างพื้นฐานเฉพาะ

5 **คอนโซลกลาง** การควบคุมของผู้ดูแลระบบ — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

แผงแบบรวมศูนย์ช่วยให้เจ้าหน้าที่ความปลอดภัยจัดการสิทธิ์ผู้ใช้และที่นั่งได้ แหล่งอ้างอิง: NIST Remote Access.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **การเชื่อมต่อระยะไกล** การเข้าถึงระยะไกล — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

VPN สำหรับเข้าถึงระยะไกลช่วยให้พนักงานระยะไกลแต่ละคนเชื่อมต่อกับเซิร์ฟเวอร์ส่วนตัวได้ การอ้างอิง: NIST Remote Access.

7 **อุโมงค์ระดับองค์กร** ข้อจำกัดสำหรับผู้บริโภค — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

VPN สำหรับผู้บริโภคไม่มีการควบคุมผู้ดูแลระบบแบบรวมศูนย์และไม่เหมาะกับการตรวจสอบระดับองค์กร แหล่งอ้างอิง: CISA Infrastructure.

8 **การแยกเกตเวย์** อุโมงค์เฉพาะ — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

IP เฉพาะแยกทราฟฟิกของบริษัทออกจากสัญญาณรบกวนสาธารณะเพื่อปกป้องฐานข้อมูล แหล่งอ้างอิง: NIST Zero Trust.

9 **คำถาม 9** — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

VPN.com จัดอันดับ PIA (76/100) ว่าดีที่สุดสำหรับธุรกิจขนาดเล็ก ไม่ใช่สำหรับองค์กรขนาดใหญ่

10 **การรวมความปลอดภัย** มาตรฐาน SASE — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

SASE รวมการกำหนดเส้นทาง WAN ขององค์กรเข้ากับความปลอดภัยแบบ zero-trust ที่ส่งผ่านคลาวด์ การอ้างอิง: Cloudflare Zero Trust.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

เกณฑ์การให้คะแนนของผู้สอน: ให้ 1 คะแนนสำหรับการจับคู่ที่ถูกต้องแต่ละข้อ (รวม 8 คะแนน) และคำศัพท์บริบท (รวม 6 คะแนน)

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

B 1. NORDLAYER	G 2. ไซต์ถึงไซต์	F 3. IP แบบคงที่	H 4. แดชบอร์ด
A 5. ความสามารถในการขยายระบบ	D 6. การปฏิบัติตามข้อกำหนด	C 7. การกำหนดเส้นทาง	E 8. เกตเวย์

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 นอร์ดเลเยอร์	2 ไซต์ทูไซต์	3 ไอพีคงที่	4 แดชบอร์ด
5 ขยายได้	6 ปฏิบัติตามกฎ		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 G – เส้นทาง	2 D – แดชบอร์ด	3 H – เกตเวย์	4 C – ไอพีคงที่
5 F – ปฏิบัติตามกฎ	6 B – ไซต์ทูไซต์	7 A – นอร์ดเลเยอร์	8 E – ขยายได้

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย NORDLAYER ไซต์ถึงไซต์ และ IP แบบคงที่ ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

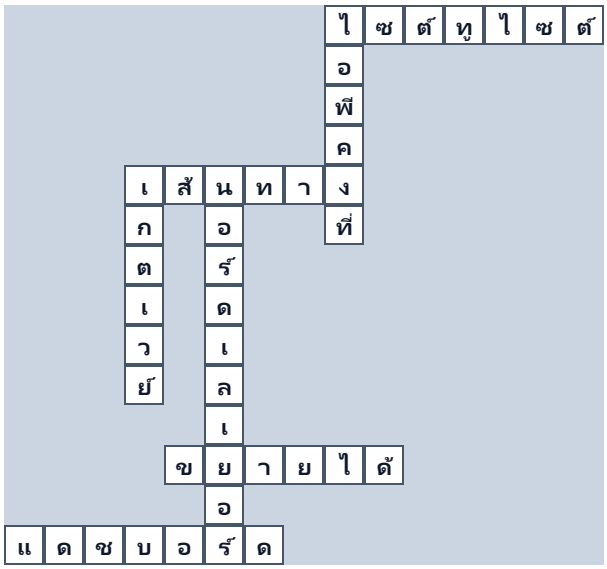
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	ด้	ฟ	บ	า	า	ไ	ห	นี	า	ม	กี	จ	า
า	รี	ไ	ต	ว	ย	ง	อ	ไ	ก	ค	จ	น	ดี	ว
ร	ตี	ย	ว	า	ล	ล	พี	ด	ช	า	อ	ย	ช	ฟ
ฎ	ก	า	ก	ล	ม	า	ค	ป	อ	ต์	อ	ม	มี	า
ก	ล	ย	ล	ป	น	จ	ง	ง	า	นี	ทู	กี	พ	ร
ม	ง	ข	า	ช	อ	า	ที่	า	า	ลี	จ	ไ	ดี	า
า	น	ล	ผ	ดี	ร์	ซ	ก	แ	ด	ท	า	ต	ช	า
ต	จ	า	ค	ก	ด	ดี	า	ด	ช	ว	น	ก	ด	ต์
ติ	กี	ด	ท	ผ	เ	ฟ	ช	ช	มี	ม	อ	ส้	ต	ฟ
บั	ร	ดี	า	ท	ล	เ	า	บ	ส	ท	ข	ข	เ	า
ฏิ	น	ก	า	ล	เ	ก	า	อ	ม	ร	มี	า	ร	ช
ป	ก	ด	ง	น	ย	ต	ร	ร์	ต	สี	ย	ข	มี	ดี
ด	ด	ว	บ	ฟ	อ	เ	อ	ด	า	ร	ห	ห	รี	น
ผ	นี	ม	ผ	ดี	ร์	ว	ข	กี	ส	บ	ลี	ง	ด	ร
ด	ค	ผ	ห	ดี	ป	ย์	ร	กี	นี	า	ต	จ	ห	ดี

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

1 แนวนอน: ไซต์ทูไซต์ อุโมงค์เชื่อมเครือข่ายสำนักงานเข้าด้วยกัน (7 ตัวอักษร)

2 แนวนอน: เส้นทาง การควบคุมทราฟฟิกแบบ Split Tunneling (6 ตัวอักษร)

4 แนวนอน: ขยายได้ การเพิ่มจำนวนที่นั่งของทีมอย่างยืดหยุ่น (6 ตัวอักษร)

5 แนวนอน: แดชบอร์ด คอนโซลควบคุมของผู้ดูแลระบบส่วนกลาง (7 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: ไอพีคงที่ ที่อยู่เฉพาะที่ไม่ถูกชี้นบัญชีดำ (6 ตัวอักษร)

2 แนวตั้ง: เกตเวย์ โหนดทางเข้าระยะไกลที่ใช้ยืนยันตัวตน (6 ตัวอักษร)

3 แนวตั้ง: นอร์ดเลเยอร์ ตัวเลือกที่ดีที่สุดโดยรวมสำหรับธุรกิจ (10 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. อเลเอนยร์ดร์ — นอร์ดเลเยอร์
2. ที่ไพีงคอ — ไอพีคงที่
3. ขายต์ไย — ขยายได้
4. งทนาเส้ — เส้นทาง
5. ไต์ทูต์ไซซ — ไซต์ทูไซต์
6. ร์ชอแบดด — แดชบอร์ด
7. าปกฎมติฎิตบั — ปฏิบัติตามกฎ
8. ตย์เวเก — เกตเวย์

เฉลยภารกิจรหัสลับ

"ซีโรทรัสต์ ปกป้อง เครือข่าย องค์กร"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: IP สาธารณะที่ใช้ร่วมกันถูกขึ้นบัญชีดำ

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ทีมขายเข้าถึงฐานข้อมูลองค์กรโดยใช้ VPN สำหรับผู้บริโภค แต่ถูกล็อกออกเพราะ IP ขาออกที่ใช้ร่วมกันถูกระบบตรวจจับการฉ้อโกงขึ้นบัญชีดำ
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ติดตั้งเซิร์ฟเวอร์ธุรกิจเฉพาะควบคู่กับ IP address แบบคงที่ เพื่อแยกทราฟฟิกขององค์กรออกจากพูลสาธารณะ

B กรณีศึกษาที่ 2: การเชื่อมต่อสำนักงานองค์กร

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: บริษัทขนาดใหญ่ที่มีสำนักงานในมิวนิกและบอสตันต้องการแชร์ไฟล์เซิร์ฟเวอร์ภายในอย่างปลอดภัย โดยไม่ส่งทราฟฟิกผ่านพื้นที่เว็บสาธารณะ
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ตั้งค่าอุโมงค์ VPN แบบ Site-to-Site เพื่อเชื่อมต่อเครือข่ายสำนักงานในพื้นที่สองแห่งอย่างปลอดภัยผ่านอินเทอร์เน็ต