ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

วิธีตั้งค่า VPN ใบงาน

การตั้งค่า VPN บน Windows, macOS, Android, iOS, Linux และเราเตอร์

ภาพรวมการเรียนรู้ VPN

ผู้เรียน
สถานะนักเรียน
สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย
สถานะการเชื่อมต่อ
การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน
การป้องกันการรั่วไหล
การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับหลักการพื้นฐานของเครือข่ายส่วนตัวเสมือน (VPN) คุณจะได้สำรวจว่าอุโมงค์ที่เข้ารหัสปกป้องข้อมูลของคุณอย่างไร โปรโตคอลเครือข่ายทำงานอย่างไร และวิธีระบุและลดการรั่วไหลของความเป็นส่วนตัว

จุดตรวจสอบของใบงาน

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

เปิดคู่มือ VPN ของ VPN.com

URL: https://www.vpn.com/th/vpn/

เส้นทางการเรียนรู้ VPN ของคุณ

- เปรียบเทียบแอป VPN เชิงพาณิชย์กับการตั้งค่าไคลเอนต์แบบเนทีฟ
- ตั้งค่าการเชื่อมต่อ VPN บนเราเตอร์เพื่อป้องกันทั้งบ้าน
- ตั้งค่าและจัดการไฟล์การกำหนดค่า เช่น OVPN หรือกุญแจ WireGuard
- เปิดและรักษาความปลอดภัยพอร์ตเราเตอร์ที่เฉพาะเจาะจงสำหรับทราฟฟิกอุโมงค์
- ตรวจสอบการตั้งค่าไคลเอนต์ด้วยการตรวจการรั่วไหลของ DNS และการทดสอบการเชื่อมต่อ

คำแนะนำใบงานการตั้งค่า

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การตั้งค่าและการทดสอบไคลเอนต์ VPN ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การกำหนดค่า VPN (บทนำ)

การตั้งค่า VPN ด้วยตนเองให้คุณควบคุมกุญแจเข้ารหัสและการกำหนดเส้นทางเครือข่ายได้อย่างเต็มที่ ไม่ว่าจะตั้งค่าไคลเอนต์เนทีฟบนอุปกรณ์มือถือหรือติดตั้งอุโมงค์ VPN บนเราเตอร์โดยตรง การกำหนดค่าที่เหมาะสมเป็นกุญแจสำคัญในการป้องกันการรั่วไหลของ DNS และการรักษาความปลอดภัยทราฟฟิกเครือข่ายทั้งหมด

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. **วิธีที่ง่ายที่สุดในการตั้งค่า VPN บนอุปกรณ์มือถือคืออะไร?**
   - A. ดาวน์โหลดแอป VPN อย่างเป็นทางการจากแอปสโตร์
   - B. แก้ไขไฟล์เคอร์เนลของระบบปฏิบัติการด้วยตนเอง
   - C. แฟลชเฟิร์มแวร์แบบกำหนดเองลงบนฮาร์ดแวร์ของอุปกรณ์
   - D. เชื่อมต่อโทรศัพท์กับคอมพิวเตอร์เดสก์ท็อปผ่าน USB

2. **ประโยชน์ของการติดตั้ง VPN บนเราเตอร์โดยตรงคืออะไร?**
   - A. เพิ่มความเร็วการเชื่อมต่อของอุปกรณ์ในเครื่องทั้งหมด
   - B. รักษาความปลอดภัยให้อุปกรณ์เครือข่ายที่เชื่อมต่อทั้งหมดโดยอัตโนมัติ
   - C. ไม่ต้องจ่ายค่าบริการ ISP ในพื้นที่
   - D. ไม่ต้องใช้เราเตอร์ฮาร์ดแวร์อีกเลย

3. **การกำหนดค่า VPN แบบ "เนทีฟ" หมายถึงอะไร?**
   - A. การตั้งค่าการเชื่อมต่อโดยใช้การตั้งค่าในตัวของระบบปฏิบัติการ
   - B. ใช้ VPN เฉพาะในบ้านเกิดของคุณ
   - C. การเชื่อมต่อเฉพาะเซิร์ฟเวอร์ในประเทศที่คุณอยู่
   - D. การเขียนโปรโตคอลแบบกำหนดเองด้วยภาษาแอสเซมบลี

4. **ต้องใช้อะไรสำหรับการกำหนดค่า OpenVPN ภายนอกด้วยตนเอง?**
   - A. การออกแบบโลโก้แบบกำหนดเองสำหรับการเชื่อมต่อเซิร์ฟเวอร์
   - B. การนำเข้าโปรไฟล์ .ovpn ที่มีกุญแจใบรับรอง
   - C. การเปลี่ยนตำแหน่งทางกายภาพของเราเตอร์ที่บ้าน
   - D. การปิดไฟร์วอลล์ของระบบปฏิบัติการทั้งหมด

5. **เหตุใดผู้ดูแลระบบจึงใช้การแยกอุโมงค์ (split tunneling) ในการตั้งค่า?**
   - A. เพื่อบล็อกทราฟฟิกอินเทอร์เน็ตทั้งหมดโดยสิ้นเชิง
   - B. เพื่ออนุญาตให้แอปที่ปลอดภัยบางตัวข้ามอุโมงค์ที่ปลอดภัย
   - C. เพื่อแบ่งเราเตอร์จริงออกเป็นสองเครื่องแยกกัน
   - D. เพื่อปิดการเข้ารหัสสำหรับการเฝ้าติดตามของผู้ดูแลระบบ

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. การตั้งค่า VPN บนเราเตอร์เป็นกระบวนการง่ายๆ ที่ไม่ต้องใช้ทักษะทางเทคนิค

○ จริง ○ เท็จ

7 คำถาม 7

7. Windows และ macOS มีไคลเอนต์แบบเนทีฟที่รองรับ IKEv2 และ L2TP

○ จริง ○ เท็จ

8 คำถาม 8

8. การตั้งค่า WireGuard ต้องสร้างกุญแจสาธารณะและกุญแจส่วนตัว

○ จริง ○ เท็จ

9 คำถาม 9

9. อุโมงค์ VPN ช่วยรักษาความปลอดภัยของเครื่องพิมพ์ในเครือข่ายภายในและงานพิมพ์ของคุณ

○ จริง ○ เท็จ

10 คำถาม 10

10. สมาร์ทล็อกที่ใช้แอป VPN ไม่ได้ต้องใช้ VPN ระดับเราเตอร์จึงจะได้รับการครอบคลุม

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. การติดตั้ง VPN ที่ระดับเกตเวย์ของ _____ ปกป้องสมาร์ตทีวีและเครื่องเล่นเกม
2. การกำหนดค่า OpenVPN ด้วยตนเองต้องนำเข้าโปรไฟล์เซิร์ฟเวอร์ _____
3. การกำหนดค่าที่มีมากับระบบปฏิบัติการใช้การตั้งค่าไคลเอนต์ _____ ของระบบ
4. การยืนยันตัวตนของ WireGuard อาศัยกุญแจสาธารณะและกุญแจส่วนตัวเข้ารหัสลับที่เป็น _____
5. การติดตั้งที่ใช้งานง่ายทำได้ผ่าน _____ ทางการของผู้ให้บริการ
6. การส่งคิวรีผ่านเซิร์ฟเวอร์ VPN ของ _____ ช่วยป้องกันการรั่วไหลจากการติดตามการแปลงชื่อ

คลังคำศัพท์

คู่กุญแจ | ดีเอ็นเอส | เนทีฟ | บันทึกล็อก | แยกอุโมงค์ | เราเตอร์ | แอป | โอวีพีเอ็น

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องเครือข่าย

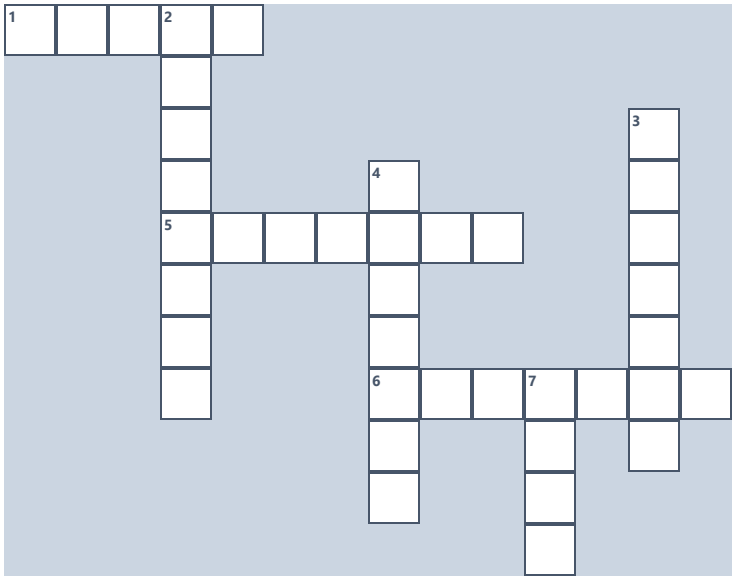
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. แอป VPN**	**A**	การเข้ารหัสระดับเกตเวย์ที่ปกป้องเครื่องใช้อัจฉริยะทั้งหมดในเครือข่ายภายใน
☐	**2. VPN บนเราเตอร์**	**B**	แพ็กเกจซอฟต์แวร์ที่บริการสมัครสมาชิกให้มาเพื่อการตั้งค่าที่ง่ายด้วยการคลิกเดียว
☐	**3. ไคลเอนต์เนทีฟ**	**C**	ตรวจสอบเอาต์พุตข้อผิดพลาดและบันทึกสถานะไคลเอนต์เพื่อดีบักการตั้งค่าที่ล้มเหลว
☐	**4. โปรไฟล์ .ovpn**	**D**	การแยกเส้นทางทราฟฟิกเพื่อให้บางแอปข้ามอุโมงค์ที่เข้ารหัสได้
☐	**5. คู่คีย์**	**E**	การรักษาความปลอดภัยทราฟฟิกภายในการตั้งค่าของระบบปฏิบัติการเองโดยไม่ต้องติดตั้งแอป
☐	**6. Split Tunneling**	**F**	การตั้งค่าที่อยู่ตัวแปลงชื่อของเครือข่ายเพื่อป้องกันการรั่วไหลของการค้นหาโดเมน
☐	**7. การตั้งค่าเซิร์ฟเวอร์ DNS**	**G**	โทเค็นเข้ารหัส (สาธารณะ/ส่วนตัว) ที่จำเป็นต่อการสร้างการแฮนด์เชค WireGuard
☐	**8. บันทึกการเชื่อมต่อ**	**H**	รูปแบบไฟล์ OpenVPN ที่มีเซิร์ฟเวอร์ การตั้งค่าพอร์ต และกุญแจใบรับรอง

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

1. โทเค็นเข้ารหัสลับ (สาธารณะ/ส่วนตัว) ที่จำเป็นต่อการสร้างการจับมือของ WireGuard (5)

5. รูปแบบไฟล์ OpenVPN ที่มีเซิร์ฟเวอร์ การตั้งค่าพอร์ต และกุญแจใบรับรอง (7)

6. การเข้ารหัสระดับเกตเวย์ที่ปกป้องเครื่องใช้อัจฉริยะทุกชิ้นในเครือข่ายภายใน (7)

แนวตั้ง

2. การแยกเส้นทางทราฟฟิกเพื่อให้บางแอปข้ามอุโมงค์ที่เข้ารหัส (8)

3. การตรวจสอบเอาต์พุตข้อผิดพลาดและล็อกสถานะไคลเอนต์เพื่อแก้ไขการตั้งค่าที่ล้มเหลว (7)

4. การกำหนดที่อยู่ตัวแปลงชื่อเครือข่ายเพื่อป้องกันการรั่วไหลของการค้นหาโดเมน (7)

7. การรักษาความปลอดภัยทราฟฟิกภายในการตั้งค่าของระบบปฏิบัติการเองโดยไม่ต้องติดตั้งแอป (4)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

1 แนวนอน: โทเค็นเข้ารหัสลับ (สาธารณะ/ส่วนตัว) ที่จำเป็นต่อการสร้างการจับมือของ WireGuard (5 ตัวอักษร):

5 แนวนอน: รูปแบบไฟล์ OpenVPN ที่มีเซิร์ฟเวอร์ การตั้งค่าพอร์ต และกุญแจใบรับรอง (7 ตัวอักษร):

6 แนวนอน: การเข้ารหัสระดับเกตเวย์ที่ปกป้องเครื่องใช้อัจฉริยะทุกชิ้นในเครือข่ายภายใน (7 ตัวอักษร):

แนวตั้ง

2 แนวตั้ง: การแยกเส้นทางทราฟฟิกเพื่อให้บางแอปข้ามอุโมงค์ที่เข้ารหัส (8 ตัวอักษร):

3 แนวตั้ง: การตรวจสอบเอาต์พุตข้อผิดพลาดและล็อกสถานะไคลเอนต์เพื่อแก้ไขการตั้งค่าที่ล้มเหลว (7 ตัวอักษร):

4 แนวตั้ง: การกำหนดที่อยู่ตัวแปลงชื่อเครือข่ายเพื่อป้องกันการรั่วไหลของการค้นหาโดเมน (7 ตัวอักษร):

7 แนวตั้ง: การรักษาความปลอดภัยทราฟฟิกภายในการตั้งค่าของระบบปฏิบัติการเองโดยไม่ต้องติดตั้งแอป (4 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า า รี ต ว ย ง ก ค จ น ตี ว ร ตี
ว า ล ล ด า อ ย ดี ซ ฟ ก ก ล ม
า ป อ อ ม มี า ล ล เ ป จ า นี กี
พ ร ก อ ล็ ก ที น บั ง อ็ า ซ า า
ลี จ ดี า น แ ล ผ ดี ซ ก น ด า ต
น า จ า ค ย ก เ ดี จ า ซ เ ว ก
อ็ ป ด กี ด ก ท ผ ร ฟ แ ซ มี อ ม
เ อ อ ต ฟ อุ ร ดี า า ท ญ า ส ส
พี แ ท ข ข โ า น ก า เ ล กุ า ม
วี ร มี า ร ม เ ช ก ด ง ต น คู่ ร
อ ต สี ย ข ง น มี ดี ด ด ว อ บ ฟ
โ อ า ร ห ค์ ที ห รี น ผ นี ม ร์ ผ
ดี ข กี ส บ ลี ฟ ง ด ร ด ค ผ ห ดี
ป ร กี นี า ต จ ห ดี ด บ ตี น สี ลี
ว ลี า ค า า ล ห ป ส ซ ตี ลี ล มี

รายการคำศัพท์

แอป เราเตอร์ เนทีฟ โอวีพีเอ็น คู่กุญแจ แยกอุโมงค์ ดีเอ็นเอส บันทึกล็อก

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. แอป
B. เราเตอร์
C. เนทีฟ
D. โอวีพีเอ็น
E. คู่กุญแจ
F. แยกอุโมงค์
G. ดีเอ็นเอส
H. บันทึกล็อก

คำนิยามและช่องจับคู่	
	1. การกำหนดที่อยู่ตัวแปลงชื่อเครือข่ายเพื่อป้องกันการรั่วไหลของการค้นหาโดเมน
	2. การแยกเส้นทางทราฟฟิกเพื่อให้บางแอปข้ามอุโมงค์ที่เข้ารหัส
	3. การเข้ารหัสระดับเกตเวย์ที่ปกป้องเครื่องใช้อัจฉริยะทุกชิ้นในเครือข่ายภายใน
	4. โทเค็นเข้ารหัสลับ (สาธารณะ/ส่วนตัว) ที่จำเป็นต่อการสร้างการจับมือของ WireGuard
	5. การรักษาความปลอดภัยทราฟฟิกภายในการตั้งค่าของระบบปฏิบัติการเองโดยไม่ต้องติดตั้งแอป
	6. การตรวจสอบเอาต์พุตข้อผิดพลาดและล็อกสถานะไคลเอนต์เพื่อแก้ไขการตั้งค่าที่ล้มเหลว
	7. รูปแบบไฟล์ OpenVPN ที่มีเซิร์ฟเวอร์ การตั้งค่าพอร์ต และกุญแจใบรับรอง
	8. ชุดซอฟต์แวร์ที่บริการสมัครสมาชิกให้มา เพื่อตั้งค่าได้ง่ายด้วยคลิกเดียว

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของ VPN เขียนคำตอบของคุณในช่องกรอกที่กรอกได้

1. อ ป แ
2. เ ท ี ฟ น
3. ญ คู่ จ แ กุ
4. ส เ แ น อ ด ี อ็
5. ต ร์ เ า เ อ ร
6. อ็ ว ี เ โ พ ี น อ
7. แ ค์ โ ม ง ย อุ ก
8. น ก ก บ้ อ ล็ ท ึ

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	สิ่งที่ควรตรวจสอบเมื่อตั้งค่าเสร็จแล้ว			
2	อุปกรณ์ที่ใช้ VPN ได้			
3	บริการ VPN ที่คุณรู้จัก			
4	เหตุผลที่ควรใช้ VPN ขณะเดินทาง			
5	ข้อผิดพลาดที่คนทำระหว่างการตั้งค่า			
6	คำจากใบงานนี้ที่คุณอยากจำ			
7	การตั้งค่าที่คุณเปิดก่อน			
8	คำมั่นสัญญาที่ผู้ให้บริการ VPN ที่ดีให้ไว้			
9	ขั้นตอนเมื่อตั้งค่า VPN			
10	สถานที่ที่คุณจะใช้ VPN			
11	วิธีสังเกตเครือข่าย Wi-Fi ปลอม			
12	สิ่งที่ VPN ซ่อนได้			
13	สิ่งที่ผู้ให้บริการอินเทอร์เน็ตของคุณมองเห็นได้			
14	สถานที่ที่ขอความช่วยเหลือได้			
15	สิ่งที่คุณต้องมีเพื่อเริ่มต้น			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

ซาราห์ (นักเรียนร้านกาแฟ)

👷 "สวัสดี! ฉันนั่งอยู่ที่ Coffee & Bytes มีเครือข่ายสาธารณะที่ไม่ปลอดภัยชื่อ 'Free_Wi-Fi_No_Password' ฉันอยากล็อกอินอีเมลโรงเรียนและอัปโหลดงานที่ได้รับมอบหมาย แต่กังวลเรื่องแฮกเกอร์ การใช้เครือข่ายนี้โดยไม่มี VPN มีความเสี่ยงอะไรบ้าง และ VPN ช่วยรักษาความปลอดภัยของข้อมูลฉันได้อย่างไร?"

อเล็กซ์ (นักเรียนนักท่องเที่ยว)

👷 "แย่แล้ว! ฉันเดินทางไปต่างประเทศเพื่อทำโปรเจกต์ และกำลังพยายามดูสารคดีชีววิทยาที่โฮสต์บนเซิร์ฟเวอร์ในประเทศบ้านเกิด แต่เว็บไซต์ขึ้นข้อความว่า 'วิดีโอนี้ไม่พร้อมใช้งานในตำแหน่งที่ตั้งปัจจุบันของคุณ' ทำไมฉันถึงถูกบล็อก และ VPN ช่วยให้ฉันดูได้อย่างไร?"

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

เพื่อให้การฝึกอบรมการกำหนดค่าเซิร์ฟเวอร์ของคุณเสร็จสมบูรณ์ ให้ถอดรหัสข้อความที่ซ่อนอยู่นี้เกี่ยวกับการตั้งค่าอุโมงค์ที่ปลอดภัย

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

21	51	20	21	48	64	7		57	1	21	57	39	34	67		20	64	39	34

57	20	33	45	25		27	37	45	20	32	48	34

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดที่ผู้สนใจมีเกี่ยวกับการใช้เครือข่ายส่วนตัวเสมือน

Q1: VPN คืออะไรและทำงานอย่างไร?

Virtual Private Network (VPN) เข้ารหัสการเชื่อมต่ออินเทอร์เน็ตของคุณและส่งทราฟฟิกผ่านเซิร์ฟเวอร์ระยะไกลที่ปลอดภัย ซึ่งปกปิดที่อยู่ IP สาธารณะของคุณและจำกัดสิ่งที่ผู้สังเกตการณ์ในเครือข่ายท้องถิ่นและ ISP ของคุณมองเห็นเกี่ยวกับทราฟฟิกที่ผ่านอุโมงค์ VPN

Q2: ฉันต้องเตรียมอะไรเพื่อเริ่มต้น?

คุณต้องมีการสมัครสมาชิก VPN ที่ใช้งานอยู่หรือเซิร์ฟเวอร์ VPN ของคุณเอง อุปกรณ์ที่รองรับ และแอปของผู้ให้บริการหรือรายละเอียดสำหรับการตั้งค่าด้วยตนเอง ได้แก่ ที่อยู่เซิร์ฟเวอร์ โปรโตคอล และข้อมูลรับรอง คีย์ หรือใบรับรองของคุณ คนส่วนใหญ่เพียงติดตั้งแอปอย่างเป็นทางการ เข้าสู่ระบบ แล้วกดเชื่อมต่อ

Q3: ฉันจะตั้งค่า VPN บน Windows โดยไม่ใช้แอปได้อย่างไร?

เปิดการตั้งค่า > เครือข่ายและอินเทอร์เน็ต > VPN เลือกเพิ่ม VPN แล้วกรอกชื่อเซิร์ฟเวอร์ของผู้ให้บริการ ประเภท VPN (เช่น IKEv2 หรือ L2TP/IPsec) และรายละเอียดการลงชื่อเข้าใช้ จากนั้นเลือกเชื่อมต่อ

Q4: VPN จะทำให้ความเร็วอินเทอร์เน็ตของฉันช้าลงหรือไม่?

ได้ เล็กน้อย กระบวนการเข้ารหัสและระยะทางกายภาพไปยังเซิร์ฟเวอร์ VPN เพิ่มความหน่วงและภาระงาน ผลกระทบแตกต่างกันตามผู้ให้บริการ โปรโตคอล ระยะทางเซิร์ฟเวอร์ อุปกรณ์ และสภาพเครือข่าย

Q5: ฉันตั้งค่า macOS ได้อย่างไร?

ติดตั้งแอป macOS ของผู้ให้บริการ หรือเปิด System Settings > VPN เพิ่มการกำหนดค่า VPN เลือก IKEv2, L2TP over IPSec หรือ Cisco IPSec แล้วกรอกที่อยู่เซิร์ฟเวอร์และข้อมูลเข้าสู่ระบบจากผู้ให้บริการของคุณ

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดที่ผู้สนใจมีเกี่ยวกับการใช้เครือข่ายส่วนตัวเสมือน

Q6: ฉันใช้ VPN ฟรีได้หรือไม่?

VPN ฟรีอาจพึ่งพาโฆษณา ฟีเจอร์ที่จำกัด การวิเคราะห์การใช้งาน โควตาข้อมูล หรือโมเดลหารายได้อื่น ผู้ใช้ควรตรวจสอบนโยบายความเป็นส่วนตัว ความเป็นเจ้าของ การตรวจสอบ และโมเดลธุรกิจของผู้ให้บริการก่อนใช้งาน

Q7: ฉันใช้ไฟล์ .ovpn ได้อย่างไร?

ติดตั้งไคลเอนต์ OpenVPN นำเข้าโปรไฟล์ .ovpn จากผู้ให้บริการหรือผู้ดูแลระบบของคุณ แล้วเชื่อมต่อ ไฟล์นี้เก็บที่อยู่เซิร์ฟเวอร์ พอร์ต การตั้งค่า UDP หรือ TCP และมักมีใบรับรองและคีย์ด้วย

Q8: ฉันเลือก VPN ที่ดีที่สุดได้อย่างไร?

มองหานโยบายไม่เก็บล็อกที่ผ่านการตรวจสอบ โปรโตคอลที่แข็งแกร่ง (WireGuard, OpenVPN) ตำแหน่งเซิร์ฟเวอร์ที่ปลอดภัย ความเร็วสูง เซิร์ฟเวอร์แบบใช้ RAM เท่านั้น ฟีเจอร์ kill switch และเขตอำนาจศาลที่อยู่นอกพันธมิตรแบ่งปันข่าวกรอง (เช่น 5/9/14 Eyes)

Q9: ฉันใช้ VPN บนโทรศัพท์และสมาร์ททีวีได้หรือไม่?

ได้ ผู้ให้บริการ VPN สมัยใหม่มีแอปเฉพาะสำหรับ iOS, Android, macOS, Windows, Linux และสมาร์ททีวี รวมถึงการตั้งค่าบนเราเตอร์เพื่อปกป้องทุกอุปกรณ์ในเครือข่ายบ้านของคุณ

Q10: Kill Switch คืออะไร?

Kill Switch คือฟีเจอร์ความปลอดภัยที่ตัดการเชื่อมต่ออุปกรณ์ของคุณจากอินเทอร์เน็ตโดยอัตโนมัติหากการเชื่อมต่อ VPN หลุด ช่วยป้องกันไม่ให้ข้อมูลที่ไม่ได้เข้ารหัสหรือที่อยู่ IP จริงของคุณรั่วไหล

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคและโครงสร้างของเครือข่ายส่วนตัวเสมือนและโปรโตคอลอุโมงค์ที่ปลอดภัย

Q1: WireGuard, OpenVPN และ IKEv2 ต่างกันอย่างไร?

WireGuard เป็นโปรโตคอลสมัยใหม่ที่เบา (โค้ดเพียงประมาณ 4,000 บรรทัด) ให้ความเร็วสูงและเชื่อมต่อได้รวดเร็ว OpenVPN เป็นโปรโตคอลโอเพนซอร์สที่ปลอดภัยสูงและผ่านการใช้งานจริงมาอย่างยาวนาน IKEv2 เหมาะอย่างยิ่งกับอุปกรณ์มือถือเพราะเชื่อมต่อใหม่ได้เร็วเมื่อสลับเครือข่าย

Q2: ฉันตั้งค่า WireGuard ด้วยตนเองได้อย่างไร?

สร้างคู่คีย์ด้วย wg genkey และ wg pubkey แชร์คีย์สาธารณะของคุณกับเซิร์ฟเวอร์ แล้วเขียนไฟล์กำหนดค่าที่ระบุคีย์ส่วนตัวของคุณ คีย์สาธารณะของเพียร์ IP ที่อนุญาต และเอนด์พอยต์ เครื่องมือ wg-quick ใช้เปิดการเชื่อมต่อ [2]

Q3: การรั่วไหลของ WebRTC คืออะไร และ VPN ป้องกันได้อย่างไร?

WebRTC คือโปรโตคอลของเบราว์เซอร์ที่อาจเปิดเผยที่อยู่ IP ภายในและสาธารณะจริงของคุณ แม้จะเปิดใช้ VPN อยู่ VPN ระดับพรีเมียมจะบล็อกหรือปลอมคำขอ WebRTC ในแอปเดสก์ท็อป/มือถือและส่วนขยายเบราว์เซอร์

Q4: ฉันตั้งค่า VPN บนเราเตอร์ที่บ้านอย่างปลอดภัยได้อย่างไร?

ตรวจสอบว่าเราเตอร์ของคุณรองรับโหมดไคลเอนต์ VPN เข้าสู่ระบบหน้าผู้ดูแล แล้วอัปโหลดไฟล์ OpenVPN หรือ WireGuard ของผู้ให้บริการ เราเตอร์บางรุ่นต้องอัปเดตเฟิร์มแวร์ก่อน หลังจากนั้นทุกอุปกรณ์ในเครือข่ายจะใช้อุโมงค์นี้

Q5: การพรางทราฟฟิก (Obfuscation) หลบเลี่ยงการบล็อก VPN ได้อย่างไร?

การอำพราง (หรือ "Stealth VPN") ทำให้ทราฟฟิก VPN ดูเหมือนทราฟฟิก HTTPS ปกติ (พอร์ต 443) ซึ่งอาจช่วยให้ผ่านการตรวจสอบแพ็กเก็ตเชิงลึก (DPI) ที่รัฐบาลหรือเครือข่ายโรงเรียน/สำนักงานใช้บล็อก VPN

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคและโครงสร้างของเครือข่ายส่วนตัวเสมือนและโปรโตคอลอุโมงค์ที่ปลอดภัย

Q6: Split Tunneling คืออะไร และฉันควรใช้เมื่อใด?

Split Tunneling ให้คุณเลือกได้ว่าแอปใดส่งผ่านอุโมงค์ VPN ที่เข้ารหัสและแอปใดเชื่อมต่ออินเทอร์เน็ตโดยตรง ใช้เพื่อส่งแอปธนาคารที่ละเอียดอ่อนผ่าน VPN ขณะที่เกมในพื้นที่เชื่อมต่อโดยตรง เพื่อหลีกเลี่ยงความหน่วงที่ VPN เพิ่มขึ้น

Q7: ฉันตรวจสอบได้อย่างไรว่าการตั้งค่า VPN ใหม่ของฉันทำงานอยู่?

เชื่อมต่อ แล้วเข้าเว็บไซต์ตรวจสอบ IP ซึ่งควรแสดง IP และตำแหน่งของเซิร์ฟเวอร์ VPN รันการทดสอบการรั่วไหลของ DNS และ WebRTC และตัดการเชื่อมต่อชั่วครู่เพื่อยืนยันว่า Kill Switch บล็อกทราฟฟิก

Q8: ฉันควรตรวจสอบอะไรหาก VPN ของฉันเชื่อมต่อไม่ได้หลังตั้งค่า?

ตรวจสอบข้อมูลเข้าสู่ระบบหรือกุญแจ ที่อยู่เซิร์ฟเวอร์ และว่าพอร์ตกับโปรโตคอลที่เลือกไม่ถูกบล็อก ลองสลับระหว่าง UDP และ TCP หรือเซิร์ฟเวอร์อื่น และอ่านบันทึกการเชื่อมต่อของแอปเพื่อหาข้อผิดพลาด

Q9: การป้องกัน DNS Leak คืออะไร?

การป้องกันการรั่วไหลของ DNS บังคับให้อุปกรณ์ของคุณส่งคำค้นหาเว็บไซต์ (คำขอ DNS) ผ่านเซิร์ฟเวอร์ DNS ส่วนตัวที่เข้ารหัสของ VPN แทนเซิร์ฟเวอร์ของ ISP ซึ่งช่วยป้องกันไม่ให้ ISP ติดตามว่าคุณเข้าเว็บไซต์ใด

Q10: VPN ควรเริ่มทำงานอัตโนมัติหรือไม่?

โดยปกติใช่ แอปส่วนใหญ่เปิดตอนเริ่มระบบและเชื่อมต่ออัตโนมัติ หรือเมื่ออยู่บน Wi-Fi ที่ไม่น่าเชื่อถือ ทำให้คุณได้รับการปกป้องก่อนที่แอปอื่นจะเริ่มส่งข้อมูล

ส่วนที่ 11: ข้อเท็จจริงน่าสนใจเกี่ยวกับ VPN 10 ข้อและข้อมูลเชิงลึกในโลกจริง

ทบทวนข้อเท็จจริงและข้อมูลเชิงลึกในโลกจริงที่มีคุณค่าสูงเกี่ยวกับประวัติ ตลาด และเทคโนโลยีของ VPN

1. ไคลเอนต์เนทีฟ

ทั้ง Windows และ macOS มีไคลเอนต์ VPN ในตัวที่รองรับ IKEv2 และ L2TP/IPsec จึงตั้งค่าการเชื่อมต่อได้หลายแบบโดยไม่ต้องใช้แอปเพิ่มเติม

2. การสร้างคีย์

การเริ่มต้นอย่างรวดเร็วของ WireGuard สร้างกุญแจส่วนตัวด้วย wg genkey และสร้างกุญแจสาธารณะจากกุญแจนั้นด้วย wg pubkey [2]

3. การปฏิวัติ WireGuard

WireGuard มีโค้ดที่เรียบง่ายมากซึ่งออกแบบมาเพื่อประสิทธิภาพ ทำให้ตรวจสอบช่องโหว่ด้านความปลอดภัยได้ง่ายกว่าโปรโตคอลแบบดั้งเดิม [1]

4. ไฟล์โปรไฟล์

โปรไฟล์ .ovpn รวมที่อยู่เซิร์ฟเวอร์ พอร์ต โปรโตคอล และใบรับรองไว้ด้วยกัน ดังนั้นการนำเข้าเพียงครั้งเดียวก็ตั้งค่าการเชื่อมต่อ OpenVPN ได้

5. พอร์ตเริ่มต้น

โดยทั่วไป OpenVPN ใช้พอร์ต 1194 ส่วนตัวอย่างทางการของ WireGuard ใช้พอร์ต UDP 51820 ไฟร์วอลล์และเราเตอร์อาจต้องอนุญาตพอร์ตเหล่านี้เพื่อให้อุโมงค์เชื่อมต่อได้

6. การตรวจสอบแพ็กเก็ตเชิงลึก

การตรวจสอบแพ็กเก็ตเชิงลึก (DPI) สามารถตรวจจับและบล็อกโปรโตคอล VPN ทั่วไปได้ การสลับไปใช้ OpenVPN ผ่านพอร์ต TCP 443 หรือโหมดอำพราง อาจช่วยได้

7. ครอบคลุมเราเตอร์

VPN บนเราเตอร์ปกป้องทุกอุปกรณ์ที่อยู่ภายใต้เราเตอร์ รวมถึงคอนโซลและสมาร์ตทีวีที่รันแอป VPN ไม่ได้ โดยไม่ต้องติดตั้งอะไรบนแต่ละอุปกรณ์

8. KEEPALIVES

เมื่ออยู่หลัง NAT หรือไฟร์วอลล์ การตั้งค่า PersistentKeepalive ของ WireGuard ซึ่งมักตั้งไว้ 25 วินาที จะทำให้อุโมงค์ยังเข้าถึงได้ [2]

9. ไดรเวอร์ TUN/TAP

OpenVPN ออกแบบมาให้ทำงานกับอินเทอร์เฟซเครือข่ายเสมือน TUN/TAP ซึ่งมีบนเกือบทุกแพลตฟอร์มและถูกตั้งค่าเมื่อคุณติดตั้งไคลเอนต์ [3]

10. การทำ Split Tunneling

ระหว่างการตั้งค่า การแยกอุโมงค์ช่วยให้คุณยกเว้นบางแอปหรือที่อยู่ออกจาก VPN ซึ่งช่วยกับเครื่องพิมพ์ในเครือข่ายหรือแอปที่บล็อกที่อยู่ IP ของ VPN

แหล่งอ้างอิงทางเทคนิค

สิ่งพิมพ์ที่อ้างอิง ข้อกำหนดด้านการเข้ารหัส และมาตรฐานเอกสารทางการที่ใช้ตลอดทั้งใบงานนี้

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[2] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

[3] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[4] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[5] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

เฉลย: การตั้งค่า VPN บน Windows, macOS, Android, iOS, Linux และเราเตอร์

1 **คำถาม 1** คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

วิธีที่ง่ายที่สุดในการตั้งค่า VPN บนอุปกรณ์มือถือคืออะไร? → ดาวน์โหลดแอป VPN อย่างเป็นทางการจากแอปสโตร์

2 **การตั้งค่าเกตเวย์เราเตอร์** เวลาแฝง คำตอบที่ถูกต้อง: B

หมายเหตุสำหรับผู้สอน

VPN บนเราเตอร์เข้ารหัสทราฟฟิกที่เกตเวย์ ปกป้องอุปกรณ์ IoT คอนโซล และเครื่องใช้อัจฉริยะที่ติดตั้งแอปพลิเคชัน VPN ในตัวไม่ได้ อ้างอิง: DD-WRT OpenVPN Clients, Linksys Router Config. [3]

3 **คำถาม 3** คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

Windows และ macOS มีไคลเอนต์ในตัวสำหรับโปรโตคอลอย่าง IKEv2 และ L2TP/IPsec จึงตั้งค่าการเชื่อมต่อได้โดยไม่ต้องติดตั้งซอฟต์แวร์เพิ่ม

4 **การนำเข้าโปรไฟล์ OpenVPN** การควบคุมการกำหนดเส้นทาง คำตอบที่ถูกต้อง: B

หมายเหตุสำหรับผู้สอน

การกำหนดค่าด้วยตนเองต้องดาวน์โหลดคีย์โปรไฟล์.ovpn ที่มีพอร์ตเซิร์ฟเวอร์ปลายทาง พารามิเตอร์โปรโตคอล (UDP/TCP) และใบรับรองการเข้ารหัส อ้างอิง: DD-WRT OpenVPN Clients.

5 **การกำหนดเส้นทางแบบ Split Tunnel** ความเป็นส่วนตัว คำตอบที่ถูกต้อง: B

หมายเหตุสำหรับผู้สอน

Split tunneling ช่วยให้ผู้ใช้สงแอปงานที่ละเอียดอ่อนผ่านอุโมงค์ที่เข้ารหัส ขณะที่สตรีมมิงหรือเกมในพื้นที่เชื่อมต่อโดยตรงโดยไม่มีภาระจาก VPN การอ้างอิง: IETF IKEv2 RFC.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

การตั้งค่าบนเราเตอร์หมายถึงการเข้าสู่หน้าผู้ดูแลระบบ ตรวจสอบการรองรับ VPN และอัปโหลดไฟล์คอนฟิก

7 **การผสานรวมกับระบบปฏิบัติการแบบเนทีฟ** ความเร็ว คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

ระบบปฏิบัติการหลักมีการผสานโปรโตคอลแบบเนทีฟในตัว เพื่อให้ตั้งค่าการเชื่อมต่อที่ปลอดภัยได้อย่างราบรื่น อ้างอิง: Microsoft Native Gateway, Apple Support Profiles.

8 **การจับคู่คีย์ WireGuard** ความเสี่ยงจากการดักจับแพ็กเก็ต คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

WireGuard ใช้กุญแจอสมมาตรเพื่อสร้างแฮนด์เชค P2P ที่ปลอดภัย แทนที่จะพึ่งรหัสผ่านหรือสายโซ่ CA การอ้างอิง: WireGuard CLI Specifications.

9 **การบล็อกทราฟฟิกภายในเครื่อง** ไฟร์วอลล์ คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

โดยปกติ VPN จะส่งทราฟฟิกอินเทอร์เน็ตสาธารณะ และบางครั้งอาจบล็อกการเข้าถึงเครื่องพิมพ์ในเครือข่ายท้องถิ่น เว้นแต่จะตั้งค่าไว้เป็นอย่างอื่น อ้างอิง: Microsoft Native Gateway.

10 **คำถาม 10** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

สมาร์ทล็อกที่ใช้แอป VPN ไม่ได้ต้องใช้ VPN ระดับเราเตอร์จึงจะได้รับการครอบคลุม

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

B 1. แอป VPN	A 2. VPN บนเราเตอร์	E 3. ไคลเอนต์เนทีฟ	H 4. โปรไฟล์ .ovpn
G 5. คู่คีย์	D 6. Split Tunneling	F 7. การตั้งค่าเซิร์ฟเวอร์ DNS	C 8. บันทึกการเชื่อมต่อ

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 เราเตอร์	2 โอวีพีเอ็น	3 เนทีฟ	4 คู่กุญแจ
5 แอป	6 ดีเอ็นเอส		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 G – ดีเอ็นเอส	2 F – แยกอุโมงค์	3 B – เราเตอร์	4 E – คู่กุญแจ
5 C – เนทีฟ	6 H – บันทึกล็อก	7 D – โอวีพีเอ็น	8 A – แอป

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย แอป VPN VPN บนเราเตอร์ และ ไคลเอนต์เนทีฟ ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

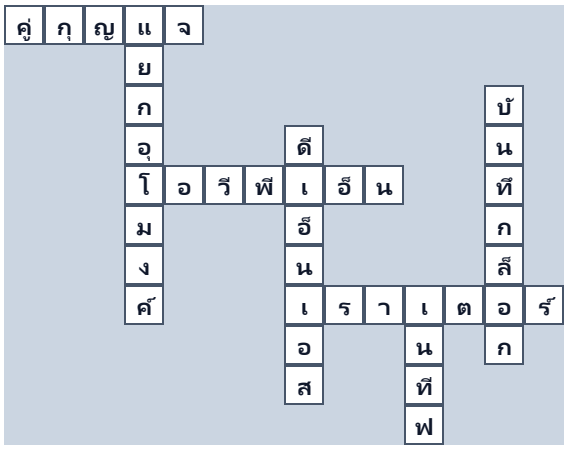
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	า	รี	ต	ว	ย	ง	ก	ค	จ	น	ตี	ว	ร	ตี
ว	า	ล	ล	ด	า	อ	ย	ดี	ช	ฟ	ก	ก	ล	ม
า	ป	อ	อ	ม	มี	า	ล	ล	เ	ป	จ	า	นี	กี
พ	ร	ก	อ	ล็	ก	ที	น	บั	ง	อ็	า	ช	า	า
ลี	จ	ดี	า	น	แ	ล	ผ	ดี	ช	ก	น	ด	า	ต
น	า	จ	า	ค	ย	ก	เ	ดี	จ	า	ช	เ	ว	ก
อ็	ป	ด	กี	ด	ก	ท	ผ	ร	ฟ	แ	ช	มี	อ	ม
เ	อ	อ	ต	ฟ	อุ	ร	ดี	า	า	ท	ญ	า	ส	ส
พี	แ	ท	ข	ข	โ	า	น	ก	า	เ	ล	กุ	า	ม
วี	ร	มี	า	ร	ม	เ	ช	ก	ด	ง	ต	น	คู่	ร
อ	ต	สี	ย	ข	ง	น	มี	ดี	ด	ด	ว	อ	บ	ฟ
โ	อ	า	ร	ห	ค์	ที	ห	รี	น	ผ	นี	ม	ร์	ผ
ดี	ข	กี	ส	บ	ลี	ฟ	ง	ด	ร	ด	ค	ผ	ห	ดี
ป	ร	กี	นี	า	ต	จ	ห	ดี	ด	บ	ตี	น	สี	ลี
ว	ลี	า	ค	า	า	ล	ห	ป	ส	ช	ตี	ลี	ล	มี

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

1 แนวนอน: คู่กุญแจ โทเค็นเข้ารหัสลับ (สาธารณะ/ส่วนตัว) ที่จำเป็นต่อการสร้างการจับมือของ WireGuard (5 ตัวอักษร)

5 แนวนอน: โอวีพีเอ็น รูปแบบไฟล์ OpenVPN ที่มีเซิร์ฟเวอร์ การตั้งค่า พอร์ต และกุญแจใบรับรอง (7 ตัวอักษร)

6 แนวนอน: เราเตอร์ การเข้ารหัสระดับเกตเวย์ที่ปกป้องเครื่องใช้อัจฉริยะทุกชิ้นในเครือข่ายภายใน (7 ตัวอักษร)

แนวตั้ง

2 แนวตั้ง: แยกอุโมงค์ การแยกเส้นทางทราฟฟิกเพื่อให้บางแอปข้ามอุโมงค์ที่เข้ารหัส (8 ตัวอักษร)

3 แนวตั้ง: บันทึกล็อก การตรวจสอบเอาต์พุตข้อผิดพลาดและล็อกสถานะไคลเอนต์เพื่อแก้ไขการตั้งค่าที่ล้มเหลว (7 ตัวอักษร)

4 แนวตั้ง: ดีเอ็นเอส การกำหนดที่อยู่ตัวแปลงชื่อเครือข่ายเพื่อป้องกันการรั่วไหลของการค้นหาโดเมน (7 ตัวอักษร)

7 แนวตั้ง: เนทีฟ การรักษาความปลอดภัยทราฟฟิกภายในการตั้งค่าของระบบปฏิบัติการเองโดยไม่ต้องติดตั้งแอป (4 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. อปแ → **แอป**
2. เทีฟน → **เนทีฟ**
3. ญคู่จแกุ → **คู่กุญแจ**
4. สแนอดีอี → **ดีเอ็นเอส**
5. ตร์เาเอร → **เราเตอร์**
6. อีวีเโพีนอ → **โอวีพีเอ็น**
7. แศ์โมงยอุก → **แยกอุโมงศ์**
8. นกกบ้อล็ทึ → **บันทึกล็อก**

เฉลยภารกิจรหัสลับ

"ติดตั้ง เกตเวย์ ด้วย เดมอน ปลอดภัย"

เฉลยกรณีศึกษา

A สถานการณ์ A: ความปลอดภัยของเครือข่ายสาธารณะ

การดักจับแพ็กเก็ตและการเข้ารหัส | ความกังวลของซาราห์

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- ความเสี่ยง: การดักจับแพ็กเก็ต การสกัดกั้นข้อมูล และการโจมตีแบบ man-in-the-middle ผู้ที่อยู่ในเครือข่ายร้านกาแฟเดียวกันอาจดักจับรายละเอียดการล็อกอินหรือไฟล์การบ้านของเธอได้
- การป้องกันของ VPN: เข้ารหัสเพย์โหลดของแพ็กเก็ตเครือข่าย ทำให้ทราฟฟิกอุโมงค์ที่ถูกดักอ่านไม่ได้สำหรับผู้แอบดูในเครือข่ายท้องถิ่นแบบพาสซีฟ เมื่อตั้งค่า VPN อย่างถูกต้อง

B สถานการณ์ B: การเข้าถึงทรัพยากรที่ถูกบล็อก

การบล็อกตามภูมิศาสตร์และ IP | ปัญหาของอเล็กซ์

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- เหตุผลที่ถูกบล็อก: โฮสต์สตรีมมิงใช้การบล็อกตามภูมิศาสตร์ ซึ่งจับคู่ที่อยู่ IP ท้องถิ่นของผู้เดินทางกับประเทศจริงของเขาและบล็อกตามการอนุญาตให้ใช้สิทธิ์ตามอาณาเขต
- VPN ช่วยได้อย่างไร: ปกปิดตำแหน่งจริงของเขาโดยกำหนดเส้นทางทราฟฟิกผ่านเซิร์ฟเวอร์ในประเทศบ้านเกิดของเขา เว็บไซต์จะเห็น IP ของประเทศบ้านเกิด ทำให้เข้าถึงได้