ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

วิธีเลือก VPN ใบงาน

การประเมินผู้ให้บริการ VPN มาตรฐานความปลอดภัย การตรวจสอบ และนโยบายการบันทึก

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

- ประเมินเขตอำนาจศาลของผู้ให้บริการและนโยบายไม่เก็บบันทึกเพื่อความเป็นส่วนตัว
- เปรียบเทียบโปรโตคอลอุโมงค์อย่าง WireGuard และ OpenVPN ในด้านความเร็ว
- วิเคราะห์ฟีเจอร์ความปลอดภัย เช่น Kill Switch และโหนดเซิร์ฟเวอร์ที่ใช้ RAM เท่านั้น
- ระบุการตรวจสอบความปลอดภัยโดยหน่วยงานอิสระและแพ็กเกจราคาเมื่อทำการเลือก
- เลือกตำแหน่งเซิร์ฟเวอร์ตามความต้องการด้านความเร็วและการปลดบล็อกตามภูมิศาสตร์ของคุณ

คำชี้แจงใบงานการเลือก

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การเลือกโครงสร้างพื้นฐาน VPN ที่ปลอดภัย ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การเลือก VPN (บทนำ)

การเลือก VPN ที่เหมาะสมต้องมองให้พ้นคำโฆษณา ผู้ให้บริการที่เชื่อถือได้ต้องมีนโยบาย zero-logs ที่พิสูจน์แล้ว โปรโตคอลเข้ารหัสที่ปลอดภัย และไคลเอนต์โอเพนซอร์ส เมื่อประเมินฟีเจอร์ด้านความปลอดภัย เขตอำนาจศาล และประสิทธิภาพความเร็ว คุณจะเลือก VPN ที่ตรงกับความต้องการในการปกป้องดิจิทัลของคุณได้

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. ปัจจัยสำคัญในการเลือกผู้ให้บริการ VPN ที่ปลอดภัยคืออะไร?
   - A. จำนวนประเทศที่มีเซิร์ฟเวอร์
   - B. นโยบาย **no-logs** ที่ผ่านการตรวจสอบโดยหน่วยงานอิสระ
   - C. ระดับราคารายเดือนต่ำสุด
   - D. การสนับสนุนโฆษณาที่ฉูดฉาด

2. โปรโตคอล VPN ใดที่ให้ความสมดุลที่ดีที่สุดระหว่างความเร็วและความสามารถในการตรวจสอบ?
   - A. PPTP (รุ่นเก่า)
   - B. L2TP/IPSec
   - C. OpenVPN ผ่าน TCP เท่านั้น
   - D. WireGuard

3. เหตุใดผู้ใช้ควรหลีกเลี่ยง VPN ฟรีสำหรับกิจกรรมที่อ่อนไหว?
   - A. ถูกห้ามในสหรัฐอเมริกา
   - B. มักขายประวัติการท่องเว็บของคุณ
   - C. ไม่รองรับการท่องเว็บพื้นฐาน
   - D. ต้องใช้ฮาร์ดแวร์พิเศษในการเชื่อมต่อ

4. เขตอำนาจศาลของประเทศต้นสังกัดผู้ให้บริการเป็นตัวกำหนดอะไร?
   - A. ความเร็วของการเชื่อมต่อเซิร์ฟเวอร์
   - B. ประเภทของอุปกรณ์ที่รองรับ
   - C. กฎหมายท้องถิ่นว่าด้วยการเก็บรักษาข้อมูลและหมายค้น
   - D. ธีมภาพของแอปไคลเอนต์

5. วัตถุประสงค์หลักของฟีเจอร์ "kill switch" ของไคลเอนต์ VPN คืออะไร?
   - A. เพื่อบล็อกการเข้าถึงอินเทอร์เน็ตหากการเชื่อมต่อ VPN หลุด
   - B. เพื่อลบแอปพลิเคชันที่ติดตั้งทั้งหมดบนอุปกรณ์
   - C. เพื่อเพิ่มความเร็วของการเชื่อมต่อเซิร์ฟเวอร์เป็นสองเท่า
   - D. เพื่อรีสตาร์ตระบบปฏิบัติการเมื่อไม่มีการใช้งาน

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. VPN ปกป้องอุปกรณ์ของคุณจากการดาวน์โหลดมัลแวร์และไฟล์ไวรัส

○ จริง ○ เท็จ

7 คำถาม 7

7. การตรวจสอบอิสระจากบริษัทอย่าง Deloitte ยืนยันข้ออ้างเรื่องไม่เก็บบันทึก

○ จริง ○ เท็จ

8 คำถาม 8

8. กฎหมายของประเทศต้นทางของผู้ให้บริการไม่มีผลต่อความเป็นส่วนตัวของข้อมูลผู้ใช้

○ จริง ○ เท็จ

9 คำถาม 9

9. โค้ดที่กะทัดรัดของ WireGuard ตรวจสอบได้ง่ายกว่าของ OpenVPN

○ จริง ○ เท็จ

10 คำถาม 10

10. VPN ฟรีมักขายโฆษณาหรือติดตามผู้ใช้เพื่อชดเชยค่าเซิร์ฟเวอร์

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. นโยบาย _____ ที่ได้รับการตรวจสอบอย่างอิสระผูกมัดผู้ให้บริการ VPN ไม่ให้บันทึกประวัติออนไลน์ของคุณ

2. โปรโตคอล _____ สมัยใหม่ให้ความเร็วสูงและใช้โค้ดขนาดเล็กมาก

3. ฟีเจอร์ความปลอดภัยที่เรียกว่า _____ จะหยุดทราฟฟิกทั้งหมดหากการเชื่อมต่อ VPN ขัดข้องกะทันหัน

4. การประเมิน _____ ทางกฎหมายของผู้ให้บริการจะบอกว่าอยู่ภายใต้สนธิสัญญาการสอดแนมหรือไม่

5. การรักษาความปลอดภัยเซิร์ฟเวอร์ด้วยดิสก์แบบ _____ ช่วยไม่ให้ข้อมูลผู้ใช้คงอยู่หลังรีบูต

6. การพิสูจน์นโยบายที่อ้างว่าไม่รู้ข้อมูลต้องมี _____ ด้านความปลอดภัยจากบริษัทที่น่าเชื่อถือ

คลังคำศัพท์

การตรวจสอบ เขตอำนาจศาล คิลสวิตช์ ไม่เก็บล็อก แรมล้วน วีพีเอ็นฟรี ไวร์การ์ด โอเพนวีพีเอ็น

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องเครือข่าย

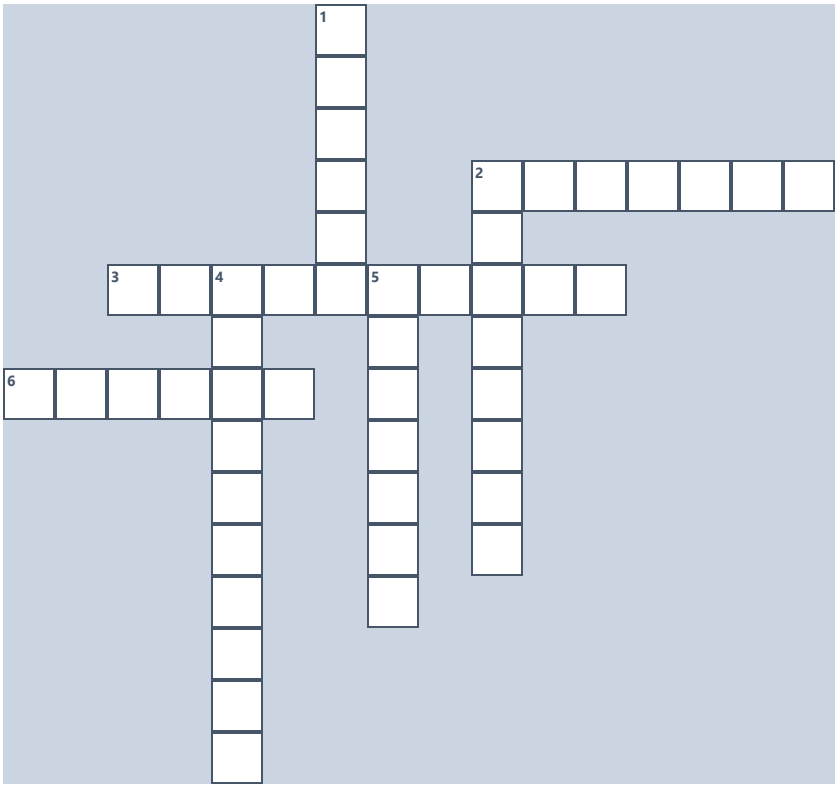
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. WireGuard**	**A**	บริการเชื่อมต่อความเสี่ยงสูงที่มักหารายได้จากการบันทึกและขายข้อมูลเบราว์เซอร์
☐	**2. บันทึกที่ผ่านการตรวจสอบ**	**B**	กลไกความปลอดภัยที่บล็อกการกำหนดเส้นทางอินเทอร์เน็ตหากอุโมงค์ที่ปลอดภัยตัดการเชื่อมต่อ
☐	**3. เขตอำนาจศาล**	**C**	พันธมิตรแบ่งปันข่าวกรองระหว่างประเทศระหว่างสหรัฐฯ สหราชอาณาจักร แคนาดา ออสเตรเลีย และนิวซีแลนด์
☐	**4. Kill Switch**	**D**	โครงสร้างพื้นฐานฮาร์ดแวร์ที่ทำงานบนหน่วยความจำชั่วคราว จึงไม่มีการเก็บข้อมูลลงดิสก์
☐	**5. Five Eyes**	**E**	ภูมิภาคทางภูมิศาสตร์ที่กำกับภาระผูกพันทางกฎหมายของผู้ให้บริการ VPN
☐	**6. VPN ฟรี**	**F**	โปรโตคอลสมัยใหม่ที่รวดเร็ว ใช้โค้ดประมาณ 4,000 บรรทัดที่ตรวจสอบได้ง่ายมาก
☐	**7. เซิร์ฟเวอร์ที่ใช้ RAM เท่านั้น**	**G**	โปรโตคอลโอเพนซอร์สที่เป็นที่ยอมรับและผ่านการตรวจสอบอย่างกว้างขวาง โดยมีโค้ดเบสใหญ่กว่า WireGuard มาก
☐	**8. OpenVPN**	**H**	คำกล่าวอ้างด้านความเป็นส่วนตัวที่ได้รับการยืนยันโดยบริษัทความปลอดภัยไซเบอร์บุคคลที่สามอิสระ

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. โปรโตคอลทันสมัยและรวดเร็วที่ใช้โค้ดประมาณ 4,000 บรรทัดซึ่งตรวจสอบได้ง่ายมาก (7)

3. โปรโตคอลโอเพนซอร์สที่ผ่านการตรวจสอบอย่างกว้างขวางและเติบโตเต็มที่ โดยมีโค้ดใหญ่กว่า WireGuard มาก (10)

6. กลไกความปลอดภัยที่บล็อกการส่งต่ออินเทอร์เน็ตหากอุโมงค์ที่ปลอดภัยขาดการเชื่อมต่อ (6)

แนวตั้ง

1. โครงสร้างพื้นฐานฮาร์ดแวร์ที่ทำงานบนหน่วยความจำชั่วคราวทั้งหมด จึงไม่มีการเก็บข้อมูล (6)

2. คำยืนยันด้านความเป็นส่วนตัวที่ได้รับการตรวจสอบโดยบริษัทความปลอดภัยไซเบอร์บุคคลที่สามอิสระ (8)

4. ภูมิภาคทางภูมิศาสตร์ที่กำกับภาระผูกพันทางกฎหมายของผู้ให้บริการ VPN (10)

5. บริการเชื่อมต่อที่มีความเสี่ยงสูง มักหารายได้โดยบันทึกและขายข้อมูลการท่องเว็บ (7)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: โปรโตคอลทันสมัยและรวดเร็วที่ใช้โค้ดประมาณ 4,000 บรรทัดซึ่งตรวจสอบได้ง่ายมาก (7 ตัวอักษร):

3 แนวนอน: โปรโตคอลโอเพนซอร์สที่ผ่านการตรวจสอบอย่างกว้างขวางและเติบโตเต็มที่ โดยมีโค้ดใหญ่กว่า WireGuard มาก (10 ตัวอักษร):

6 แนวนอน: กลไกความปลอดภัยที่บล็อกการส่งต่ออินเทอร์เน็ตหากอุโมงค์ที่ปลอดภัยขาดการเชื่อมต่อ (6 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: โครงสร้างพื้นฐานฮาร์ดแวร์ที่ทำงานบนหน่วยความจำชั่วคราวทั้งหมด จึงไม่มีการเก็บข้อมูล (6 ตัวอักษร):

2 แนวตั้ง: คำยืนยันด้านความเป็นส่วนตัวที่ได้รับการตรวจสอบโดยบริษัทความปลอดภัยไซเบอร์บุคคลที่สามอิสระ (8 ตัวอักษร):

4 แนวตั้ง: ภูมิภาคทางภูมิศาสตร์ที่กำกับภาระผูกพันทางกฎหมายของผู้ให้บริการ VPN (10 ตัวอักษร):

5 แนวตั้ง: บริการเชื่อมต่อที่มีความเสี่ยงสูง มักหารายได้โดยบันทึกและขายข้อมูลการท่องเว็บ (7 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ร ต น อ า นี า วี ส์ น นี ส ช มี ฟ
บ า ว า ห นี า พี ย ม คิ กี จ า า
น รี ล้ ต ว ย ง เ า ก ล ค จ น ตี
อ็ ว ม ร ตี ว า อ็ อ ล ส ล ด า อ
เ ย ร ช ฟ เ ก น ฟ์ ก วิ ล ม ไ า
พี ป แ อ อ ข ม ฟ ฟ มี ต า ล ม่ ล
วี ป จ า นี ต กี รี ไ พ ช์ ร ง เ า
น ช า า ลี อำ จ ดี ว า น ล ผ ก็ ดี
พ ช ก ด า น ต า ร์ จ า ค ก บ ดี
เ า ช ว ก า ด กี ก ด ท ผ ฟ ล็ ช
อ มี ม อ ต จ ฟ ร า ดี า ท า อ ส
โ ท ข ข า ศ น ก ร์ า ล า ม ก ร
มี า ร ช ก า ด ง ด น ร ต สี ย ข
มี ดี ด ด ว ล บ ฟ อ า ร ห ห รี น
ผ นี ม ผ ดี ข กี ส บ ลี ง ด ร ด ค

รายการคำศัพท์

ไวร์การ์ด ไม่เก็บล็อก เขตอำนาจศาล คิลสวิตช์ ไฟฟ้าอายส์ วีพีเอ็นฟรี แรมล้วน โอเพนวีพีเอ็น

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. ไวร์การ์ด

B. ไม่เก็บล็อก

C. เขตอำนาจศาล

D. คิลสวิตช์

E. ไฟฟ์อายส์

F. วีพีเอ็นฟรี

G. แรมล้วน

H. โอเพนวีพีเอ็น

คำนิยามและช่องจับคู่

1. พันธมิตรแบ่งปันข่าวกรองระหว่างประเทศของสหรัฐฯ สหราชอาณาจักร แคนาดา ออสเตรเลีย และนิวซีแลนด์

2. โปรโตคอลทันสมัยและรวดเร็วที่ใช้โค้ดประมาณ 4,000 บรรทัดซึ่งตรวจสอบได้ง่ายมาก

3. โปรโตคอลโอเพนซอร์สที่ผ่านการตรวจสอบอย่างกว้างขวางและเติบโตเต็มที่ โดยมีโค้ดใหญ่กว่า WireGuard มาก

4. บริการเชื่อมต่อที่มีความเสี่ยงสูง มักหารายได้โดยบันทึกและขายข้อมูลการท่องเว็บ

5. กลไกความปลอดภัยที่บล็อกการส่งต่ออินเทอร์เน็ตหากอุโมงค์ที่ปลอดภัยขาดการเชื่อมต่อ

6. โครงสร้างพื้นฐานฮาร์ดแวร์ที่ทำงานบนหน่วยความจำชั่วคราวทั้งหมด จึงไม่มีการเก็บข้อมูล

7. ภูมิภาคทางภูมิศาสตร์ที่กำกับภาระผูกพันทางกฎหมายของผู้ให้บริการ VPN

8. คำยืนยันด้านความเป็นส่วนตัวที่ได้รับการตรวจสอบโดยบริษัทความปลอดภัยไซเบอร์บุคคลที่สามอิสระ

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของ VPN เขียนคำตอบของคุณในช่องกรอกที่กรอกได้

1. ก ร์ ไ า ด ร์ ว
2. า อำ เ ข น ล จ ศ า ต
3. อ ไ า ส์ ฟ ี ย ฟ
4. น ล้ ม ว แ ร
5. บ ล็ ม ก ก็ ไ อ เ
6. ต ว ิ ค ิ ส ช์ ล
7. ว ี ฟ น ร ี พ ี อ็ เ
8. อ็ พ ว ี น โ น อ พ ี เ เ

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	สิ่งที่ VPN ซ่อนได้			
2	สิ่งที่สำคัญกว่าราคา			
3	สถานที่ที่อ่านรีวิว VPN ได้			
4	สิ่งที่ VPN ปกป้องคุณไม่ได้			
5	คำถามสำหรับทีมขายของ VPN			
6	สิ่งที่ผู้ให้บริการอินเทอร์เน็ตของคุณมองเห็นได้			
7	รายการในเซ็กลิสต์ของคุณเมื่อเลือก VPN			
8	สถานที่ที่คุณจะใช้ VPN			
9	สัญญาณเตือนในผู้ให้บริการ VPN			
10	คำที่เกี่ยวข้องกับความเป็นส่วนตัว			
11	สิ่งที่คุณจะทดสอบก่อน			
12	คำมั่นสัญญาที่ผู้ให้บริการ VPN ที่ดีให้ไว้			
13	เหตุผลที่ควรใช้ VPN ขณะเดินทาง			
14	อุปกรณ์ที่ใช้ VPN ได้			
15	ความเชื่อผิด ๆ เกี่ยวกับ VPN			

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

เพื่อให้การฝึกอบรมคู่มือการเลือกของคุณเสร็จสมบูรณ์ ให้ถอดรหัสข้อความที่ซ่อนอยู่นี้เกี่ยวกับการเลือกโครงสร้างพื้นฐานที่ปลอดภัย

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

57	27	35	52	34	26	57	23	52	34	26		35	49	34	7	49	25
20	64	39	34		35	47	26	26		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: ทำไมฉันควรใช้ VPN?

VPN ปกป้องความเป็นส่วนตัวทางดิจิทัลของคุณ รักษาความปลอดภัยของการเชื่อมต่อบนเครือข่าย Wi-Fi สาธารณะ (เช่น ร้านกาแฟหรือสนามบิน) อาจลดการหน่วงความเร็วตามกิจกรรมเมื่อ ISP ระบุประเภทของทราฟฟิกที่เข้ารหัสไม่ได้ ข้ามข้อจำกัดทางภูมิศาสตร์เพื่อเข้าถึงเนื้อหาทั่วโลก และช่วยรักษาความปลอดภัยของทรัพยากรการทำงานระยะไกล

Q3: VPN ทำให้ฉันไม่เปิดเผยตัวตนบนออนไลน์โดยสมบูรณ์หรือไม่?

ไม่ แม้ VPN จะซ่อนที่อยู่ IP ของคุณและเข้ารหัสการรับส่งข้อมูล แต่คุณก็ยังถูกติดตามได้ผ่านคุกกี้ของเบราว์เซอร์ บัญชีที่ล็อกอินอยู่ (เช่น Google หรือ Facebook) การพิมพ์ลายนิ้วมือเบราว์เซอร์ หรือหากผู้ให้บริการ VPN ของคุณบันทึกข้อมูลของคุณ

Q4: VPN จะทำให้ความเร็วอินเทอร์เน็ตของฉันช้าลงหรือไม่?

ได้ เล็กน้อย กระบวนการเข้ารหัสและระยะทางกายภาพไปยังเซิร์ฟเวอร์ VPN เพิ่มความหน่วงและภาระงาน ผลกระทบแตกต่างกันตามผู้ให้บริการ โปรโตคอล ระยะทางเซิร์ฟเวอร์ อุปกรณ์ และสภาพเครือข่าย

Q5: สร้างรายได้อย่างไร?

ตรวจสอบรูปแบบธุรกิจ การสมัครสมาชิก แพ็กเกจฟรีเมียม และการขายข้อมูลล้วนส่งผลต่อระดับความน่าเชื่อถือของ VPN และบริการที่ไม่เคยเก็บข้อมูลของคุณก็ไม่สามารถขายข้อมูลนั้นได้ อ่านนโยบายความเป็นส่วนตัวก่อน [1]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดที่ผู้สนใจมีเกี่ยวกับการใช้เครือข่ายส่วนตัวเสมือน

Q6: ฉันใช้ VPN ฟรีได้หรือไม่?

VPN ฟรีอาจพึ่งพาโฆษณา ฟีเจอร์ที่จำกัด การวิเคราะห์การใช้งาน โควตาข้อมูล หรือโมเดลหารายได้อื่น ผู้ใช้ควรตรวจสอบนโยบายความเป็นส่วนตัว ความเป็นเจ้าของ การตรวจสอบ และโมเดลธุรกิจของผู้ให้บริการก่อนใช้งาน

Q7: นโยบาย "no-logs" คืออะไร?

นโยบายไม่เก็บบันทึกอธิบายว่าผู้ให้บริการระบุว่าไม่เก็บกิจกรรมและข้อมูลการเชื่อมต่อใดบ้าง ขอบเขตที่แน่นอนแตกต่างกันไป ผู้อ่านจึงควรตรวจสอบนโยบายและผลการตรวจสอบอิสระ

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: การกำหนดเส้นทางแบบ double VPN หรือ Multi-Hop คืออะไร?

Multi-Hop ส่งการรับส่งข้อมูลของคุณผ่านเซิร์ฟเวอร์ VPN สองเครื่องขึ้นไปตามลำดับ ซึ่งเพิ่มการเข้ารหัสชั้นที่สองและช่วยซ่อนที่อยู่ IP จริงของคุณจากฮอปที่สองหากเซิร์ฟเวอร์ใดเครื่องหนึ่งถูกบุกรุก

Q3: การรั่วไหลของ WebRTC คืออะไร และ VPN ป้องกันได้อย่างไร?

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

Q4: เซิร์ฟเวอร์แบบ RAM-only คืออะไร และเหตุใดจึงสำคัญ?

เซิร์ฟเวอร์แบบดั้งเดิมเขียนข้อมูลลงฮาร์ดไดรฟ์ ซึ่งอาจถูกยึดหรือถูกเจาะได้ เซิร์ฟเวอร์ที่ใช้ RAM เท่านั้น (ไร้ดิสก์) ทำงานทั้งหมดในหน่วยความจำชั่วคราว (RAM) เมื่อรีบูตหรือปิดเครื่อง ข้อมูลในหน่วยความจำจะถูกล้าง

Q5: การพรางทราฟฟิก (Obfuscation) หลบเลี่ยงการบล็อก VPN ได้อย่างไร?

การอำพราง (หรือ "Stealth VPN") ทำให้แพ็กเก็ตทราฟฟิก VPN ดูเหมือนทราฟฟิกเว็บ HTTPS ปกติ (พอร์ต 443) ช่วยให้ผ่านการตรวจสอบแพ็กเก็ตเชิงลึก (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: Forward Secrecy (Perfect Forward Secrecy) ทำงานอย่างไร?

PFS ทำให้มีการสร้างกุญแจเข้ารหัสชั่วคราวที่ไม่ซ้ำกันสำหรับทุกเซสชัน แม้กุญแจส่วนตัวจะถูกบุกรุกในอนาคต ก็ไม่สามารถใช้ถอดรหัสเซสชันในอดีตหรืออนาคตได้ เพราะแต่ละเซสชันใช้กุญแจที่เป็นอิสระต่อกัน

Q8: พันธมิตร 5/9/14 Eyes คืออะไร และเหตุใดฉันจึงควรใส่ใจ?

เขตอำนาจศาลอาจส่งผลต่อกระบวนการทางกฎหมายที่ผู้ให้บริการอาจเผชิญ แต่ความเสี่ยงด้านความเป็นส่วนตัวในทางปฏิบัติยังขึ้นอยู่กับข้อมูลที่ผู้ให้บริการเก็บรักษา สถาปัตยกรรมทางเทคนิค ความเป็นเจ้าของ การรายงานความโปร่งใส และประวัติการตรวจสอบด้วย

Q9: การป้องกัน DNS Leak คืออะไร?

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

Q10: ทำไมต้องตรวจสอบว่าใครดำเนินงานและรับรอง VPN?

ชื่อเสียงสำคัญ ศึกษาข้อมูลเจ้าของและผู้นำของบริษัท ดูผลการตรวจสอบสาธารณะจากบุคคลที่สาม และตรวจสอบว่าผู้เชี่ยวชาญด้านความปลอดภัยอิสระและสื่อกล่าวถึงอย่างไรก่อนไว้วางใจ [1]

ส่วนที่ 11: ข้อเท็จจริงน่าสนใจเกี่ยวกับ VPN 10 ข้อและข้อมูลเชิงลึกในโลกจริง

ทบทวนข้อเท็จจริงและข้อมูลเชิงลึกในโลกจริงที่มีคุณค่าสูงเกี่ยวกับประวัติ ตลาด และเทคโนโลยีของ VPN

1. โปรโตคอล VPN แรก

PPTP (Point-to-Point Tunneling Protocol) โปรโตคอล VPN ยุคแรกจากกลุ่มที่นำโดย Microsoft ในทศวรรษ 1990 ปัจจุบันถือว่าไม่ปลอดภัย VPN สมัยใหม่จึงใช้ WireGuard หรือ OpenVPN [1]

2. การประเมินมูลค่าตลาด

ตลาด VPN ทั่วโลกเติบโตอย่างรวดเร็ว โดยมีแรงขับเคลื่อนจากความต้องการทำงานทางไกลที่เพิ่มขึ้นและความต้องการด้านความปลอดภัยขององค์กร

3. การปฏิวัติ WireGuard

WireGuard มีโค้ดที่เรียบง่ายมากซึ่งออกแบบมาเพื่อประสิทธิภาพ ทำให้ตรวจสอบช่องโหว่ด้านความปลอดภัยได้ง่ายกว่าโปรโตคอลแบบดั้งเดิม [3]

4. มาตรฐานการตรวจสอบที่เข้มงวด

ผู้ให้บริการ VPN ชั้นนำจ้างบริษัทอย่าง Deloitte, KPMG หรือ PwC ตรวจสอบข้ออ้างเรื่องไม่เก็บบันทึก และจ้างบริษัทความปลอดภัยอย่าง Cure53 ทดสอบแอปและเซิร์ฟเวอร์ของตน [4]

5. จุดกำเนิดของพันธมิตร 5-Eyes

ความร่วมมือด้านข่าวกรอง Five Eyes ของสหรัฐฯ สหราชอาณาจักร แคนาดา ออสเตรเลีย และนิวซีแลนด์ เติบโตมาจากความร่วมมือด้านข่าวกรองสัญญาณระหว่างฝ่ายสัมพันธมิตรในยุคสงครามโลกครั้งที่สอง

6. การตรวจสอบแพ็กเก็ตเชิงลึก

ไฟร์วอลล์ขั้นสูงใช้ Deep Packet Inspection (DPI) เพื่อวิเคราะห์เมทาดาทาของแพ็กเก็ตเครือข่ายและบล็อกลักษณะการเชื่อมต่อ VPN มาตรฐาน

7. การใช้งานในองค์กร

หลายองค์กรให้พนักงานระยะไกลใช้ VPN เพื่อเข้าถึงระบบภายใน เช่น ฐานข้อมูล ทำให้ VPN เป็นเครื่องมือรักษาความปลอดภัยที่พบบ่อยในที่ทำงาน

8. VPN แบบกระจายศูนย์

VPN แบบกระจายศูนย์ (dVPN) กระจายทราฟฟิกไปทั่วเครือข่ายโหนดที่ผู้ใช้ดูแลเอง ช่วยลดการพึ่งพาผู้ให้บริการส่วนกลางรายเดียว

9. ความเป็นนิรนามของ TOR เทียบกับ VPN

VPN ส่งทราฟฟิกผ่านผู้ให้บริการรายเดียว ส่วน Tor (The Onion Router) ส่งทราฟฟิกผ่านรีเลย์อาสาสมัครสามตัว (guard, middle, exit) เพื่อเพิ่มความเป็นส่วนตัวสูงสุด [5]

10. ต้นทุนของการละเมิดข้อมูล

การใช้ VPN ร่วมกับโมเดลการเข้าถึงแบบ Zero Trust ซึ่งตรวจสอบผู้ใช้และอุปกรณ์ทุกราย ช่วยให้องค์กรปกป้องข้อมูลและจำกัดความเสียหายจากการละเมิดข้อมูลได้

แหล่งอ้างอิงทางเทคนิค

สิ่งพิมพ์ที่อ้างอิง ข้อกำหนดด้านการเข้ารหัส และมาตรฐานเอกสารทางการที่ใช้ตลอดทั้งใบงานนี้

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

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

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

เฉลย: การประเมินผู้ให้บริการ VPN มาตรฐานความปลอดภัย การตรวจสอบ และนโยบายการบันทึกข้อมูล

1 **นโยบายล็อกที่ผ่านการตรวจสอบ** โปรโตคอล — **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

นโยบายไม่เก็บบันทึกที่ผ่านการตรวจสอบอิสระเป็นวิธีที่ใช้ได้จริงที่สุดในการตรวจสอบคำกล่าวอ้างเรื่องความเป็นส่วนตัวแบบ Zero-knowledge ของผู้ให้บริการ การตลาดที่ฉูดฉาดหรือการกล่าวอ้างเองไม่เพียงพอ อ้างอิง: Deloitte Advisory, Cure53 Audit.

2 **ความเหนือกว่าของ WireGuard** เวลาแฝง — **คำตอบที่ถูกต้อง: D**

หมายเหตุสำหรับผู้สอน

WireGuard ให้การกำหนดเส้นทางการเชื่อมต่อที่ทันสมัยและรวดเร็วในพื้นที่เคอร์เนลด้วยโค้ดที่กะทัดรัด (ประมาณ 4,000 บรรทัด) ทำให้การตรวจสอบมีประสิทธิภาพสูง การอ้างอิง: IETF Protocol RFC, WireGuard Project.

3 **คำถาม 3** — **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

VPN ฟรียังต้องจ่ายค่าเซิร์ฟเวอร์ และ FTC เตือนว่าแอป VPN บางตัวแบ่งปันข้อมูลผู้ใช้กับบุคคลที่สาม เช่น เพื่อแสดงโฆษณา

4 **เขตอำนาจศาลทางกฎหมาย** การควบคุมการกำหนดเส้นทาง — **คำตอบที่ถูกต้อง: C**

หมายเหตุสำหรับผู้สอน

เขตอำนาจศาลเป็นตัวกำหนดว่า VPN อยู่ภายใต้กฎหมายสอดแนม ข้อบังคับการเก็บข้อมูลในพื้นที่ และหมายเรียกลับของรัฐบาลหรือไม่ การอ้างอิง: Privacy Rights Clearinghouse.

5 **การป้องกันด้วย Kill Switch** ความเป็นส่วนตัว — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

Kill Switch ตัดการกำหนดเส้นทางของอะแดปเตอร์เครือข่ายระบบทันทีหากอุโมงค์หลุด ป้องกัน IP จริงและ DNS รั่วไหล อ้างอิง: IETF Tunnel RFC.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **ข้อจำกัดของมัลแวร์** การปกปิด IP — คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

VPN ให้ท่อส่งข้อมูลที่เข้ารหัสอย่างปลอดภัย แต่ไม่ได้สแกนเพย์โหลดหรือไฟล์ จึงต้องใช้ซอฟต์แวร์แอนติไวรัสเพื่อบล็อกมัลแวร์ อ้างอิง: Deloitte Advisory.

7 **การตรวจสอบโดยหน่วยงานอิสระ** ความเร็ว — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

รายงานการตรวจสอบยืนยันการกำหนดค่าซอฟต์แวร์เซิร์ฟเวอร์ การปฏิบัติตามการตั้งค่า RAM เท่านั้น และการไม่มีฐานข้อมูลบันทึกล็อก อ้างอิง: Deloitte Advisory, Cure53 Audit.

8 **คำถาม 8** — คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

ผู้ให้บริการต้องปฏิบัติตามกฎหมายของประเทศที่ตนตั้งอยู่ ซึ่งอาจรวมถึงกฎการเก็บรักษาข้อมูลและคำสั่งให้ส่งมอบข้อมูลที่ตนถือครอง

9 **ขนาดโค้ดเบสของโปรโตคอล** ไฟร์วอลล์ — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

โค้ดเบสที่เล็กกว่าช่วยลดพื้นที่การโจมตีที่เป็นไปได้ และทำให้ทีมความปลอดภัยตรวจสอบความสมบูรณ์ของโปรโตคอลได้ง่ายขึ้น อ้างอิง: WireGuard Project.

10 **การหารายได้จากโฆษณา** ไม่เก็บล็อก — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

เมื่อไม่มีค่าสมัครสมาชิก VPN ฟรีจึงพึ่งพาการขุดข้อมูล การทำโปรไฟล์ทราฟฟิก และการแทรกโฆษณาในเบราว์เซอร์เพื่อสร้างรายได้ การอ้างอิง: EDRi Retention Guidelines.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

F 1. WireGuard	H 2. บันทึกที่ผ่านการตรวจสอบ	E 3. เขตอำนาจศาล	B 4. Kill Switch
C 5. Five Eyes	A 6. VPN ฟรี	D 7. เซิร์ฟเวอร์ที่ใช้ RAM เท่านั้น	G 8. OpenVPN

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ไม่เก็บล็อก	2 ไวร์การ์ด	3 คิลสวิตช์	4 เขตอำนาจศาล
5 แรมล้วน	6 การตรวจสอบ		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 E – ไฟฟ้อายส์	2 A – ไวร์การ์ด	3 H – โอเพนวีพีเอ็น	4 F – วีพีเอ็นฟรี
5 D – คิลสวิตช์	6 G – แรมล้วน	7 C – เขตอำนาจศาล	8 B – ไม่เก็บล็อก

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย WireGuard บันทึกที่ผ่านการตรวจสอบ และ เขตอำนาจศาล ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

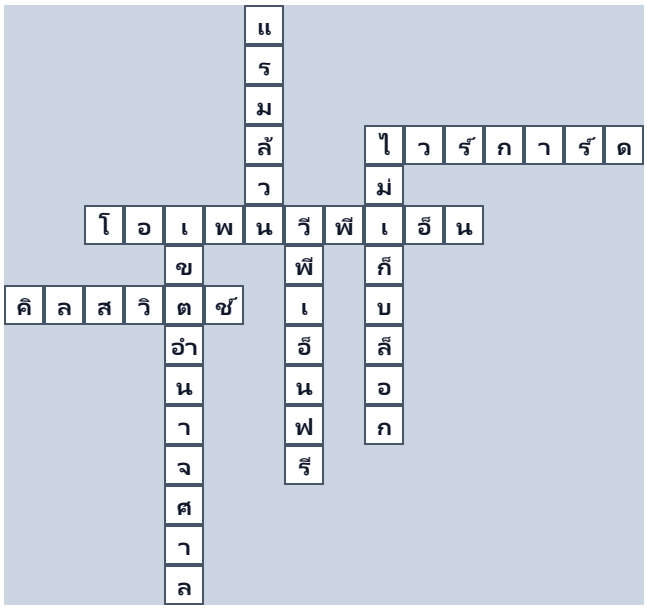
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ร	ต	น	อ	า	นี	า	วี	ส์	น	นี	ส	ช	มี	ฟ
บ	า	ว	า	ห	นี	า	พี	ย	ม	คิ	กี	จ	า	า
น	รี	ล้	ต	ว	ย	ง	เ	า	ก	ล	ค	จ	น	ดี
อิ	ว	ม	ร	ตี	ว	า	อิ	อ	ล	ส	ล	ด	า	อ
เ	ย	ร	ช	ฟ	เ	ก	น	ฟ	ก	วิ	ล	ม	ไ	า
พี	ป	แ	อ	อ	ข	ม	ฟ	ฟ	มี	ต	า	ล	ม่	ล
วี	ป	จ	า	นี	ต	กี	รี	ไ	พ	ช์	ร	ง	เ	า
น	ช	า	า	ลี	อำ	จ	ดี	ว	า	น	ล	ผ	ก็	ดี
พ	ช	ก	ด	า	น	ต	า	ร์	จ	า	ค	ก	บ	ดี
เ	า	ช	ว	ก	า	ด	กี	ก	ด	ท	ผ	ฟ	ล็	ช
อ	มี	ม	อ	ต	จ	ฟ	ร	า	ดี	า	ท	า	อ	ส
โ	ท	ข	ข	า	ศ	น	ก	ร์	า	ล	า	ม	ก	ร
มี	า	ร	ช	ก	า	ด	ง	ด	น	ร	ต	สี	ย	ข
มี	ดี	ต	ด	ว	ล	บ	ฟ	อ	า	ร	ห	ห	รี	น
ผ	นี	ม	ผ	ดี	ข	กี	ส	บ	ลี	ง	ด	ร	ด	ค

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: ไวร์การ์ด โปรโตคอลทันสมัยและรวดเร็วที่ใช้โค้ดประมาณ 4,000 บรรทัดซึ่งตรวจสอบได้ง่ายมาก (7 ตัวอักษร)

3 แนวนอน: โอเพนวีพีเอ็น โปรโตคอลโอเพนซอร์สที่ผ่านการตรวจสอบอย่างกว้างขวางและเติบโตเต็มที่ โดยมีโค้ดใหญ่กว่า WireGuard มาก (10 ตัวอักษร)

6 แนวนอน: คิลสวิตช์ กลไกความปลอดภัยที่บล็อกการส่งต่ออินเทอร์เน็ตหากอุโมงค์ที่ปลอดภัยขาดการเชื่อมต่อ (6 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: แรมล้วน โครงสร้างพื้นฐานฮาร์ดแวร์ที่ทำงานบนหน่วยความจำชั่วคราวทั้งหมด จึงไม่มีการเก็บข้อมูล (6 ตัวอักษร)

2 แนวตั้ง: ไม่เก็บล็อก คำยืนยันด้านความเป็นส่วนตัวที่ได้รับการตรวจสอบโดยบริษัทความปลอดภัยไซเบอร์บุคคลที่สามอิสระ (8 ตัวอักษร)

4 แนวตั้ง: เขตอำนาจศาล ภูมิภาคทางภูมิศาสตร์ที่กำกับภาระผูกพันทางกฎหมายของผู้ให้บริการ VPN (10 ตัวอักษร)

5 แนวตั้ง: วีพีเอ็นฟรี บริการเชื่อมต่อที่มีความเสี่ยงสูง มักหารายได้โดยบันทึกและขายข้อมูลการท่องเว็บ (7 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. กร์ไดร์ว → ไวร์การ์ด
2. าอำเขนลจศาต → เขตอำนาจศาล
3. อไาส์ฟียฟ → ไฟฟ์อายส์
4. นล้มวแร → แรมล้วน
5. บล็มกก์ไอเ → ไม่เก็บล็อก
6. ตวิคิสช์ล → คิลสวิตช์
7. วีฟนรีพีอีเ → วีพีเอ็นฟรี
8. อ็พวีนโนอพีแ → โอเพนวีพีเอ็น

เฉลยภารกิจรหัสลับ

"เปรียบเทียบ รายงาน ด้วย ระบบ 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