ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

VPN คืออะไร ใบงาน

แบบฝึกหัดภาคปฏิบัติเกี่ยวกับโปรโตคอลเครือข่าย อุโมงค์ และการควบคุมความปลอดภัย

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

- อธิบายแนวคิดของการสร้างอุโมงค์ข้อมูลและการห่อหุ้ม
- ระบุการกำหนดค่าโปรโตคอลมาตรฐานและวิธีการเข้ารหัส
- วิเคราะห์บทบาทของเซิร์ฟเวอร์และการปกปิด IP ใน Virtual Private Network
- ทำความเข้าใจว่า ISP ติดตามการท่องเว็บอย่างไร และ VPN ป้องกันได้อย่างไร
- จำแนกขอบเขตการดำเนินงานของโทโพโลยีเครือข่ายเสมือน

คำแนะนำคู่มือ VPN คืออะไร

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ สถานการณ์ในโลกจริงในส่วนกรณีศึกษา ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

VPN คืออะไร (บทนำ)

Virtual Private Network ไม่ใช่แค่สวิตช์เปิดปิดความเป็นส่วนตัว แต่เป็นอุโมงค์เข้ารหัสที่ส่งทราฟฟิกอินเทอร์เน็ตของคุณผ่านเซิร์ฟเวอร์ระยะไกล ซึ่งซ่อนที่อยู่ IP ของคุณ ป้องกันไม่ให้ ISP รวบรวมบันทึกการกระทำออนไลน์ของคุณ และปกป้องข้อมูลของคุณบนเครือข่ายสาธารณะ การเข้าใจศัพท์เฉพาะเป็นสิ่งจำเป็นต่อการรักษาความปลอดภัยทางดิจิทัล

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. หน้าที่หลักของเครือข่ายส่วนตัวเสมือน (VPN) คืออะไร?
   - A. เพื่อเพิ่มความเร็วการเรนเดอร์ของเว็บเบราว์เซอร์
   - B. เพื่อเข้ารหัสแพ็กเก็ตข้อมูลและซ่อน IP สาธารณะของคุณ
   - C. เพื่อจัดเก็บฐานข้อมูลคุกกี้ของเว็บไซต์ในเครื่อง
   - D. เพื่อแทนที่ฮาร์ดแวร์คอมพิวเตอร์จริงของคุณ

2. การทำอุโมงค์เครือข่ายในบริบทของ VPN คืออะไร?
   - A. การลบไฟล์บันทึกเครือข่ายที่ซ้ำกัน
   - B. การติดตั้งไฟล์จัดเก็บฐานข้อมูลในเครื่อง
   - C. แชร์ไฟล์กับคอมพิวเตอร์เครื่องอื่นในเครือข่ายภายใน
   - D. การห่อหุ้มแพ็กเก็ตเครือข่ายหนึ่งไว้ภายในอีกแพ็กเก็ตที่ปลอดภัย

3. มาตรฐานการเข้ารหัสใดที่ใช้กันอย่างแพร่หลายเพื่อปกป้องทราฟฟิก VPN?
   - A. การเข้ารหัส DES รุ่นเก่า
   - B. มาตรฐาน AES-256 สมัยใหม่
   - C. การเข้ารหัส base64 แบบข้อความธรรมดา
   - D. การเข้ารหัสแบบ rot13 มาตรฐาน

4. ส่วนใดของทราฟฟิกเครือข่ายของคุณที่ถูกเข้ารหัสโดย VPN?
   - A. เฉพาะงานพิมพ์ในเครือข่ายของอุปกรณ์ภายในเครื่อง
   - B. เส้นทางของสายอีเทอร์เน็ตทางกายภาพ
   - C. ส่วนเพย์โหลดข้อมูลทั้งหมดของแพ็กเก็ตเครือข่าย
   - D. เฉพาะประวัติการค้นหาของเว็บเบราว์เซอร์ของคุณ

5. คำว่า "การเข้ารหัส" หมายถึงอะไรในเครือข่าย?
   - A. การแปลงข้อมูลข้อความธรรมดาเป็นข้อความเข้ารหัสที่อ่านไม่ได้
   - B. การลบบันทึกการสื่อสารเก่า
   - C. เพิ่มขีดจำกัดความเร็วแบนด์วิดท์ในเครื่องของคุณ
   - D. การแชร์กุญแจเข้าถึงฐานข้อมูลต่อสาธารณะ

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. VPN เข้ารหัสทราฟฟิกของคุณเพื่อป้องกันการแอบดักข้อมูลบน Wi-Fi สาธารณะ

○ จริง ○ เท็จ

7 คำถาม 7

7. VPN เปลี่ยนแปลงการกำหนดค่าฮาร์ดแวร์ของเราเตอร์ของคุณทางกายภาพ

○ จริง ○ เท็จ

8 คำถาม 8

8. โปรโตคอลอุโมงค์ห่อแพ็กเก็ตข้อมูลไว้ในเลเยอร์การขนส่งที่เข้ารหัส

○ จริง ○ เท็จ

9 คำถาม 9

9. การเข้ารหัสแบบสมมาตรใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัสทราฟฟิก

○ จริง ○ เท็จ

10 คำถาม 10

10. การใช้ VPN ทำให้การเชื่อมต่ออินเทอร์เน็ตของคุณไม่ได้รับผลกระทบทางกายภาพจากไฟดับออฟไลน์

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. เพื่อรักษาความปลอดภัยทราฟฟิก VPN ห่อแพ็กเก็ตข้อมูลของคุณไว้ในอีกโปรโตคอลหนึ่ง ซึ่งเรียกว่า _____
2. หากความเร็วดาวน์โหลดช้าขณะสตรีม อาจเกิดจาก _____ เครือข่ายที่จำกัด
3. บริการสตรีมที่ใช้ได้เฉพาะบางประเทศใช้ _____ เพื่อจำกัดผู้ใช้ทั่วโลก
4. กฎการเชื่อมต่อที่กำหนดพารามิเตอร์การเข้ารหัสและการเชื่อมต่อเรียกว่า _____ ของ VPN
5. คอมพิวเตอร์ของคุณใช้ _____ ในเครื่องเฝ้าดูทราฟฟิกเครือข่ายและบล็อกการเชื่อมต่อที่ไม่ปลอดภัย
6. เมื่อเชื่อมต่อ VPN ข้อมูลของคุณถูกส่งผ่าน _____ ระยะไกลเพื่อซ่อนไอพีสาธารณะ

คลังคำศัพท์

ความเป็นส่วนตัว จีโอบล็อก เซิร์ฟเวอร์ แบนด์วิดท์ โปรโตคอล ไฟร์วอลล์ อุโมงค์ ไอเอสพี

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องเครือข่าย

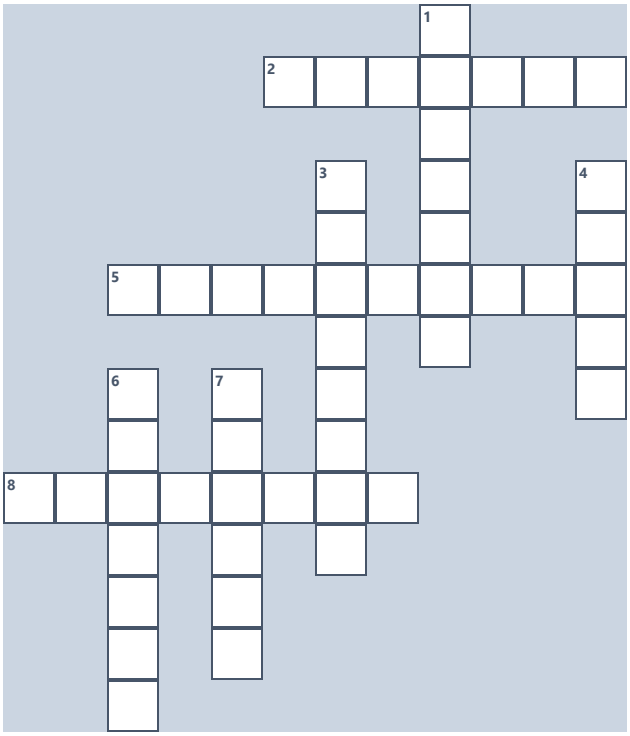
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. การทำอุโมงค์**	**A**	คอมพิวเตอร์ระยะไกลที่ส่งทราฟฟิกของคุณและปกปิด IP ของคุณ
☐	**2. โปรโตคอล**	**B**	ผู้ให้บริการอินเทอร์เน็ตที่ส่งผ่านทราฟฟิกของคุณและสามารถเห็นกิจกรรมที่ไม่เข้ารหัส
☐	**3. แบนด์วิดท์**	**C**	ข้อจำกัดที่ป้องกันการเข้าถึงเว็บตามตำแหน่งที่ตั้งทางกายภาพ
☐	**4. เซิร์ฟเวอร์**	**D**	ระบบรักษาความปลอดภัยที่ตรวจสอบและบล็อกทราฟฟิกที่ไม่ได้รับอนุญาต
☐	**5. การบล็อกตามภูมิศาสตร์**	**E**	ชุดกฎที่กำหนดวิธีส่งข้อมูลผ่านเครือข่าย
☐	**6. ไฟร์วอลล์**	**F**	สภาวะที่ปราศจากการติดตามหรือการสอดแนมสาธารณะ
☐	**7. ความเป็นส่วนตัว**	**G**	อัตราการถ่ายโอนข้อมูลสูงสุดผ่านการเชื่อมต่อ
☐	**8. ISP**	**H**	การห่อแพ็กเก็ตข้อมูลไว้ในแพ็กเก็ตอื่นเพื่อการส่งผ่านที่ปลอดภัย

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. ข้อจำกัดที่ป้องกันการเข้าเว็บตามตำแหน่งทางกายภาพ (7)

5. สถานะที่ปลอดจากการติดตามหรือการสอดแนมสาธารณะ (10)

8. คอมพิวเตอร์ระยะไกลที่ส่งต่อทราฟฟิกของคุณและปกปิดไอพี (8)

แนวตั้ง

1. อัตราสูงสุดของการถ่ายโอนข้อมูลผ่านการเชื่อมต่อ (7)

3. ชุดกฎที่กำหนดวิธีส่งข้อมูลผ่านเครือข่าย (8)

4. การห่อแพ็กเก็ตข้อมูลไว้ในแพ็กเก็ตอื่นเพื่อส่งอย่างปลอดภัย (5)

6. ระบบความปลอดภัยที่เฝ้าดูและบล็อกทราฟฟิกที่ไม่ได้รับอนุญาต (7)

7. ผู้ให้บริการอินเทอร์เน็ตซึ่งบันทึกทราฟฟิกของคุณหากไม่ได้เข้ารหัส (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: ข้อจำกัดที่ป้องกันการเข้าเว็บตามตำแหน่งทางกายภาพ (7 ตัวอักษร):

5 แนวนอน: สถานะที่ปลอดจากการติดตามหรือการสอดแนมสาธารณะ (10 ตัวอักษร):

8 แนวนอน: คอมพิวเตอร์ระยะไกลที่ส่งต่อทราฟฟิกของคุณและปกปิดไอพี (8 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: อัตราสูงสุดของการถ่ายโอนข้อมูลผ่านการเชื่อมต่อ (7 ตัวอักษร):

3 แนวตั้ง: ชุดกฎที่กำหนดวิธีส่งข้อมูลผ่านเครือข่าย (8 ตัวอักษร):

4 แนวตั้ง: การห่อแพ็กเก็ตข้อมูลไว้ในแพ็กเก็ตอื่นเพื่อส่งอย่างปลอดภัย (5 ตัวอักษร):

6 แนวตั้ง: ระบบความปลอดภัยที่เฝ้าดูและบล็อกทราฟฟิกที่ไม่ได้รับอนุญาต (7 ตัวอักษร):

7 แนวตั้ง: ผู้ให้บริการอินเทอร์เน็ตซึ่งบันทึกทราฟฟิกของคุณหากไม่ได้เข้ารหัส (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ไ	อ	เ	อ	ส	พี	ล	ม	า	ป	อ	อ	ม	มี	า
ล	ล	ป	จ	า	นี	กี	พ	แ	ร	ง	า	ซ	า	า
ลี	ล์	จ	ดี	า	น	ล	ผ	ดี	บ	ซ	ก	ด	า	ต
า	ล	ก	อ	ล็	บ	อ	โ	จี	จ	น	า	ค	ก	ดี
ร์	อ	า	ซ	ว	ไ	ก	ด	กี	ด	ท	ด์	ผ	ฟ	ซ
อ	ว	มี	ม	อ	ร้	ต	โ	ฟ	ร	ดี	า	วิ	ท	า
ว	ร์	ส	ท	ข	ก	ข	า	ป	น	ก	า	ล	ด	า
เ	ฟ	ม	ร	มี	า	า	อุ	ร	ร	ซ	ก	ด	ง	ท์
ฟ	ไ	น	ร	ต	ร	สี	ย	โ	ข	โ	มี	ดี	ด	ด
ร์	ว	บ	ฟ	อ	ติ	า	ร	ห	ม	ห	ต	รี	น	ผ
ชิ	นี	ม	ผ	ดี	ด	ข	กี	ส	บ	ง	ลี	ค	ง	ด
เ	ร	ด	ค	ผ	ต	ห	ดี	ป	ร	กี	ค์	นี	อ	า
ต	จ	ห	ดี	ด	า	บ	ตี	น	สี	ลี	ว	ลี	า	ล
ค	า	า	ล	ห	ม	ป	ส	ช	ตี	ลี	ล	มี	ข	ต
ดี	ตี	ห	ร	ม	า	ฟ	น	ซ	ข	ซ	ร	ม	า	ต

รายการคำศัพท์

อุโมงค์ โปรโตคอล แบนด์วิดท์ เซิร์ฟเวอร์ จิโอบล็อก ไฟร์วอลล์ ไร้การติดตาม ไอเอสพี

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. อุโมงค์
B. โปรโตคอล
C. แบนด์วิดท์
D. เซิร์ฟเวอร์
E. จีโอบล็อก
F. ไฟร์วอลล์
G. ไร้การติดตาม
H. ไอเอสพี

คำนิยามและช่องจับคู่
1. ชุดกฎที่กำหนดวิธีส่งข้อมูลผ่านเครือข่าย
2. ข้อจำกัดที่ป้องกันการเข้าเว็บตามตำแหน่งทางกายภาพ
3. ระบบความปลอดภัยที่เฝ้าดูและบล็อกทราฟฟิกที่ไม่ได้รับอนุญาต
4. สถานะที่ปลอดจากการติดตามหรือการสอดแนมสาธารณะ
5. ผู้ให้บริการอินเทอร์เน็ตซึ่งบันทึกทราฟฟิกของคุณหากไม่ได้เข้ารหัส
6. การห่อแพ็กเก็ตข้อมูลไว้ในแพ็กเก็ตอื่นเพื่อส่งอย่างปลอดภัย
7. คอมพิวเตอร์ระยะไกลที่ส่งต่อทราฟฟิกของคุณและปกปิดไอพี
8. อัตราสูงสุดของการถ่ายโอนข้อมูลผ่านการเชื่อมต่อ

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของ VPN เขียนคำตอบของคุณในช่องกรอกที่กรอกได้

1. ง ม อุ ค์ โ
2. แ น ท์ ด ว ิ ด์ บ
3. บ จ ี ล็ ก อ อ โ
4. ต ิ า ร ม า ต ด ไ ร้ ก
5. ต ค ป ล โ โ อ ร
6. อ ร์ ฟ ว เ เ ซ ิ ร์
7. ไ ล อ ส์ ฟ ว ร์
8. เ พ ี ไ ส อ อ

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	สิ่งที่ที่อยู่ IP เปิดเผยได้			
2	ความเชื่อผิด ๆ เกี่ยวกับ VPN			
3	สิ่งที่เดินทางผ่านอินเทอร์เน็ต			
4	คำมั่นสัญญาที่ผู้ให้บริการ VPN ที่ดีให้ไว้			
5	ความลับที่คุณจะเข้ารหัส			
6	สิ่งที่ VPN ปกป้องคุณไม่ได้			
7	วิธีสังเกตเครือข่าย Wi-Fi ปลอม			
8	คำที่เกี่ยวข้องกับความเป็นส่วนตัว			
9	อุปกรณ์ที่ใช้ VPN ได้			
10	สิ่งที่เกิดขึ้นเมื่อคุณกด "เชื่อมต่อ"			
11	สถานที่ที่คุณจะใช้ VPN			
12	เหตุผลที่ควรใช้ VPN ขณะเดินทาง			
13	สิ่งในชีวิตจริงที่ดูเหมือนอุโมงค์			
14	คำจากใบงานนี้ที่คุณอยากจำ			
15	คำที่ใช้อธิบาย VPN ให้เด็กฟัง			

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

VPN เข้ารหัสทราฟฟิกของคุณเพื่อรักษาความปลอดภัย ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความด้านความปลอดภัยไซเบอร์ 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

27	1	27	64	45	7

4	39	49	33	57	27	62	25	42	63	39	25	21	48	39		20	64	39	34

45	55	59	33	7	4	67

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: การใช้ VPN ถูกกฎหมายหรือไม่?

การใช้ VPN ถูกกฎหมายในหลายประเทศ แต่บางเขตอำนาจศาลจำกัด ควบคุม หรือบล็อกบริการ VPN ผู้ใช้ควรตรวจสอบกฎหมายท้องถิ่นปัจจุบันก่อนใช้งาน สำหรับรายละเอียดเพิ่มเติม โปรดดูคู่มือด้านความถูกกฎหมายบน VPN.com

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 [4]

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") 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: 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: VPN หลบการจำกัดความเร็วอินเทอร์เน็ตของ ISP ได้หรือไม่?

บางครั้ง VPN อาจช่วยได้เมื่อ ISP ชะลอกิจกรรมที่ระบุได้บางประเภทโดยเฉพาะ แต่จะไม่สามารถแก้ปัญหาความคับคั่ง ขีดจำกัดข้อมูล ข้อจำกัดความเร็วระดับบัญชี หรือคุณภาพเครือข่ายที่ไม่ดีได้

ส่วนที่ 11: ข้อเท็จจริงน่าสนใจเกี่ยวกับ VPN 10 ข้อและข้อมูลเชิงลึกในโลกจริง

ทบทวนข้อเท็จจริงและข้อมูลเชิงลึกในโลกจริงที่มีคุณค่าสูงเกี่ยวกับประวัติ ตลาด และเทคโนโลยีของ VPN

1. โปรโตคอล VPN แรก

PPTP (Point-to-Point Tunneling Protocol) พัฒนาโดยกลุ่มผู้ผลิตรวมถึง Microsoft และเผยแพร่เป็น RFC 2637 ในเดือนกรกฎาคม 1999 เพื่อรองรับ VPN สำหรับการเข้าถึงระยะไกล [6]

2. การประเมินมูลค่าตลาด

ตลาด VPN ทั่วโลกเติบโตอย่างรวดเร็ว โดยมีแรงขับเคลื่อนจากความต้องการทำงานทางไกลที่เพิ่มขึ้นและความต้องการด้านความปลอดภัยขององค์กร

3. การปฏิวัติ WireGuard

WireGuard มีโค้ดที่เรียบง่ายมากซึ่งออกแบบมาเพื่อประสิทธิภาพ ทำให้ตรวจสอบช่องโหว่ด้านความปลอดภัยได้ง่ายกว่าโปรโตคอลแบบดั้งเดิม [4]

4. มาตรฐานการตรวจสอบที่เข้มงวด

ผู้ให้บริการ VPN ชั้นนำจ้างผู้ตรวจสอบภายนอก (เช่น Cure53 หรือ PwC) ให้ตรวจสอบโค้ดอย่างอิสระและยืนยันว่าไม่บันทึกกิจกรรมของผู้ใช้

5. จุดกำเนิดของพันธมิตร 5-Eyes

พันธมิตร Five Eyes พัฒนามาจากข้อตกลงข่าวกรองสัญญาณ UKUSA ปี 1946 ระหว่างสหรัฐฯ และสหราชอาณาจักร ต่อมาแคนาดา ออสเตรเลีย และนิวซีแลนด์เข้าร่วม

6. การตรวจสอบแพ็กเก็ตเชิงลึก

การตรวจสอบแพ็กเก็ตเชิงลึก (DPI) ตรวจสอบเนื้อหาแพ็กเก็ตและรูปแบบทราฟฟิก ไม่ใช่แค่ส่วนหัว และไฟร์วอลล์บางตัวใช้ DPI เพื่อตรวจจับและบล็อกโปรโตคอล VPN ทั่วไป

7. การใช้งานในองค์กร

พนักงานองค์กรทั่วโลกจำนวนมากใช้ VPN ที่ปลอดภัยเพื่อเข้าสู่ฐานข้อมูลภายใน ทำให้เป็นมาตรฐานความปลอดภัยสำคัญ

8. VPN แบบกระจายศูนย์

VPN แบบกระจายศูนย์ (dVPN) กระจายทราฟฟิกไปทั่วเครือข่ายโหนดที่ผู้ใช้ดูแลเอง ช่วยลดการพึ่งพาผู้ให้บริการส่วนกลางรายเดียว

9. ความเป็นนิรนามของ TOR เทียบกับ VPN

VPN ส่งทราฟฟิกผ่านผู้ให้บริการรายเดียว ส่วน Tor (The Onion Router) ส่งทราฟฟิกผ่านรีเลย์อาสาสมัครสามตัว (guard, middle และ exit) จึงไม่มีรีเลย์ตัวใดรู้ทั้งสองปลายทาง

10. ต้นทุนของการละเมิดข้อมูล

การใช้โมเดลการเข้าถึงที่ปลอดภัยแบบ zero-trust ร่วมกับ VPN ช่วยให้องค์กรปกป้องทรัพย์สินทางปัญญาและลดผลกระทบทางการเงินจากข้อมูลรั่วไหล

แหล่งอ้างอิงทางเทคนิค

สิ่งพิมพ์ที่อ้างอิง ข้อกำหนดด้านการเข้ารหัส และมาตรฐานเอกสารทางการที่ใช้ตลอดทั้งใบงานนี้

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

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

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

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

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

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

เฉลย: ใบงาน VPN คืออะไร

1 **หน้าที่หลัก** โปรโตคอล **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

หน้าที่หลักของ VPN คือสร้างอุโมงค์เข้ารหัสที่ปกป้องข้อมูลเพย์โหลดของแพ็กเก็ตและปกปิดที่อยู่ IP สาธารณะของผู้ใช้ อ้างอิง: IETF Tunnel RFC.

2 **อุโมงค์เครือข่าย** เวลาแฝง **คำตอบที่ถูกต้อง: D**

หมายเหตุสำหรับผู้สอน

โปรโตคอลอุโมงค์ห่อหุ้มแพ็กเก็ตข้อมูลดั้งเดิมไว้ในแพ็กเก็ตพาหะชั้นนอกเพื่อให้ผ่านเครือข่ายสาธารณะได้อย่างปลอดภัย อ้างอิง: IETF Tunnel RFC.

3 **คำถาม 3** **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

มาตรฐานการเข้ารหัสใดที่ใช้กันอย่างแพร่หลายเพื่อปกป้องทราฟฟิก VPN? → มาตรฐาน AES-256 สมัยใหม่

4 **ส่วนประกอบที่เข้ารหัส** การควบคุมการกำหนดเส้นทาง **คำตอบที่ถูกต้อง: C**

หมายเหตุสำหรับผู้สอน

VPN เข้ารหัสส่วนเพย์โหลดทั้งหมดของแพ็กเก็ตข้อมูล IP เพื่อรักษาเนื้อหาที่ส่งไว้เป็นความลับ อ้างอิง: IETF Tunnel RFC.

5 **คำถาม 5** **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

การเข้ารหัสใช้อัลกอริทึมและคีย์เพื่อเปลี่ยนข้อความธรรมดาให้เป็นข้อความเข้ารหัสที่อ่านไม่ออก

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **การบล็อกการดักฟัง** การปกปิด IP — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

อุโมงค์ที่เข้ารหัสช่วยให้เพย์โหลดของแพ็กเก็ตอ่านไม่ออกสำหรับผู้ที่ดักข้อมูลบนเครือข่าย Wi-Fi ในพื้นที่ แหล่งอ้างอิง: Deloitte Advisory.

7 **การเปลี่ยนแปลงฮาร์ดแวร์** ความเร็ว — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

VPN เป็นอุโมงค์เครือข่ายบนซอฟต์แวร์และไม่ได้ปรับเปลี่ยนฮาร์ดแวร์เราเตอร์เกตเวย์ของคุณทางกายภาพ อ้างอิง: Cure53 Audit.

8 **แพ็กเก็ตอุโมงค์** ความเสี่ยงจากการดักจับแพ็กเก็ต — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

การทำอุโมงค์ทำงานโดยห่อแพ็กเก็ตเครือข่ายดั้งเดิมไว้ในส่วนหัวการขนส่งเพื่อส่งผ่านเครือข่าย อ้างอิง: IETF Tunnel RFC.

9 **กุญแจสมมาตร** ไฟร์วอลล์ — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

การเข้ารหัสแบบสมมาตรใช้กุญแจที่ใช้ร่วมกันทั้งสำหรับเข้ารหัสและถอดรหัสสตรีมเครือข่าย การอ้างอิง: WireGuard Project.

10 **ภูมิคุ้มกันด้านพลังงาน** ไม่เก็บล็อก — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

VPN เข้ารหัสเฉพาะสัญญาณการเชื่อมต่อที่ใช้งานอยู่ จึงป้องกันบริการหลุดจากไฟดับในพื้นที่ไม่ได้ อ้างอิง: EDRi Retention Guidelines.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

H 1. การทำอุโมงค์	E 2. โปรโตคอล	G 3. แบนด์วิดท์	A 4. เซิร์ฟเวอร์
C 5. การบล็อกตามภูมิศาสตร์	D 6. ไฟร์วอลล์	F 7. ความเป็นส่วนตัว	B 8. ISP

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 อุโมงค์	2 แบนด์วิดท์	3 จีโอบล็อก	4 โปรโตคอล
5 ไฟร์วอลล์	6 เซิร์ฟเวอร์		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 B – โปรโตคอล	2 E – จีโอบล็อก	3 F – ไฟร์วอลล์	4 G – ไร้การติดตาม
5 H – ไอเอสพี	6 A – อุโมงค์	7 D – เซิร์ฟเวอร์	8 C – แบนด์วิดท์

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย การทำอุโมงค์ โปรโตคอล และ แบนด์วิดท์ ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

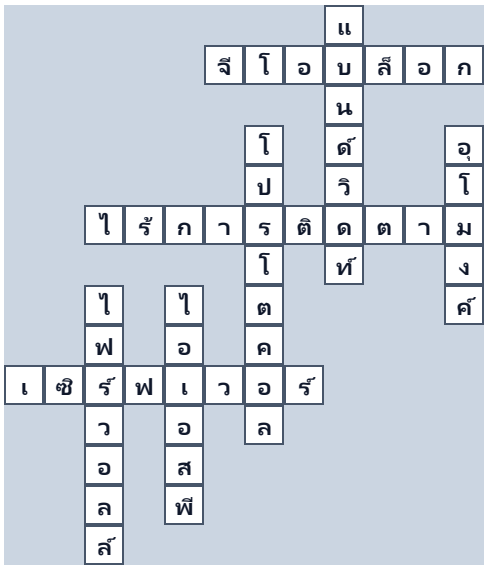
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ไ	อ	เ	อ	ส	พี	ล	ม	า	ป	อ	อ	ม	มี	า
ล	ล	ป	จ	า	นี	กี	พ	แ	ร	ง	า	ช	า	า
ลี	ล์	จ	ดี	า	น	ล	ผ	ดี	บ	ช	ก	ด	า	ต
า	ล	ก	อ	ล็	บ	อ	โ	จี	จ	น	า	ค	ก	ดี
ร์	อ	า	ช	ว	ไ	ก	ด	กี	ด	ท	ด์	ผ	ฟ	ช
อ	ว	มี	ม	อ	ร้	ต	โ	ฟ	ร	ดี	า	วิ	ท	า
ว	ร์	ส	ท	ข	ก	ข	า	ป	น	ก	า	ล	ด	า
เ	ฟ	ม	ร	มี	า	า	อุ	ร	ร	ช	ก	ด	ง	ท์
ฟ	ไ	น	ร	ต	ร	สี	ย	โ	ข	โ	มี	ดี	ด	ด
ร์	ว	บ	ฟ	อ	ติ	า	ร	ห	ม	ห	ต	รี	น	ผ
ซิ	นี	ม	ผ	ดี	ด	ข	กี	ส	บ	ง	ลี	ค	ง	ด
เ	ร	ด	ค	ผ	ต	ห	ดี	ป	ร	กี	ค์	นี	อ	า
ต	จ	ห	ดี	ด	า	บ	ดี	น	สี	ลี	ว	ลี	า	ล
ค	า	า	ล	ห	ม	ป	ส	ช	ดี	ลี	ล	มี	ข	ต
ดี	ดี	ห	ร	ม	า	ฟ	น	ช	ข	ช	ร	ม	า	ต

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: จีโอบล็อก ข้อจำกัดที่ป้องกันการเข้าเว็บตามตำแหน่งทางกายภาพ (7 ตัวอักษร)

5 แนวนอน: ไร้การติดตาม สถานะที่ปลอดจากการติดตามหรือการสอดแนมสาธารณะ (10 ตัวอักษร)

8 แนวนอน: เซิร์ฟเวอร์ คอมพิวเตอร์ระยะไกลที่ส่งต่อทราฟฟิกของคุณและปกปิดไอพี (8 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: แบนด์วิดท์ อัตราสูงสุดของการถ่ายโอนข้อมูลผ่านการเชื่อมต่อ (7 ตัวอักษร)

3 แนวตั้ง: โปรโตคอล ชุดกฎที่กำหนดวิธีส่งข้อมูลผ่านเครือข่าย (8 ตัวอักษร)

4 แนวตั้ง: อุโมงค์ การห่อแพ็กเก็ตข้อมูลไว้ในแพ็กเก็ตอื่นเพื่อส่งอย่างปลอดภัย (5 ตัวอักษร)

6 แนวตั้ง: ไฟร์วอลล์ ระบบความปลอดภัยที่เฝ้าดูและบล็อกทราฟฟิกที่ไม่ได้รับอนุญาต (7 ตัวอักษร)

7 แนวตั้ง: ไอเอสพี ผู้ให้บริการอินเทอร์เน็ตซึ่งบันทึกทราฟฟิกของคุณหากไม่ได้เข้ารหัส (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. งมอุศ์โ → **อุ่โมงศ์**
2. แนท์ดวิด์บ → **แบนด์วิดท์**
3. บจีล็กออโ → **จีโอบล็อก**
4. ติารมาตดไร้ก → **ไร้การติดตาม**
5. ตคปลโโอร → **โปรโตคอล**
6. อร์ฟวแซิร์ → **เซิร์ฟเวอร์**
7. ไลอล์ฟวร์ → **ไฟร์วอลล์**
8. เพีไสออ → **ไอเอสพี**

เฉลยภารกิจรหัสลับ

"ปกป้อง ความเป็นส่วนตัว ด้วย อุโมงค์"

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