ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

พร็อกซีเทียบกับ VPN ใบงาน

การเปรียบเทียบพร็อกซีเซิร์ฟเวอร์กับเครือข่ายส่วนตัวเสมือน ความแตกต่างของการเข้ารหัส และการกำหนดเส้นทางระดับแอปเทียบกับทั้งระบบ

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

- เปรียบเทียบพร็อกซีระดับแอปกับการเข้ารหัส VPN ทั้งระบบ
- ระบุความสามารถของ SOCKS5 เมื่อเทียบกับพร็อกซี HTTP พื้นฐาน
- วิเคราะห์ว่าพร็อกซีบนเบราว์เซอร์ทำให้แอปเบื้องหลังเสี่ยงต่อการถูกเปิดเผยอย่างไร
- ทำความเข้าใจว่า ISP บันทึกทราฟฟิกที่ไม่เข้ารหัสบนอุโมงค์พร็อกซีอย่างไร
- เลือกเครื่องมือกำหนดเส้นทางที่เหมาะสมตามความต้องการด้านความเร็วและความปลอดภัย

คำแนะนำใบงานเปรียบเทียบพร็อกซี

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การเปรียบเทียบพร็อกซีกับ VPN ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

พร็อกซีเทียบกับ VPN (บทนำ)

พร็อกซีและ VPN ทำหน้าที่ด้านความเป็นส่วนตัวดิจิทัลที่แตกต่างกัน เซิร์ฟเวอร์พร็อกซีทำหน้าที่เป็นการเปลี่ยนเส้นทางระดับแอปพลิเคชัน ซ่อนที่อยู่ IP ของคุณสำหรับโปรแกรมเฉพาะโดยไม่เข้ารหัสข้อมูล ส่วน VPN ทำงานในระดับเครือข่าย รักษาความปลอดภัยทราฟฟิกทั้งระบบด้วยการเข้ารหัส การเลือกเครื่องมือที่เหมาะสมขึ้นอยู่กับข้อกำหนดด้านความปลอดภัยของคุณ

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. การทำงานของพร็อกซี HTTP มาตรฐานอยู่ที่เลเยอร์ใดของโมเดล OSI?
   - A. ชั้นกายภาพ
   - B. เลเยอร์เครือข่าย
   - C. เลเยอร์แอปพลิเคชัน
   - D. ชั้น Data Link

2. ข้อได้เปรียบด้านโปรโตคอลที่สำคัญของ SOCKS5 เหนือพร็อกซี HTTP มาตรฐานคืออะไร?
   - A. บังคับให้เข้ารหัสเพย์โหลดเต็มรูปแบบ
   - B. รองรับการกำหนดเส้นทางทราฟฟิก TCP/UDP ทุกชนิด
   - C. ไม่ถูกการรั่วไหลของ DNS
   - D. ทำงานโดยตรงในพื้นที่เคอร์เนล

3. เหตุใด VPN จึงมักปลอดภัยกว่าพร็อกซีเซิร์ฟเวอร์?
   - A. ทำงานบนฮาร์ดแวร์ระยะไกลที่เร็วกว่า
   - B. เข้ารหัสทราฟฟิกเครือข่ายทั้งหมดทั่วทั้งระบบ
   - C. ไม่ต้องใช้ตารางเส้นทางในเครื่อง
   - D. กำจัดความหน่วงของเครือข่ายได้ทั้งหมด

4. พร็อกซีประเภทใดที่เปลี่ยนเส้นทางทราฟฟิกโดยไม่มีการเข้ารหัสตามค่าเริ่มต้น?
   - A. พร็อกซี HTTP พื้นฐาน
   - B. พร็อกซี HTTPS ที่เข้ารหัส
   - C. ไคลเอนต์ WireGuard ที่ปลอดภัย
   - D. เซิร์ฟเวอร์ VPN ที่อำพรางทราฟฟิก

5. ทราฟฟิกของแอปเบื้องหลังจะเป็นอย่างไรเมื่อใช้พร็อกซีของเบราว์เซอร์?
   - A. ถูกเข้ารหัสโดยอัตโนมัติ
   - B. ถูกบล็อกโดยพร็อกซีเซิร์ฟเวอร์
   - C. ถูกส่งผ่านอุโมงค์พร็อกซี
   - D. ข้ามพร็อกซีและเปิดเผย IP ของคุณ

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 **คำถาม 6**

6. พร็อกซี SOCKS5 เข้ารหัสเพย์โหลดของแพ็กเก็ตทั้งหมดที่ผ่านเซิร์ฟเวอร์

○ จริง ○ เท็จ

7 **คำถาม 7**

7. VPN ทำงานที่ชั้นเครือข่ายเพื่อรักษาความปลอดภัยของทราฟฟิกทั้งระบบ

○ จริง ○ เท็จ

8 **คำถาม 8**

8. โดยทั่วไปพร็อกซีเร็วกว่า VPN เพราะทำการเข้ารหัสแพ็กเก็ตเชิงลึก

○ จริง ○ เท็จ

9 **คำถาม 9**

9. การตั้งค่าพร็อกซีต้องตั้งค่าการเปลี่ยนเส้นทางทราฟฟิกภายในแต่ละแอป

○ จริง ○ เท็จ

10 **คำถาม 10**

10. การใช้พร็อกซีไม่ได้ปกป้องทราฟฟิกข้อมูลของคุณจากการติดตามของ ISP ในพื้นที่

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. _____ ชั้นแอปพลิเคชันเปลี่ยนเส้นทางทราฟฟิกเบราว์เซอร์เฉพาะโดยไม่ปกป้องแอปอื่น
2. _____ ที่แข็งแกร่งห่อหุ้มและเข้ารหัสแพ็กเก็ตข้อมูลทั้งหมดของอุปกรณ์
3. โปรโตคอล _____ อยู่ระหว่างชั้นแอปพลิเคชันและชั้นทรานสปอร์ต
4. พร็อกซี HTTP ทำงานที่ชั้น _____ ของโมเดล OSI
5. เซิร์ฟเวอร์พร็อกซีมาตรฐานไม่มี _____ เพย์โหลด ทำให้ข้อมูลเสี่ยง
6. VPN ให้การป้องกัน _____ แก่อะแดปเตอร์เครือข่ายทั้งหมด

คลังคำศัพท์

การเข้ารหัส | การมองเห็น | ซ็อกส์ห้า | ทั้งระบบ | พร็อกซี | ยูดีพี | อุโมงค์ | แอปพลิเคชัน

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องเครือข่าย

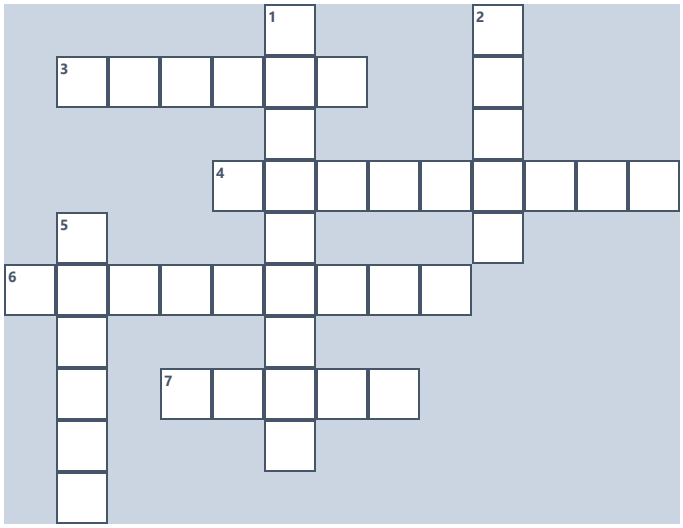
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. พร็อกซี HTTP**	**A**	การกำหนดเส้นทางระดับระบบปฏิบัติการที่เข้ารหัสทราฟฟิกของทุกแอปพลิเคชัน
☐	**2. พร็อกซี SOCKS5**	**B**	ชั้นแอปพลิเคชัน ซึ่งเป็นที่ทำงานของโปรโตคอลพร็อกซีเว็บมาตรฐาน
☐	**3. อุโมงค์ VPN**	**C**	ความสามารถของ SOCKS5 ในการส่งต่อ UDP รวมถึง TCP ต่างจากพร็อกซี HTTP ทั่วไป
☐	**4. ทั้งระบบ**	**D**	ส่วนขยายฝั่งไคลเอนต์ที่ซ่อนทราฟฟิกเฉพาะภายในแซนด์บ็อกซ์ของเบราว์เซอร์เท่านั้น
☐	**5. OSI Layer 7**	**E**	การเข้ารหัสและการห่อหุ้มที่ครอบคลุมทราฟฟิกเบื้องหลังทั้งหมดของอุปกรณ์
☐	**6. การรองรับ UDP**	**F**	สถานะทราฟฟิกที่ข้อมูลพร็อกซีที่ไม่เข้ารหัสยังมองเห็นได้โดย ISP
☐	**7. พร็อกซีของเบราว์เซอร์**	**G**	พร็อกซีระดับแอปพลิเคชันที่เปลี่ยนเส้นทางทราฟฟิกของเว็บเบราว์เซอร์เฉพาะ
☐	**8. การมองเห็นของ ISP**	**H**	โปรโตคอลพร็อกซีระหว่างชั้นแอปพลิเคชันและชั้นขนส่ง โดยไม่มีการเข้ารหัส

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

3. การกำหนดเส้นทางระดับระบบปฏิบัติการที่เข้ารหัสทราฟฟิกของทุกแอป (6)

4. สถานะทราฟฟิกที่ข้อมูลพร็อกซีแบบไม่เข้ารหัสยังคงมองเห็นได้โดย ISP (9)

6. ชั้นแอปพลิเคชันที่โปรโตคอลพร็อกซีเว็บมาตรฐานทำงาน (9)

7. พร็อกซีชั้นแอปพลิเคชันที่เปลี่ยนเส้นทางทราฟฟิกเบราว์เซอร์เฉพาะ (5)

แนวตั้ง

1. ส่วนขยายไคลเอนต์ที่ซ่อนทราฟฟิกเฉพาะภายในแซนด์บอกซ์ของเบราว์เซอร์ (9)

2. การเข้ารหัสและห่อหุ้มที่ครอบทราฟฟิกเบื้องหลังทั้งหมดของอุปกรณ์ (5)

5. โปรโตคอลพร็อกซีระหว่างชั้นแอปพลิเคชันกับชั้นทรานสปอร์ต โดยไม่มีการเข้ารหัส (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

3 แนวนอน: การกำหนดเส้นทางระดับระบบปฏิบัติการที่เข้ารหัสทราฟฟิกของทุกแอป (6 ตัวอักษร):

4 แนวนอน: สถานะทราฟฟิกที่ข้อมูลพร็อกซีแบบไม่เข้ารหัสยังคงมองเห็นได้โดย ISP (9 ตัวอักษร):

6 แนวนอน: ชั้นแอปพลิเคชันที่โปรโตคอลพร็อกซีเว็บมาตรฐานทำงาน (9 ตัวอักษร):

7 แนวนอน: พร็อกซีชั้นแอปพลิเคชันที่เปลี่ยนเส้นทางทราฟฟิกเบราว์เซอร์เฉพาะ (5 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ส่วนขยายไคลเอนต์ที่ซ่อนทราฟฟิกเฉพาะภายในแซนด์บอกซ์ของเบราว์เซอร์ (9 ตัวอักษร):

2 แนวตั้ง: การเข้ารหัสและห่อหุ้มที่ครอบทราฟฟิกเบื้องหลังทั้งหมดของอุปกรณ์ (5 ตัวอักษร):

5 แนวตั้ง: โปรโตคอลพร็อกซีระหว่างชั้นแอปพลิเคชันกับชั้นทรานสปอร์ต โดยไม่มีการเข้ารหัส (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า นี า น นี ส ช ทั้ มี ฟ บ า า ห นี
า ม ค์ กี จ า า ง รี ต พ ว ย ง ก
ค จ ง น ตี ว ร ร ดี ว ร็ า ล ล ด
ร์ า ม อ ย ช ฟ ะ ก ก อ ล ม า ป
อ อ โ อ ม แ มี บ า ล ก ล ป ก จ
ช า อุ นี กี อ พ บ ร ง ซี า ช า า
เ า ลี จ ดี ป า น ซ็ ล ผ ดี ช ร ก
ว์ ด า ต า พ จ า อ ค ก ดี า ม ช
า ว ก ด กี ลิ ด ท ก ผ ฟ ช มี อ ม
ร อ ต ฟ ร เ ดี า ส์ ท า ส ท ง ข
บ ข า น ก ค า ล ห้ า ม ร มี เ า
เ ร ช ก ด ชั้ ง น า พี ร ต สี ห็ ย
ข มี ดี ด ด น ว บ ดี ฟ อ า ร น ห
ห รี น ผ นี ม ผ ยู ดี ข กี ส บ ลี ง
ด ร ด ค ผ ห ดี ป ร กี นี า ต จ ห

รายการคำศัพท์

พร็อกซี ซ็อกส์ห้า อุโมงค์ ทั้งระบบ แอปพลิเคชัน ยูดีพี เบราว์เซอร์ การมองเห็น

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. พร็อกซี
B. ซ็อกส์ห้า
C. อุโมงค์
D. ทั้งระบบ
E. แอปพลิเคชัน
F. ยูดีพี
G. เบราว์เซอร์
H. การมองเห็น

คำนิยามและช่องจับคู่	
	1. ชั้นแอปพลิเคชันที่โปรโตคอลพร็อกซีเว็บมาตรฐานทำงาน
	2. ความสามารถของ SOCKS5 ในการส่งต่อ UDP และ TCP ซึ่งต่างจากพร็อกซี HTTP ธรรมดา
	3. พร็อกซีชั้นแอปพลิเคชันที่เปลี่ยนเส้นทางทราฟฟิกเบราว์เซอร์เฉพาะ
	4. ส่วนขยายไคลเอนต์ที่ซ่อนทราฟฟิกเฉพาะภายในแซนด์บอกซ์ของเบราว์เซอร์
	5. การเข้ารหัสและห่อหุ้มที่ครอบทราฟฟิกเบื้องหลังทั้งหมดของอุปกรณ์
	6. การกำหนดเส้นทางระดับระบบปฏิบัติการที่เข้ารหัสทราฟฟิกของทุกแอป
	7. สถานะทราฟฟิกที่ข้อมูลพร็อกซีแบบไม่เข้ารหัสยังคงมองเห็นได้โดย ISP
	8. โปรโตคอลพร็อกซีระหว่างชั้นแอปพลิเคชันกับชั้นทรานสปอร์ต โดยไม่มีการเข้ารหัส

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของ VPN เขียนคำตอบของคุณในช่องกรอกที่กรอกได้

1. ก อ พ ซี ร็
2. อุ ค์ ง ม โ
3. แ เ ล อ ค น พ ช ป
4. ว์ ร์ อ า ซ เ เ บ ร
5. ส์ ก า ซี ห้ อ
6. บ ะ ทั้ ร บ ง
7. พี ดี ยู
8. น อ ห็ ก ม า ง เ ร

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	ความแตกต่างระหว่างพร็อกซีกับ VPN			
2	สิ่งที่ไม่ถูกเข้ารหัสหากไม่มี VPN			
3	วิธีสังเกตเครือข่าย Wi-Fi ปลอม			
4	สิ่งที่คนกลางทำในชีวิตประจำวัน			
5	สถานการณ์ที่พร็อกซีก็เพียงพอ			
6	อุปกรณ์ที่ใช้ VPN ได้			
7	ประเภทของพร็อกซีที่คุณรู้จัก			
8	สิ่งที่ VPN ซ่อนได้			
9	ความเชื่อผิด ๆ เกี่ยวกับ VPN			
10	คำมั่นสัญญาที่ผู้ให้บริการ VPN ที่ดีให้ไว้			
11	สิ่งที่ VPN ปกป้องคุณไม่ได้			
12	คำจากใบงานนี้ที่คุณอยากจำ			
13	เหตุผลที่ควรใช้ VPN ขณะเดินทาง			
14	สถานการณ์ที่คุณต้องการ VPN			
15	สถานที่ที่คุณจะใช้ VPN			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

ซาราห์ (นักเรียนร้านกาแฟ)

👷 "สวัสดี! ตอนนี้ฉันอยู่ที่ร้าน Coffee & Bytes ใช้เครือข่ายเปิดชื่อ 'Free_Wi-Fi_No_Password' ฉันต้องล็อกอินอีเมลโรงเรียน และเพื่อนบอกว่าใช้พร็อกซีของเบราว์เซอร์ฟรีก็ปลอดภัยพอแล้ว พร็อกซีจะปกป้องการล็อกอินและไฟล์ของฉันได้ไหม หรือฉันต้องใช้ VPN?"

อเล็กซ์ (นักเรียนนักท่องเที่ยว)

👷 "ฉันอยู่ต่างประเทศ และสารคดีชีววิทยาที่โฮสต์ในประเทศบ้านเกิดของฉันขึ้นข้อความว่า 'วิดีโอนี้ไม่พร้อมใช้งานในตำแหน่งที่ตั้งปัจจุบันของคุณ' เพื่อนร่วมชั้นใช้พร็อกซี ส่วนฉันมี VPN ทำไมฉันถึงถูกบล็อก และเครื่องมือใดจะใช้ได้ดีกว่า?"

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

เพื่อให้การฝึกอบรมการเปรียบเทียบพร็อกซีของคุณเสร็จสมบูรณ์ ให้ถอดรหัสข้อความลับนี้เกี่ยวกับการทำอุโมงค์ที่ปลอดภัย

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

42	63	7	21	63	45		23	35	49	31	31	51	1		2	45	7	4	55	19
						28	63	49	25		30	35	62	45	1	11	52			

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: เซิร์ฟเวอร์พร็อกซีคืออะไร?

เซิร์ฟเวอร์พร็อกซีคือตัวกลางที่ส่งต่อคำขอระหว่างแอปพลิเคชันของคุณกับเซิร์ฟเวอร์ปลายทาง เว็บไซต์จะเห็นที่อยู่ IP ของพร็อกซีแทนของคุณ แต่ทราฟฟิกที่ถูกเปลี่ยนเส้นทางมีเฉพาะจากแอปที่ตั้งค่าให้ใช้พร็อกซี และพร็อกซีพื้นฐานไม่เข้ารหัสทราฟฟิกนั้น

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: พร็อกซีคือ VPN หรือไม่?

ไม่ พร็อกซีส่งต่อการรับส่งข้อมูลสำหรับบางแอปโดยปกติไม่มีการเข้ารหัส ส่วน VPN สร้างอุโมงค์เข้ารหัสที่ชั้นเครือข่ายซึ่งรองรับการรับส่งข้อมูลทั้งหมดของอุปกรณ์ รวมถึงแอปเบื้องหลัง

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดที่ผู้สนใจมีเกี่ยวกับการใช้เครือข่ายส่วนตัวเสมือน

Q6: ฉันใช้พร็อกซีฟรีได้หรือไม่?

ทำได้ แต่พร็อกซีฟรีมักดำเนินการโดยผู้ให้บริการที่ไม่ทราบที่มา เนื่องจากพร็อกซีพื้นฐานไม่เข้ารหัสทราฟฟิก ผู้ดำเนินการจึงเห็นและแก้ไขหน้าที่ไม่ได้เข้ารหัสได้ ควรตรวจสอบว่าใครเป็นผู้ให้บริการก่อนใช้งาน

Q7: พร็อกซีเก็บบันทึกข้อมูลหรือไม่?

ได้ พร็อกซีจัดการทุกคำขอที่ส่งต่อ ผู้ดำเนินการจึงอาจบันทึกที่อยู่ IP ของคุณ เว็บไซต์ที่คุณเข้าชม และเวลาที่เข้าชม ควรตรวจสอบว่าใครเป็นผู้ดำเนินการและนโยบายความเป็นส่วนตัวระบุไว้อย่างไร

Q8: เมื่อใดที่พร็อกซีก็เพียงพอ?

พร็อกซีอาจเพียงพอสำหรับงานที่มีความเสี่ยงต่ำ เช่น การเปลี่ยนตำแหน่งที่ตั้งที่ปรากฏของเบราว์เซอร์เดียว สำหรับการทำธุรกรรมธนาคาร Wi-Fi สาธารณะ หรือการปกป้องทุกแอปบนอุปกรณ์ VPN เป็นตัวเลือกที่ปลอดภัยกว่า เพราะเข้ารหัสทราฟฟิกทั้งหมด

Q9: พร็อกซีปกป้องแอปทั้งหมดบนโทรศัพท์ของฉันได้หรือไม่?

ไม่ มีเฉพาะแอปที่ยึดตามการตั้งค่าพร็อกซีเท่านั้นที่ใช้พร็อกซี แอปที่เหลือเชื่อมต่อโดยตรง ส่วนแอป VPN ส่งทุกแอปของโทรศัพท์ผ่านอุโมงค์เข้ารหัสของตนแทน

Q10: พร็อกซี SOCKS5 คืออะไร?

SOCKS5 ซึ่งกำหนดใน RFC 1928 เป็นโปรโตคอลพร็อกซีที่อยู่ระหว่างชั้นแอปพลิเคชันและชั้นการขนส่ง สามารถส่งต่อการเชื่อมต่อ TCP และดาตาแกรม UDP และรองรับการยืนยันตัวตน แต่ไม่มีการเข้ารหัสในตัว [1]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคและโครงสร้างของเครือข่ายส่วนตัวเสมือนและโปรโตคอลอุโมงค์ที่ปลอดภัย

Q1: พร็อกซีและ VPN ทำงานที่ชั้นเครือข่ายใด?

พร็อกซี HTTP ทำงานที่ชั้นแอปพลิเคชัน (Layer 7) และเข้าใจคำขอเว็บ ส่วน SOCKS5 อยู่ระหว่างชั้นแอปพลิเคชันกับชั้นทรานสปอร์ต โปรโตคอล VPN เช่น IPsec หรือ WireGuard ทำงานที่ชั้นเครือข่าย จึงส่งทราฟฟิก IP ทั้งหมดจากอุปกรณ์ได้

Q2: เว็บไซต์ HTTPS ยังคงเข้ารหัสอยู่เมื่อผ่านพร็อกซีหรือไม่?

ได้ เมื่อคุณเปิดเว็บไซต์ HTTPS ผ่านพร็อกซี การเข้ารหัส TLS ทำงานตั้งแต่ต้นทางถึงปลายทางระหว่างเบราว์เซอร์ของคุณกับเว็บไซต์ พร็อกซีจึงเห็นโดเมน แต่ไม่เห็นเนื้อหาของหน้า ส่วนหน้า HTTP ธรรมดายังอ่านได้

Q3: การรั่วไหลของ WebRTC คืออะไร และ VPN ป้องกันได้อย่างไร?

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

Q4: พร็อกซีแบบโปร่งใส (transparent proxy) คืออะไร และใครใช้?

พร็อกซีโปร่งใสดักทราฟฟิกโดยไม่ต้องตั้งค่าใดๆ บนอุปกรณ์ของผู้ใช้ โรงเรียน บริษัท และ ISP ใช้เพื่อแคชหรือกรองเนื้อหา ผู้ใช้มักไม่รู้ว่ามีพร็อกซีอยู่ และไม่ได้รับความเป็นส่วนตัวใดๆ

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: ทำไมพร็อกซีจึงรู้สึกเร็วกว่าการเชื่อมต่อ VPN?

พร็อกซีพื้นฐานข้ามการเข้ารหัสและจัดการทราฟฟิกจากแอปเดียวเท่านั้น จึงเพิ่มภาระการประมวลผลน้อยกว่า ส่วน VPN เข้ารหัสทุกแพ็กเก็ตจากอุปกรณ์ เมื่อใช้โปรโตคอลสมัยใหม่ ความแตกต่างมักมีเพียงเล็กน้อย และพร็อกซีให้การปกป้องน้อยกว่ามาก

Q8: เว็บไซต์บอกได้หรือไม่ว่าฉันใช้พร็อกซีหรือ VPN?

บ่อยครั้งใช่ หลายเว็บไซต์ตรวจสอบที่อยู่ IP เทียบกับรายชื่อเซิร์ฟเวอร์พร็อกซีและ VPN ที่รู้จัก และพร็อกซี HTTP อาจเพิ่มส่วนหัวเช่น Via หรือ X-Forwarded-For บริการสตรีมมิงมักบล็อกทั้งสองอย่าง

Q9: การป้องกัน DNS Leak คืออะไร?

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

Q10: พร็อกซีหยุดการจำกัดความเร็วของ ISP ได้หรือไม่?

แทบไม่ได้ พร็อกซีพื้นฐานไม่เข้ารหัสทราฟฟิก ISP จึงยังเห็นได้ว่าเป็นกิจกรรมประเภทใด VPN ซ่อนประเภทของทราฟฟิก แต่เครื่องมือทั้งสองไม่ช่วยแก้ปัญหาความแออัดหรือขีดจำกัดข้อมูล

ส่วนที่ 11: ข้อเท็จจริงน่าสนใจเกี่ยวกับ VPN 10 ข้อและข้อมูลเชิงลึกในโลกจริง

ทบทวนข้อเท็จจริงและข้อมูลเชิงลึกในโลกจริงที่มีคุณค่าสูงเกี่ยวกับประวัติ ตลาด และเทคโนโลยีของ VPN

1. มาตรฐาน SOCKS

SOCKS Protocol Version 5 ได้รับการเผยแพร่โดย IETF เป็น RFC 1928 ในเดือนมีนาคม 1996 และยังคงเป็นข้อกำหนดอ้างอิงของพร็อกซี SOCKS5 ที่เบราว์เซอร์และแอปใช้ในปัจจุบัน [1]

2. ชั้น SHIM

RFC 1928 อธิบาย SOCKS ว่าเป็นชั้นกลางระหว่างชั้นแอปพลิเคชันกับชั้นทรานสปอร์ต จึงไม่สามารถส่งต่อทราฟฟิกชั้นเครือข่ายอย่าง ICMP ได้ [1]

3. รีเลย์ UDP

SOCKS5 เพิ่มคำสั่ง UDP ASSOCIATE ทำให้พร็อกซีส่งต่อดาตาแกรม UDP ได้เช่นเดียวกับการเชื่อมต่อ TCP ซึ่งพร็อกซี HTTP ธรรมดาไม่รองรับ [1]

4. พอร์ต SOCKS เริ่มต้น

ไคลเอนต์ SOCKS5 เชื่อมต่อกับเซิร์ฟเวอร์พร็อกซีที่พอร์ต TCP 1080 โดยค่าเริ่มต้นตามที่กำหนดใน RFC 1928 บริการพร็อกซีหลายรายให้ผู้ใช้เลือกพอร์ตอื่นได้ [1]

5. ตัวกลาง HTTP

มาตรฐาน HTTP (RFC 9110) กำหนดให้พร็อกซีเป็นตัวแทนส่งต่อข้อความที่ไคลเอนต์เลือก ซึ่งส่งต่อคำขอไปยังเซิร์ฟเวอร์ต้นทาง

6. การตรวจสอบแพ็กเก็ตเชิงลึก

การตรวจสอบแพ็กเก็ตเชิงลึก (DPI) ตรวจสอบเนื้อหาแพ็กเก็ตและรูปแบบทราฟฟิก ทราฟฟิกพร็อกซีที่ไม่เข้ารหัสมองเห็นได้ทั้งหมด ส่วนทราฟฟิก VPN เผยข้อมูลน้อยกว่ามาก

7. VPN ระดับชั้นเครือข่าย

IPsec ซึ่งอธิบายไว้ใน NIST SP 800-77 ปกป้องทราฟฟิกที่ชั้นเครือข่าย จึงรักษาความปลอดภัยแพ็กเก็ต IP ของทุกแอปพลิเคชันได้โดยไม่ต้องตั้งค่าทีละแอป [2]

8. ขอบเขตเฉพาะเบราว์เซอร์

พร็อกซีที่ตั้งไว้ในเบราว์เซอร์หนึ่งส่งผลกับเบราว์เซอร์นั้นเท่านั้น ไคลเอนต์อีเมล เกม และการอัปเดตระบบยังคงใช้การเชื่อมต่อปกติของอุปกรณ์

9. TOR กับพร็อกซี

Tor ส่งทราฟฟิกผ่านรีเลย์อาสาสมัครสามตัว (guard, middle และ exit) และมักเข้าถึงผ่านพร็อกซี SOCKS ในเครื่อง ซึ่งเพิ่มชั้นที่พร็อกซีเดี่ยวทำไม่ได้

10. การแลกเปลี่ยนระหว่างความเร็ว

พร็อกซีอาจดูเร็วกว่าเพราะข้ามการเข้ารหัส แต่โปรโตคอล VPN สมัยใหม่อย่าง WireGuard เพิ่มภาระเพียงเล็กน้อยในขณะที่ปกป้องทราฟฟิกทั้งหมดของอุปกรณ์

แหล่งอ้างอิงทางเทคนิค

สิ่งพิมพ์ที่อ้างอิง ข้อกำหนดด้านการเข้ารหัส และมาตรฐานเอกสารทางการที่ใช้ตลอดทั้งใบงานนี้

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

เฉลย: การเปรียบเทียบพร็อกซีเซิร์ฟเวอร์กับเครือข่ายส่วนตัวเสมือน ความแตกต่างด้านการเข้ารหัส และการกำหนดเส้นทางระดับแอปกับทั้งระบบ

1 **ชั้น OSI ของพร็อกซี** โปรโตคอล — **คำตอบที่ถูกต้อง: C**

หมายเหตุสำหรับผู้สอน

พร็อกซี HTTP/HTTPS มาตรฐานทำงานที่ชั้นแอปพลิเคชัน (Layer 7) และเปลี่ยนเส้นทางทราฟฟิกเบราว์เซอร์เฉพาะส่วน ไม่มีการกำหนดเส้นทางเครือข่ายทั่วทั้งระบบ การอ้างอิง: Tor Project Foundation.

2 **คำถาม 2** — **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

SOCKS5 ส่งต่อทราฟฟิก TCP และ UDP ระหว่างชั้นแอปพลิเคชันและชั้นขนส่ง แต่ไม่เข้ารหัสโดยค่าเริ่มต้น ส่วนพร็อกซี HTTP จัดการคำขอเว็บ

3 **การเข้ารหัสระบบของ VPN** ความปลอดภัย Wi-Fi — **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

VPN ห่อหุ้มและเข้ารหัสทราฟฟิกทั้งหมดของระบบปฏิบัติการทั่วทั้งระบบ ในขณะที่พร็อกซีเพียงเปลี่ยนเส้นทางทราฟฟิกของแอปพลิเคชันที่กำหนดค่าไว้เท่านั้น อ้างอิง: Deloitte Advisory.

4 **การขาดการเข้ารหัสของพร็อกซี** การควบคุมการกำหนดเส้นทาง — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

พร็อกซี HTTP ส่งต่อทราฟฟิกของเบราว์เซอร์ที่ชั้นแอปพลิเคชันโดยไม่เข้ารหัสเพย์โหลดของแพ็กเก็ต ซึ่งหมายความว่าผู้ให้บริการเครือข่ายหรือ ISP ของคุณยังคงติดตามทราฟฟิกเนื้อหาของคุณได้ การอ้างอิง: IETF Proxy Vulnerabilities.

5 **ช่องโหว่จากการข้าม** ความเป็นส่วนตัว — **คำตอบที่ถูกต้อง: D**

หมายเหตุสำหรับผู้สอน

พร็อกซีของเบราว์เซอร์ใช้กฎกับตัวเว็บเบราว์เซอร์เท่านั้น แอปเบื้องหลัง การอัปเดตระบบปฏิบัติการ และไคลเอนต์อีเมลจะข้ามพร็อกซีไป ทำให้ที่อยู่ IP จริงของคุณถูกเปิดเผย อ้างอิง: W3C Consortium.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

SOCKS5 ส่งต่อทราฟฟิกระหว่างชั้นแอปพลิเคชันและชั้นขนส่ง แต่ไม่มีการเข้ารหัสโดยค่าเริ่มต้น เนื้อหาของแพ็กเก็ตจึงยังอ่านได้ระหว่างการส่ง

7 **อุโมงค์ระดับชั้นเครือข่าย** ความเร็ว คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

เพราะทำงานที่เลเยอร์เครือข่าย VPN จึงกำหนดเส้นทางและเข้ารหัสทราฟฟิกขาออกจากอุปกรณ์ของคุณ ช่วยปกป้องทราฟฟิกทั้งระบบ อ้างอิง: Deloitte Advisory.

8 **ขีดจำกัดการเข้ารหัสของพร็อกซี** ความเสี่ยงจากการดักจับแพ็กเก็ต คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

บางครั้งพร็อกซีอาจเร็วกว่า แต่เป็นเพราะไม่ได้ทำการเข้ารหัส การไม่เข้ารหัสนี้ทำให้ข้อมูลเสี่ยงต่อการถูกตรวจสอบ อ้างอิง: IETF Proxy Vulnerabilities.

9 **การเปลี่ยนเส้นทางระดับแอป** ไฟร์วอลล์ คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

ต่างจาก VPN ทั่วทั้งระบบ พร็อกซีเซิร์ฟเวอร์ต้องตั้งค่าด้วยตนเองในการตั้งค่าเบราว์เซอร์หรือซ่องพร็อกซีเฉพาะแอป อ้างอิง: W3C Consortium.

10 **ความเสี่ยงจากการติดตามโดย ISP** ไม่เก็บล็อก คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

เพราะพร็อกซี HTTP/SOCKS5 มาตรฐานไม่เข้ารหัสข้อมูลเพย์โหลด ISP ในพื้นที่ของคุณจึงยังเห็นการกระทำออนไลน์ของคุณได้ครบถ้วน อ้างอิง: EDRi Retention Guidelines.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

G 1. พร็อกซี HTTP	H 2. พร็อกซี SOCKS5	E 3. อุโมงค์ VPN	A 4. ทั้งระบบ
B 5. OSI Layer 7	C 6. การรองรับ UDP	D 7. พร็อกซีของเบราว์เซอร์	F 8. การมองเห็นของ ISP

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 พร็อกซี	2 อุโมงค์	3 ซ็อกส์ห้า	4 แอปพลิเคชัน
5 การเข้ารหัส	6 ทั้งระบบ		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 E – แอปพลิเคชัน	2 F – ยูดีพี	3 A – พร็อกซี	4 G – เบราว์เซอร์
5 C – อุโมงค์	6 D – ทั้งระบบ	7 H – การมองเห็น	8 B – ซ็อกส์ห้า

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย พร็อกซี HTTP พร็อกซี SOCKS5 และ อุโมงค์ VPN ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

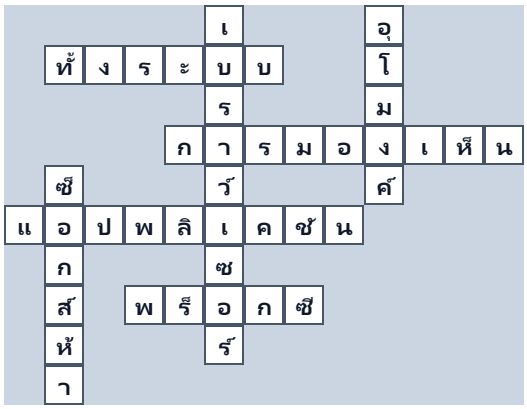
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	นี	า	น	นี	ส	ช	ทั้	มี	ฟ	บ	า	า	ห	นี
า	ม	ค์	กี	จ	า	า	ง	รี	ต	พ	ว	ย	ง	ก
ค	จ	ง	น	ดี	ว	ร	ร	ดี	ว	ร์	า	ล	ล	ด
ร์	า	ม	อ	ย	ช	ฟ	ะ	ก	ก	อ	ล	ม	า	ป
อ	อ	โ	อ	ม	แ	มี	บ	า	ล	ก	ล	ป	ก	จ
ช	า	อุ	นี	กี	อ	พ	บ	ร	ง	ซี	า	ช	า	า
เ	า	ลี	จ	ดี	ป	า	น	ซ็	ล	ผ	ดี	ช	ร	ก
ว์	ด	า	ต	า	พ	จ	า	อ	ค	ก	ดี	า	ม	ช
า	ว	ก	ด	กี	ลิ	ด	ท	ก	ผ	ฟ	ช	มี	อ	ม
ร	อ	ต	ฟ	ร	เ	ดี	า	ส์	ท	า	ส	ท	ง	ข
บ	ข	า	น	ก	ค	า	ล	ห้	า	ม	ร	มี	เ	า
เ	ร	ช	ก	ด	ช้	ง	น	า	พื	ร	ต	สี	ห็	ย
ข	มี	ดี	ด	ด	น	ว	บ	ดี	ฟ	อ	า	ร	น	ห
ห	รี	น	ผ	นี	ม	ผ	ยู	ดี	ข	กี	ส	บ	ลี	ง
ด	ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

3 แนวนอน: ทั้งระบบ การกำหนดเส้นทางระดับระบบปฏิบัติการที่เข้ารหัสทราฟฟิกของทุกแอป (6 ตัวอักษร)

4 แนวนอน: การมองเห็น สถานะทราฟฟิกที่ข้อมูลพร็อกซีแบบไม่เข้ารหัสยังคงมองเห็นได้โดย ISP (9 ตัวอักษร)

6 แนวนอน: แอปพลิเคชัน ชั้นแอปพลิเคชันที่โปรโตคอลพร็อกซีเว็บมาตรฐานทำงาน (9 ตัวอักษร)

7 แนวนอน: พร็อกซี พร็อกซีชั้นแอปพลิเคชันที่เปลี่ยนเส้นทางทราฟฟิกเบราว์เซอร์เฉพาะ (5 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: เบราว์เซอร์ ส่วนขยายไคลเอนต์ที่ซ่อนทราฟฟิกเฉพาะภายในแซนด์บอกซ์ของเบราว์เซอร์ (9 ตัวอักษร)

2 แนวตั้ง: อุโมงค์ การเข้ารหัสและห่อหุ้มที่ครอบทราฟฟิกเบื้องหลังทั้งหมดของอุปกรณ์ (5 ตัวอักษร)

5 แนวตั้ง: ซ็อกส์ห้า โปรโตคอลพร็อกซีระหว่างชั้นแอปพลิเคชันกับชั้นทรานสปอร์ต โดยไม่มีการเข้ารหัส (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. กอพซีร็ — พร็อกซี
2. อุศ์งม์โ — อุโมงค์
3. แลิอคนพซ์ป — แอปพลิเคชัน
4. ว์ร์อาซแบร — เบราว์เซอร์
5. ส์กาซ์ห้อ — ซ็อกส์ห้า
6. บะทั้รบง — ทั้งระบบ
7. พีดียู — ยูดีพี
8. นอห็กมางเร — การมองเห็น

เฉลยภารกิจรหัสลับ

"ส่งต่อ ทราฟฟิก ของคุณ ผ่าน พร็อกซี"

เฉลยกรณีศึกษา

A สถานการณ์ A: ความปลอดภัยของเครือข่ายสาธารณะ

การดักจับแพ็กเก็ตและการเข้ารหัส | ความกังวลของซาราห์

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- ความเสี่ยง: การดักจับแพ็กเก็ต การสกัดกั้นข้อมูล และการโจมตีแบบ man-in-the-middle ผู้ที่อยู่ในเครือข่ายร้านกาแฟเดียวกันอาจดักจับรายละเอียดการล็อกอินหรือไฟล์การบ้านของเธอได้
- พร็อกซีเทียบกับ VPN: พร็อกซีเบราว์เซอร์พื้นฐานไม่เข้ารหัสทราฟฟิกของเธอ ส่วน VPN เข้ารหัสทุกอย่างบนอุปกรณ์ ทำให้แพ็กเก็ตที่ถูกดักจับอ่านไม่ได้สำหรับผู้แอบดูในพื้นที่

B สถานการณ์ B: การเข้าถึงทรัพยากรที่ถูกบล็อก

การบล็อกตามภูมิศาสตร์และ IP | ปัญหาของอเล็กซ์

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- เหตุผลที่ถูกบล็อก: โฮสต์สตรีมมิงใช้การบล็อกตามภูมิศาสตร์ ซึ่งจับคู่ที่อยู่ IP ท้องถิ่นของผู้เดินทางกับประเทศจริงของเขาและบล็อกตามการอนุญาตให้ใช้สิทธิ์ตามอาณาเขต
- แบบไหนดีกว่า: ทั้งสองอย่างให้ IP ของประเทศบ้านเกิดแก่เขา แต่พร็อกซีครอบคลุมเฉพาะแอปที่กำหนดค่าไว้ ขณะที่ VPN ยังเข้ารหัสทราฟฟิกทั้งหมดของอุปกรณ์เขาด้วย