ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

WireGuard เทียบกับ OpenVPN ใบงาน

การเปรียบเทียบโปรโตคอล WireGuard และ OpenVPN ขนาดโค้ดเบส ความเร็ว และมาตรฐานการเข้ารหัส

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

- เปรียบเทียบความซับซ้อนของโค้ดและความเร็วในการตรวจสอบของโปรโตคอล
- วิเคราะห์ประสิทธิภาพที่ได้จากการทำงานภายในพื้นที่เคอร์เนล
- เปรียบเทียบชุดรหัส OpenSSL กับการเข้ารหัสสมัยใหม่ของ WireGuard
- ตั้งค่าคู่กุญแจสาธารณะและกุญแจส่วนตัวสำหรับการแฮนด์เชคระหว่างเพียร์
- ส่งทราฟฟิก VPN ผ่านพอร์ตไฟร์วอลล์ TCP และ UDP

คำแนะนำใบงานเปรียบเทียบโปรโตคอล

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การตรวจสอบโปรโตคอลสมัยใหม่ ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

WireGuard เทียบกับ OpenVPN (บทนำ)

การเลือกโปรโตคอล VPN ต้องสร้างสมดุลระหว่างความเร็วและตัวเลือกการกำหนดค่า OpenVPN เป็นมาตรฐานมานานหลายสิบปี และให้ความยืดหยุ่นในการตั้งค่า TCP/UDP ส่วน WireGuard เป็นตัวทดแทนสมัยใหม่ที่ทำงานโดยตรงในพื้นที่เคอร์เนลด้วยโค้ดเพียง 4,000 บรรทัด การเข้าใจความแตกต่างของโปรโตคอลเป็นกุญแจสำคัญในการเพิ่มประสิทธิภาพเครือข่ายที่ปลอดภัยของคุณ

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. ขนาดโค้ดโดยประมาณของโปรโตคอล WireGuard คือเท่าใด?

- A. ประมาณ 70,000 บรรทัด
- B. มากกว่า 100,000 บรรทัด
- C. น้อยกว่า 1,000 บรรทัด
- D. ประมาณ 4,000 บรรทัด

2. WireGuard ทำงานในพื้นที่ใดของระบบปฏิบัติการ?

- A. ยูเซอร์สเปซ
- B. พื้นที่เคอร์เนล
- C. พื้นที่แอปพลิเคชัน
- D. พื้นที่เสมือน

3. OpenVPN พึ่งพาไลบรารีการเข้ารหัสลับใดเป็นหลัก?

- A. ChaCha20-Poly1305
- B. ไลบรารีการเข้ารหัสลับ OpenSSL
- C. เฟรมเวิร์กโปรโตคอล Noise
- D. การเข้ารหัส DES แบบข้อความธรรมดา

4. ข้อได้เปรียบด้านประสิทธิภาพที่สำคัญของ WireGuard เหนือ OpenVPN คืออะไร?

- A. การแฮนด์เชคการเชื่อมต่อเร็วขึ้นและความหน่วงต่ำลง
- B. การไม่ต้องใช้ที่อยู่ IP สาธารณะ
- C. การรองรับ dial-up รุ่นเก่าในตัวแบบเนทีฟ
- D. ไม่มีภาระต่อแบตเตอรี่บนอุปกรณ์มือถือ

5. WireGuard ยืนยันตัวตนการเชื่อมต่อของเพียร์อย่างไร?

- A. ด้วยการแลกเปลี่ยนรหัสผ่านผู้ใช้มาตรฐาน
- B. ด้วยการตรวจสอบใบรับรองการจดทะเบียนโดเมน
- C. ด้วยการใช้คู่กุญแจสาธารณะและกุญแจส่วนตัวแบบคงที่
- D. ด้วยการตรวจสอบหมายเลขซีเรียลของฮาร์ดแวร์

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. โค้ดที่กะทัดรัดของ WireGuard ทำให้ตรวจสอบได้ง่ายขึ้นอย่างมาก

จริง เท็จ

7 คำถาม 7

7. โดยทั่วไป OpenVPN เร็วกว่า WireGuard เพราะทำงานในพื้นที่เคอร์เนล

จริง เท็จ

8 คำถาม 8

8. OpenVPN ปรับแต่งได้สูงและรองรับทั้งโปรโตคอล UDP และ TCP

จริง เท็จ

9 คำถาม 9

9. WireGuard ใช้การเข้ารหัสสมัยใหม่อย่าง ChaCha20 เพื่อเข้ารหัสแพ็กเก็ตอย่างรวดเร็ว

จริง เท็จ

10 คำถาม 10

10. WireGuard ต้องตั้งค่าผู้ออกใบรับรองที่ซับซ้อนเพื่อยืนยันตัวตน

จริง เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. โปรโตคอล _____ สมัยใหม่ทำงานโดยตรงภายในเคอร์เนลของระบบปฏิบัติการ
2. โปรโตคอลรุ่นเก่า _____ อาศัยไลบรารีเข้ารหัสลับ OpenSSL
3. การรันโค้ดใน _____ ลดภาระการสลับบริบท
4. OpenVPN ทำงานใน _____ โดยส่งแพ็กเก็ตผ่านอินเทอร์เฟซเสมือน
5. WireGuard ใช้กุญแจสาธารณะและส่วนตัวเป็น _____ เพื่อระบุเพียร์ที่เชื่อมต่อ
6. ขนาดฐานโค้ดที่เล็กเพิ่ม _____ ด้านความปลอดภัยของซอฟต์แวร์

คลังคำศัพท์

การตรวจสอบได้ | คู่กุญแจ | เคอร์เนล | โค้ดกะทัดรัด | ทีซีพียูดีพี | พื้นที่ผู้ใช้ | ไวร์การ์ด | โอเพนวีพีเอ็น

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องเครือข่าย

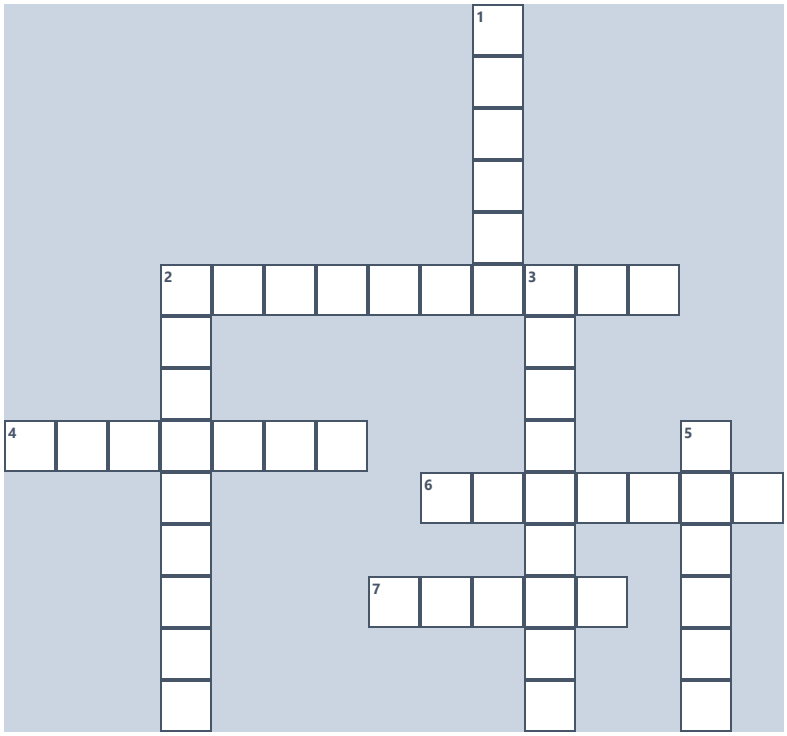
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. WireGuard**	**A**	พื้นที่ประมวลผลที่ OpenVPN ทำงาน ซึ่งสร้างภาระจากการสลับบริบท
☐	**2. OpenVPN**	**B**	ขนาดโค้ดเบสที่กะทัดรัดของ WireGuard ทำให้ตรวจสอบได้ง่ายขึ้นมาก
☐	**3. เคอร์เนลสเปซ**	**C**	ไลบรารีการเข้ารหัสที่ OpenVPN ใช้สำหรับอัลกอริทึมชุดรหัส
☐	**4. ยูสเซอร์สเปซ**	**D**	โปรโตคอลขนส่งที่ OpenVPN รองรับ ส่วน WireGuard เองทำงานบน UDP เท่านั้น
☐	**5. 4,000 บรรทัด**	**E**	พื้นที่การทำงานของระบบปฏิบัติการที่ WireGuard ทำงานเพื่อความเร็ว
☐	**6. OpenSSL**	**F**	โทเคนแบบอสมมาตรที่ WireGuard ใช้ยืนยันการเชื่อมต่อของเพียร์
☐	**7. คู่คีย์**	**G**	โปรโตคอล VPN สมัยใหม่ที่ออกแบบมาเพื่อความเร็วสูงและการตรวจสอบโค้ดที่ง่าย
☐	**8. TCP/UDP**	**H**	โปรโตคอลรุ่นเก่าที่แข็งแกร่งซึ่งใช้โค้ดกำหนดค่าขนาดใหญ่และซับซ้อน

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. โปรโตคอลรุ่นเก่าที่แข็งแกร่งซึ่งใช้ฐานโค้ดการกำหนดค่าขนาดใหญ่และซับซ้อน (10)

4. โปรโตคอล VPN สมัยใหม่ที่ออกแบบเพื่อความเร็วสูงและการตรวจสอบโค้ดที่ง่าย (7)

6. พื้นที่ประมวลผลของระบบปฏิบัติการที่ WireGuard ทำงานเพื่อความเร็ว (7)

7. โทเค็นอสมมาตรที่ WireGuard ใช้ยืนยันการเชื่อมต่อของเพียร์ (5)

แนวตั้ง

1. โปรโตคอลขนส่งที่ OpenVPN รองรับ ส่วน WireGuard ทำงานบน UDP เท่านั้น (6)

2. ขนาดกะทัดรัดของฐานโค้ด WireGuard ทำให้ตรวจสอบได้ง่ายขึ้นมาก (9)

3. ไลบรารีเข้ารหัสลับที่ OpenVPN พึ่งพาสำหรับอัลกอริทึมไซเฟอร์ (9)

5. พื้นที่ประมวลผลที่ OpenVPN ทำงาน ทำให้เกิดภาระการสลับบริบท (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: โปรโตคอลรุ่นเก่าที่แข็งแกร่งซึ่งใช้ฐานโค้ดการกำหนดค่าขนาดใหญ่และซับซ้อน (10 ตัวอักษร):

4 แนวนอน: โปรโตคอล VPN สมัยใหม่ที่ออกแบบเพื่อความเร็วสูงและการตรวจสอบโค้ดที่ง่าย (7 ตัวอักษร):

6 แนวนอน: พื้นที่ประมวลผลของระบบปฏิบัติการที่ WireGuard ทำงานเพื่อความเร็ว (7 ตัวอักษร):

7 แนวนอน: โทเค็นอสมมาตรที่ WireGuard ใช้ยืนยันการเชื่อมต่อของเพียร์ (5 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: โปรโตคอลขนส่งที่ OpenVPN รองรับ ส่วน WireGuard ทำงานบน UDP เท่านั้น (6 ตัวอักษร):

2 แนวตั้ง: ขนาดกะทัดรัดของฐานโค้ด WireGuard ทำให้ตรวจสอบได้ง่ายขึ้นมาก (9 ตัวอักษร):

3 แนวตั้ง: ไลบรารีเข้ารหัสลับที่ OpenVPN พึ่งพาสำหรับอัลกอริทึมไซเฟอร์ (9 ตัวอักษร):

5 แนวตั้ง: พื้นที่ประมวลผลที่ OpenVPN ทำงาน ทำให้เกิดภาระการสลับบริบท (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช	มี	พี	ฟ	บ	า	า	เ	ห	นี	า	ม	กี	จ	า
า	รี	ดี	ต	ว	ย	ง	ค	ก	ค	พี้	จ	น	ตี	ว
ร	ตี	ยู	ว	า	ล	ล	อ	ด	า	น	อ	ย	ซ	ฟ
ด	ก	พี	ก	ล	ม	า	ร์	ป	อ	ที่	อ	ม	มี	า
รั	ล	ซี	ล	ป	โ	จ	เ	า	นี	ผู้	กี	พ	เ	ร
ด	ง	ที	า	ซ	อ	า	น	า	ลี	ใ	จ	ดี	อ	า
ทั	น	ล	ผ	ดี	เ	ซ	ล	ไ	ก	ช้	ด	า	ส	ต
ะ	า	จ	า	ค	พ	ก	ดี	ว	า	ซ	ว	ก	เ	ด
ก	กี	ด	ท	ผ	น	ฟ	ซ	ร์	มี	ม	อ	ต	อ	ฟ
ด	ร	ดี	า	ท	วี	คู่	า	ก	ส	ท	ข	ข	ส	า
ค้	น	ก	า	ล	พี	กุ	า	า	ม	ร	มี	า	แ	ร
โ	ช	ก	ด	ง	เ	ญ	น	ร์	ร	ต	สี	ย	อ	ข
มี	ดี	ด	ด	ว	อ็	แ	บ	ด	ฟ	อ	า	ร	ล	ห
ห	รี	น	ผ	นี	น	จ	ม	ผ	ดี	ข	กี	ส	บ	ลี
ง	ด	ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ

รายการคำศัพท์

ไวร์การ์ด โอเพนวีพีเอ็น เคอร์เนล พื้นที่ผู้ใช้ โค้ดกะทัดรัด เอสเอสแอล คู่กุญแจ ทีซีพียูดีพี

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. ไวร์การ์ด
B. โอเพนวีพีเอ็น
C. เคอร์เนล
D. พื้นที่ผู้ใช้
E. โค้ดกะทัดรัด
F. เอสเอสแอล
G. คู่กุญแจ
H. ทีซีพียูดีพี

คำนิยามและช่องจับคู่
1. ไลบรารีเข้ารหัสลับที่ OpenVPN พึ่งพาสำหรับอัลกอริทึมไซเฟอร์
2. พื้นที่ประมวลผลของระบบปฏิบัติการที่ WireGuard ทำงานเพื่อความเร็ว
3. โปรโตคอลรุ่นเก่าที่แข็งแกร่งซึ่งใช้ฐานโค้ดการกำหนดค่าขนาดใหญ่และซับซ้อน
4. โทเค็นอสมมาตรที่ WireGuard ใช้ยืนยันการเชื่อมต่อของเพียร์
5. โปรโตคอลขนส่งที่ OpenVPN รองรับ ส่วน WireGuard ทำงานบน UDP เท่านั้น
6. ขนาดกะทัดรัดของฐานโค้ด WireGuard ทำให้ตรวจสอบได้ง่ายขึ้นมาก
7. โปรโตคอล VPN สมัยใหม่ที่ออกแบบเพื่อความเร็วสูงและการตรวจสอบโค้ดที่ง่าย
8. พื้นที่ประมวลผลที่ OpenVPN ทำงาน ทำให้เกิดภาระการสลับบริบท

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของ VPN เขียนคำตอบของคุณในช่องกรอกที่กรอกได้

1. ก ร์ ไ า ด ร์ ว
2. เ อ ล น เ ร์ ค
3. โ ท้ ะ ค้ ด ด ก ร้ ด
4. ญ จ แ คู่ กุ
5. เ ว็ น อ พ พี น โ อ็ เ
6. ใ ผู้ พื้ ที่ ซ้ น
7. ส เ อ ล แ เ อ อ ส
8. พี พี ที ดี ยู ซี

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	เหตุผลที่ควรเลือก **WireGuard**			
2	คำมั่นสัญญาที่ผู้ให้บริการ **VPN** ที่ดีให้ไว้			
3	เหตุผลที่ควรเลือก **OpenVPN**			
4	เหตุผลที่ควรใช้ **VPN** ขณะเดินทาง			
5	สิ่งที่ผู้ให้บริการอินเทอร์เน็ตของคุณมองเห็นได้			
6	วิธีสังเกตเครือข่าย **Wi-Fi** ปลอม			
7	ความเชื่อผิด ๆ เกี่ยวกับ **VPN**			
8	สถานที่ที่คุณจะใช้ **VPN**			
9	สิ่งที่รวดเร็วในชีวิตประจำวัน			
10	สิ่งที่ **VPN** ปกป้องคุณไม่ได้			
11	สิ่งที่ทำให้ตรวจสอบโค้ดได้ง่ายขึ้น			
12	สิ่งที่ **VPN** ซ่อนได้			
13	ความแตกต่างระหว่าง **WireGuard** กับ **OpenVPN**			
14	คำที่เกี่ยวข้องกับความเป็นส่วนตัว			
15	ชื่อการเข้ารหัสที่คุณรู้จัก			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

ซาราห์ (นักเรียนร้านกาแฟ)

👷 "สวัสดี! ฉันอยู่ที่ร้านกาแฟและใช้ Wi-Fi ของร้าน แอป VPN ของฉันให้เลือก WireGuard หรือ OpenVPN วิดีโอคอลของฉันหลุดบ่อยเมื่อเดินสลับระหว่างเครือข่ายของร้านกับฮอตสปอตจากมือถือ ฉันควรเลือกโปรโตคอลใด และทำไมโปรโตคอลนั้นจึงรับมือกับการสลับได้ดีกว่า?"

อเล็กซ์ (นักเรียนนักท่องเที่ยว)

👷 "ฉันอยู่ต่างประเทศบนเครือข่ายของโรงแรมที่ดูเหมือนจะบล็อกทราฟฟิก VPN ส่วนใหญ่ WireGuard เชื่อมต่อไม่ได้เลย แต่ฉันต้องเข้าถึงทรัพยากรของโรงเรียนที่บ้าน อะไรน่าจะถูกบล็อกอยู่ และ OpenVPN จะช่วยให้ฉันผ่านไปได้อย่างไร?"

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

เพื่อให้การฝึกอบรมการตรวจสอบโปรโตคอลของคุณเสร็จสมบูรณ์ ให้ถอดรหัสข้อความที่ซ่อนอยู่นี้เกี่ยวกับการทำงานในเคอร์เนลสเปซ

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

45	48	27	57	1	35	20		20	64	39	34		45	55	59	33	7	4	67

23	52	63	57	35	62	39	1	39	63	49

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: เหตุใดโปรโตคอลจึงสำคัญ?

โปรโตคอลกำหนดวิธีที่ VPN ของคุณสร้างอุโมงค์ การเข้ารหัสแบบใดที่ปกป้องข้อมูลของคุณ และความเร็วในการเชื่อมต่อและเชื่อมต่อใหม่ WireGuard และ OpenVPN เป็นสองโปรโตคอลโอเพนซอร์สที่แอป VPN ส่วนใหญ่มีให้ และแลกเปลี่ยนระหว่างความเรียบง่าย ความเร็ว และความยืดหยุ่นในการตั้งค่าต่างกัน

Q3: ตัวใดตัวหนึ่งเป็นส่วนตัวกว่าอีกตัวหรือไม่?

ไม่มีโปรโตคอลใดทำให้คุณเป็นนิรนามได้ ทั้งสองเข้ารหัสการรับส่งข้อมูลในอุโมงค์ด้วยรหัสที่แข็งแกร่ง ความเป็นส่วนตัวของคุณขึ้นอยู่กับสิ่งที่ผู้ให้บริการ VPN บันทึกและวิธีที่จัดการคีย์ บัญชี และเซิร์ฟเวอร์เป็นหลัก

Q4: VPN จะทำให้ความเร็วอินเทอร์เน็ตของฉันช้าลงหรือไม่?

ได้ เล็กน้อย กระบวนการเข้ารหัสและระยะทางกายภาพไปยังเซิร์ฟเวอร์ VPN เพิ่มความหน่วงและภาระงาน ผลกระทบแตกต่างกันตามผู้ให้บริการ โปรโตคอล ระยะทางเซิร์ฟเวอร์ อุปกรณ์ และสภาพเครือข่าย

Q5: ทั้งสองเป็นโอเพนซอร์สหรือไม่?

ได้ ทั้ง WireGuard และ OpenVPN รุ่นคอมมิวนิตีเผยแพร่ซอร์สโค้ด นักวิจัยอิสระจึงตรวจสอบได้ โค้ดขนาดเล็กของ WireGuard ทำให้ตรวจสอบทั้งหมดได้เร็วกว่ามาก

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดที่ผู้สนใจมีเกี่ยวกับการใช้เครือข่ายส่วนตัวเสมือน

Q6: ตัวไหนเร็วกว่ากัน?

โดยปกติ WireGuard เร็วกว่า: ทำงานในเคอร์เนล ใช้การเข้ารหัส ChaCha20-Poly1305 ที่เบา และแฮนด์เชคเสร็จเร็ว ส่วน OpenVPN มีภาระมากกว่า แต่ความเร็วจริงยังขึ้นอยู่กับโหลดของเซิร์ฟเวอร์และระยะทางด้วย

Q7: ทั้งสองทำงานผ่าน TCP และ UDP ได้หรือไม่?

ไม่ OpenVPN ทำงานผ่าน UDP หรือ TCP ได้ และโหมด TCP ช่วยในเครือข่ายที่บล็อก UDP ส่วน WireGuard ส่งแพ็กเก็ตผ่าน UDP เท่านั้น จึงอาจใช้งานไม่ได้บนเครือข่ายที่อนุญาตเฉพาะ TCP [4]

Q8: ฉันเลือก VPN ที่ดีที่สุดได้อย่างไร?

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

Q9: ฉันใช้ WireGuard และ OpenVPN บนโทรศัพท์ได้หรือไม่?

ได้ WireGuard ใช้ได้หลายแพลตฟอร์ม มีแอปสำหรับ Windows, macOS, Linux, iOS และ Android และมีไคลเอนต์ OpenVPN สำหรับระบบเดียวกัน แอป VPN ส่วนใหญ่ให้เลือกใช้ได้ทั้งสองแบบ [1]

Q10: ทำไม WireGuard จึงมีขนาดเล็กมาก?

WireGuard รองรับชุดรหัสเข้ารหัสสมัยใหม่ชุดเดียวที่ตายตัวแทนที่จะมีตัวเลือกมากมาย การใช้งานบน Linux ใช้โค้ดไม่ถึง 4,000 บรรทัด ซึ่งตรวจสอบได้ง่ายกว่าโค้ดของ VPN ที่ใหญ่กว่า [3]

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: WireGuard ใช้ชุดรหัส (cipher) อะไรบ้าง?

WireGuard ใช้ ChaCha20 ร่วมกับ Poly1305 สำหรับการเข้ารหัส Curve25519 สำหรับการแลกเปลี่ยนกุญแจ BLAKE2s สำหรับการแฮช และกรอบงาน Noise สำหรับแฮนด์เชค ไม่มีการเจรจารหัสเข้ารหัส ผู้ใช้จึงเลือกตัวเลือกที่อ่อนแอไม่ได้ [2]

Q3: OpenVPN ใช้ชุดรหัสและไลบรารีใดได้บ้าง?

OpenVPN ผสานกับไลบรารี OpenSSL อย่างแน่นแฟ้นและใช้ TLS แลกเปลี่ยนกุญแจ ผู้ดูแลระบบเลือกรหัสของช่องข้อมูลเช่น AES-256-GCM ได้ ซึ่งเพิ่มความยืดหยุ่นแต่ก็เปิดช่องให้ตั้งค่าที่อ่อนแอได้ [4]

Q4: แต่ละโปรโตคอลพิสูจน์ตัวตนของเพียร์อย่างไร?

เพียร์ของ WireGuard ระบุกันและกันด้วยกุญแจสาธารณะแบบคงที่ คล้ายกับการแลกเปลี่ยนกุญแจ SSH และกุญแจแต่ละอันจะจับคู่กับ IP ของอุโมงค์ที่อนุญาต ส่วน OpenVPN มักอาศัยผู้ออกใบรับรองพร้อมใบรับรอง X.509 ซึ่งมักใช้ร่วมกับชื่อผู้ใช้และรหัสผ่าน

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: จะเกิดอะไรขึ้นเมื่อฉันสลับจาก Wi-Fi ไปใช้เครือข่ายมือถือ?

WireGuard เป็นแบบไร้การเชื่อมต่อ (connectionless): ส่งแพ็กเก็ตจากที่อยู่ใหม่และอุโมงค์ทำงานต่อได้หลังแฮนด์เชคสั้นๆ ส่วน OpenVPN เก็บสถานะเซสชัน ดังนั้นการเปลี่ยนเครือข่ายอาจต้องเชื่อมต่อใหม่ซึ่งใช้เวลานานกว่าเล็กน้อย

Q7: Forward Secrecy (Perfect Forward Secrecy) ทำงานอย่างไร?

PFS ทำให้มีการสร้างกุญแจเข้ารหัสชั่วคราวที่ไม่ซ้ำกันสำหรับทุกเซสชัน แม้กุญแจส่วนตัวจะถูกบุกรุกในอนาคต ก็ไม่สามารถใช้ถอดรหัสเซสชันในอดีตหรืออนาคตได้ เพราะแต่ละเซสชันใช้กุญแจที่เป็นอิสระต่อกัน

Q8: OpenVPN ยังเป็นตัวเลือกที่ดีอยู่หรือไม่หาก WireGuard เร็วกว่า?

ได้ OpenVPN มีความสมบูรณ์และใช้งานแพร่หลาย ทำงานบน TCP เมื่อ UDP ถูกบล็อก และรองรับการติดตั้งองค์กรที่ใช้ใบรับรอง ผู้ให้บริการหลายรายมีทั้งสองโปรโตคอลเพื่อให้ผู้ใช้สลับได้หากโปรโตคอลหนึ่งถูกบล็อกหรือช้า

Q9: ใช้พอร์ตใดบ้าง?

พอร์ตมาตรฐานของ OpenVPN คือ 1194 แต่ย้ายไปใช้พอร์ต UDP หรือ TCP ใดก็ได้ รวมถึง 443 ส่วน WireGuard รับฟังที่พอร์ต UDP ที่กำหนดในการตั้งค่า โดย 51820 คือพอร์ตที่ใช้ในตัวอย่างทางการ

Q10: โปรโตคอลใดตั้งค่าด้วยตนเองได้ง่ายกว่า?

โดยปกติ WireGuard ง่ายกว่า: สร้างคู่กุญแจ แลกเปลี่ยนกุญแจสาธารณะ และระบุรายการ IP ที่อนุญาต ส่วน OpenVPN ต้องใช้ใบรับรอง CA และตัวเลือกมากกว่า แม้โปรไฟล์ .ovpn จะรวมสิ่งเหล่านี้ไว้ในไฟล์เดียวก็ตาม

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. ทรานสปอร์ตสองแบบ

OpenVPN ส่งอุโมงค์ผ่าน UDP หรือ TCP ได้ และในโหมด TLS ช่องควบคุมกับช่องข้อมูลใช้พอร์ตเดียวร่วมกัน [4]

3. การปฏิวัติ WireGuard

WireGuard มีโค้ดที่เรียบง่ายมากซึ่งออกแบบมาเพื่อประสิทธิภาพ ทำให้ตรวจสอบช่องโหว่ด้านความปลอดภัยได้ง่ายกว่าโปรโตคอลแบบดั้งเดิม [3]

4. การเข้ารหัสลับสมัยใหม่

WireGuard รวม ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 และ HKDF ไว้ภายในกรอบงานโปรโตคอล Noise โดยไม่มีตัวเลือกรหัสเข้ารหัสให้ผู้ใช้เลือกผิดพลาด [2]

5. OPENSSL ภายใน OPENVPN

OpenVPN ผสานกับไลบรารี OpenSSL อย่างแน่นแฟ้นและได้ความสามารถด้านการเข้ารหัสหลายอย่างจากไลบรารีนั้น รวมถึง TLS ที่ใช้แลกเปลี่ยนกุญแจ [4]

6. การตรวจสอบแพ็กเก็ตเชิงลึก

การตรวจสอบแพ็กเก็ตเชิงลึก (DPI) ตรวจสอบเนื้อหาแพ็กเก็ตและรูปแบบทราฟฟิก ไม่ใช่แค่ส่วนหัว และไฟร์วอลล์บางตัวใช้ DPI เพื่อตรวจจับและบล็อกโปรโตคอล VPN ทั่วไป

7. คีย์แบบ SSH

การเชื่อมต่อ WireGuard ตั้งค่าโดยการแลกเปลี่ยนกุญแจสาธารณะแบบง่าย ซึ่งคล้ายกับการแลกเปลี่ยนกุญแจ SSH โดยไม่ต้องมีผู้ออกใบรับรอง [1]

8. ข้ามแพลตฟอร์ม

WireGuard เปิดตัวครั้งแรกสำหรับเคอร์เนล Linux และปัจจุบันมีให้ใช้บน Windows, macOS, BSD, iOS และ Android ดังนั้นโปรโตคอลเดียวกันจึงใช้ได้กับอุปกรณ์ส่วนใหญ่ [1]

9. FORWARD SECRECY

WireGuard ทำแฮนด์เชค Noise_IK ซ้ำทุกไม่กี่นาทีเพื่อหมุนเวียนกุญแจเซสชันแบบสมมาตร ทำให้มี perfect forward secrecy แม้กุญแจระยะยาวจะรั่วไหลในภายหลัง [2]

10. อินเทอร์เฟซ TUN/TAP

OpenVPN ออกแบบมาให้ทำงานกับอินเทอร์เฟซเครือข่ายเสมือน TUN/TAP ซึ่งมีบนเกือบทุกแพลตฟอร์มและใช้ส่งแพ็กเก็ตของอุโมงค์ [4]

แหล่งอ้างอิงทางเทคนิค

สิ่งพิมพ์ที่อ้างอิง ข้อกำหนดด้านการเข้ารหัส และมาตรฐานเอกสารทางการที่ใช้ตลอดทั้งใบงานนี้

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

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

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

[3] 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/

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

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

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

เฉลย: การเปรียบเทียบโปรโตคอล WireGuard และ OpenVPN ขนาดโค้ดเบส ความเร็ว และมาตรฐานการเข้ารหัส

1 **ขนาดโค้ดของ WireGuard** โปรโตคอล — **คำตอบที่ถูกต้อง: D**

หมายเหตุสำหรับผู้สอน

WireGuard กะทัดรัดมาก ทำงานด้วยโค้ดประมาณ 4,000 บรรทัด ซึ่งช่วยให้พื้นผิวการโจมตีเล็กและตรวจสอบได้ง่ายขึ้น การอ้างอิง: WireGuard Project.

2 **ความเร็วระดับเคอร์เนลสเปซ** เวลาแฝง — **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

ด้วยการทำงานโดยตรงในพื้นที่เคอร์เนล WireGuard จึงหลีกเลี่ยงภาระจากการสลับบริบท ทำให้มีอัตราการส่งผ่านข้อมูลสูง อ้างอิง: WireGuard Project.

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

หมายเหตุสำหรับผู้สอน

OpenVPN ผสานรวมกับ OpenSSL อย่างแน่นหนา ซึ่งจัดหาชุดรหัสลับ เช่น AES-GCM และทำให้ปรับแต่งได้สูงแต่ซับซ้อนกว่า

4 **ประสิทธิภาพของโปรโตคอล** การควบคุมการกำหนดเส้นทาง — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

WireGuard สร้างแฮนด์เชคได้ในเวลาไม่กี่มิลลิวินาทีและตอบสนองทันทีเมื่อเครือข่ายโรมมิ่ง (เช่น สลับจาก Wi-Fi ไปเครือข่ายมือถือ) การอ้างอิง: Microsoft Native Gateway, Apple Support. [3]

5 **การเข้ารหัสแบบอสมมาตร** ความเป็นส่วนตัว — **คำตอบที่ถูกต้อง: C**

หมายเหตุสำหรับผู้สอน

WireGuard ใช้ Cryptokey Routing ซึ่งเชื่อมโยงกุญแจสาธารณะกับที่อยู่ IP ของอุโมงค์ที่อนุญาต คล้ายกับการตั้งค่า SSH การอ้างอิง: WireGuard Project.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

การพัฒนา WireGuard บน Linux มีไม่ถึง 4,000 บรรทัด ทีมความปลอดภัยจึงตรวจสอบได้เร็วกว่าโค้ดเบส VPN ที่ใหญ่กว่ามาก เช่น OpenVPN

7 **ความหน่วงในยูสเซอร์สเปซ** ความเร็ว คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

OpenVPN ทำงานในพื้นที่ผู้ใช้ โดยส่งแพ็กเก็ตไปมากับอินเทอร์เฟซเสมือนของเคอร์เนล ซึ่งเพิ่มภาระการสลับบริบท (เว้นแต่ใช้การถ่ายโอนภาระไปยังเคอร์เนลเช่น OpenVPN DCO) อ้างอิง: DD-WRT custom firmware.

8 **การกำหนดค่า OpenVPN** ความเสี่ยงจากการดักจับแพ็กเก็ต คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

OpenVPN รองรับการทำงานบน TCP (เพื่อความน่าเชื่อถือ/ข้ามไฟร์วอลล์) หรือ UDP (เพื่อความเร็ว) จึงเข้ากันได้กับไฟร์วอลล์องค์กรที่ซับซ้อน อ้างอิง: IETF Cryptographic Protocols.

9 **การเข้ารหัสสมัยใหม่** ไฟร์วอลล์ คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

WireGuard หิ้งรหัสเข้ารหัสรุ่นเก่าและใช้พื้นฐานการเข้ารหัสที่ทันสมัยและปลอดภัย เช่น ChaCha20 และ Poly1305 ซึ่งทำงานได้เร็วบน CPU มือถือ การอ้างอิง: WireGuard Project.

10 **การทำให้คู่คีย์ง่ายขึ้น** ไม่เก็บล็อก คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

WireGuard ไม่ใช้ใบรับรองหรือลำดับชั้น CA ที่ซับซ้อน แต่อาศัยคู่กุญแจสาธารณะ/ส่วนตัวแบบง่ายที่แลกเปลี่ยนกันระหว่างเพียร์ การอ้างอิง: WireGuard Project.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

G 1. WireGuard	H 2. OpenVPN	E 3. เคอร์เนลสเปซ	A 4. ยูสเซอร์สเปซ
B 5. 4,000 บรรทัด	C 6. OpenSSL	F 7. คู่คีย์	D 8. TCP/UDP

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ไวร์การ์ด	2 โอเพนวีพีเอ็น	3 เคอร์เนล	4 พื้นที่ผู้ใช้
5 คู่กุญแจ	6 การตรวจสอบได้		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 F – เอสเอสแอล	2 C – เคอร์เนล	3 B – โอเพนวีพีเอ็น	4 G – คู่กุญแจ
5 H – ทีซีพียูดีพี	6 E – โค้ดกะทัดรัด	7 A – ไวร์การ์ด	8 D – พื้นที่ผู้ใช้

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย WireGuard OpenVPN และ เคอร์เนลสเปซ ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

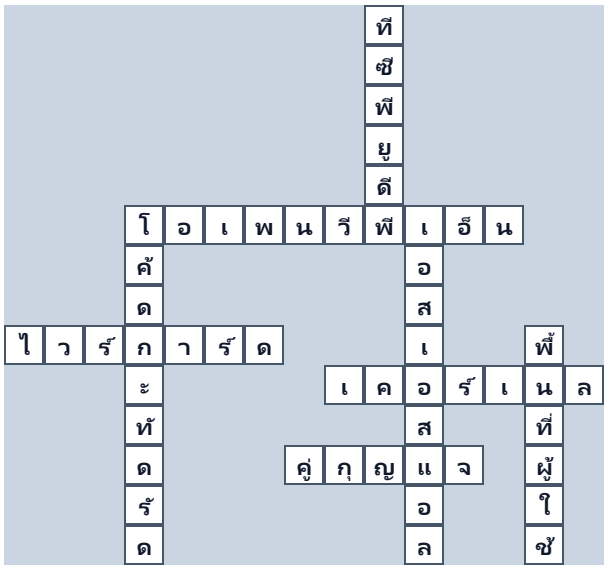
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	พี	ฟ	บ	า	า	เ	ห	นี	า	ม	กี	จ	า
า	รี	ดี	ต	ว	ย	ง	ค	ก	ค	พื้	จ	น	ตี	ว
ร	ตี	ยู	ว	า	ล	ล	อ	ด	า	น	อ	ย	ช	ฟ
ด	ก	พี	ก	ล	ม	า	ร์	ป	อ	ที่	อ	ม	มี	า
รั	ล	ซี	ล	ป	โ	จ	เ	า	นี	ผู้	กี	พ	เ	ร
ด	ง	ที	า	ช	อ	า	น	า	ลี	ใ	จ	ดี	อ	า
ท้	น	ล	ผ	ดี	เ	ช	ล	ไ	ก	ช้	ด	า	ส	ต
ะ	า	จ	า	ค	พ	ก	ดี	ว	า	ช	ว	ก	เ	ด
ก	กี	ด	ท	ผ	น	ฟ	ช	ร์	มี	ม	อ	ต	อ	ฟ
ด	ร	ดี	า	ท	วี	คู่	า	ก	ส	ท	ข	ข	ส	า
ค้	น	ก	า	ล	พี	กุ	า	า	ม	ร	มี	า	แ	ร
โ	ช	ก	ด	ง	เ	ญ	น	ร์	ร	ต	สี	ย	อ	ข
มี	ดี	ด	ด	ว	อิ	แ	บ	ด	ฟ	อ	า	ร	ล	ห
ห	รี	น	ผ	นี	น	จ	ม	ผ	ดี	ข	กี	ส	บ	ลี
ง	ด	ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: โอเพนวีพีเอ็น โปรโตคอลรุ่นเก่าที่แข็งแกร่งซึ่งใช้ฐานโค้ดการกำหนดค่าขนาดใหญ่และซับซ้อน (10 ตัวอักษร)

4 แนวนอน: ไวร์การ์ด โปรโตคอล VPN สมัยใหม่ที่ออกแบบเพื่อความเร็วสูงและการตรวจสอบโค้ดที่ง่าย (7 ตัวอักษร)

6 แนวนอน: เคอร์เนล พื้นที่ประมวลผลของระบบปฏิบัติการที่ WireGuard ทำงานเพื่อความเร็ว (7 ตัวอักษร)

7 แนวนอน: คู่กุญแจ โทเคนอสมมาตรที่ WireGuard ใช้ยืนยันการเชื่อมต่อของเพียร์ (5 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: ทีซีพียูดีพี โปรโตคอลขนส่งที่ OpenVPN รองรับ ส่วน WireGuard ทำงานบน UDP เท่านั้น (6 ตัวอักษร)

2 แนวตั้ง: โค้ดกะทัดรัด ขนาดกะทัดรัดของฐานโค้ด WireGuard ทำให้ตรวจสอบได้ง่ายขึ้นมาก (9 ตัวอักษร)

3 แนวตั้ง: เอสเอสแอล ไลบรารีเข้ารหัสลับที่ OpenVPN พึ่งพาสำหรับอัลกอริทึมไซเฟอร์ (9 ตัวอักษร)

5 แนวตั้ง: พื้นที่ผู้ใช้ พื้นที่ประมวลผลที่ OpenVPN ทำงาน ทำให้เกิดภาระการสลับบริบท (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. กร์ไาดร์ว — ไวร์การ์ด
2. เอลนเร์ค — เคอร์เนล
3. โท้ะค้ดดกรัด — โค้ดกะทัดรัด
4. ญจแคู่กุ — คู่กุญแจ
5. เวินอพพีนโอ็เ — โอเพนวีพีเอ็น
6. ใผู้พื้ที่ซ้น — พื้นที่ผู้ใช้
7. สเอลแเออส — เอสเอสแอล
8. พีพีทีดียูซี — ทีซีพียูดีพี

เฉลยภารกิจรหัสลับ

"อัปเกรด ด้วย อุโมงค์ ที่เร็วกว่า"

เฉลยกรณีศึกษา

A สถานการณ์ A: การเลือกโปรโตคอล

การดักจับแพ็กเก็ตและการเข้ารหัส ความกังวลของซาราห์

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- คำแนะนำ: WireGuard ดีไซน์ที่เบาและไม่ต้องคงการเชื่อมต่อทำให้อุโมงค์กลับมาทำงานได้เร็วเมื่อเครือข่ายของเธอเปลี่ยน และ ChaCha20-Poly1305 ช่วยให้การเข้ารหัสทำงานได้เร็ว
- ความปลอดภัย: ทั้งสองโปรโตคอลเข้ารหัสทราฟฟิกของเธอบน Wi-Fi ของคาเฟ่ ดังนั้นไม่ว่าเลือกแบบใดก็ช่วยปกป้องการเข้าสู่ระบบของเธอได้เมื่อตั้งค่าอย่างถูกต้อง การเลือกส่งผลหลักต่อความเร็วและความเสถียร

B สถานการณ์ B: การหลีกเลี่ยงการบล็อก VPN

การบล็อกตามภูมิศาสตร์และ IP ปัญหาของอเล็กซ์

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- เหตุผลที่ถูกบล็อก: WireGuard ใช้ UDP เท่านั้น และไฟร์วอลล์ของโรงแรมน่าจะบล็อก UDP หรือรู้จำแพ็กเก็ต WireGuard ผ่านการกรองหรือการตรวจสอบแพ็กเก็ตเชิงลึก
- OpenVPN ช่วยได้อย่างไร: ทำงานบน TCP ได้ รวมถึงพอร์ต 443 ที่ HTTPS ใช้ ซึ่งไฟร์วอลล์ของโรงแรมแทบไม่บล็อกโดยตรงเพราะการท่องเว็บต้องพึ่งพอร์ตนี้