ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

ความปลอดภัยของ Surfshark

การตรวจสอบฟีเจอร์ความปลอดภัยของ Surfshark รวมถึงการบล็อกโฆษณา CleanWeb การกำหนดเส้นทางไดนามิก MultiHop สถาปัตยกรรม Nexus SDN ฝูงเซิร์ฟเวอร์ที่ใช้เฉพาะ RAM และโหมด Camouflage

ภาพรวมการเรียนรู้เรื่องความปลอดภัยของ SURFSHARK

ผู้เรียน
สถานะนักเรียน
สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย
สถานะการเชื่อมต่อ
การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน
การป้องกันการรั่วไหล
การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับสถาปัตยกรรมความปลอดภัยของ Surfshark คุณจะได้ศึกษาฮาร์ดแวร์เซิร์ฟเวอร์แบบ RAM เท่านั้น การหมุนเวียน IP แบบไดนามิกของ Nexus SDN ตัวบล็อกโฆษณา CleanWeb และการกำหนดเส้นทาง MultiHop

จุดตรวจสอบของใบงาน

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

เปิดคู่มือ VPN ที่ดีที่สุดของ VPN.com

URL: https://www.vpn.com/th/vpn/surfshark/khwam-plodphai/

เส้นทางการเรียนรู้ความปลอดภัยของ Surfshark ของคุณ

- วิเคราะห์สถาปัตยกรรมทางเทคนิคและกฎการกำหนดค่าของความปลอดภัยของ Surfshark
- ตั้งค่าไคลเอนต์เพื่อป้องกันการรั่วไหลของทราฟฟิก IP, DNS และ WebRTC
- เปรียบเทียบราคากำหนดเอง ช่วงทดลอง และฟีเจอร์ด้านประสิทธิภาพกับรุ่นมาตรฐาน

คำชี้แจงคู่มือความปลอดภัยของ SURFSHARK

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ โครงสร้างพื้นฐานที่ใช้ RAM เท่านั้น Nexus SDN และ CleanWeb ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

กลุ่มเซิร์ฟเวอร์แบบ RAM-only, Nexus SDN และสถาปัตยกรรม CleanWeb (บทนำ)

Surfshark ปกป้องความเป็นส่วนตัวของผู้ใช้ด้วยกลุ่มเซิร์ฟเวอร์แบบ RAM เท่านั้น เครือข่ายที่กำหนดโดยซอฟต์แวร์ Nexus พร้อม IP Rotator การบล็อกโฆษณา CleanWeb และเส้นทางเข้ารหัสแบบ Dynamic MultiHop

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. ตัวบล็อกโฆษณาและมัลแวร์ในตัวของ Surfshark ชื่ออะไร?
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. Surfshark ใช้สถาปัตยกรรมฮาร์ดแวร์แบบใดในเซิร์ฟเวอร์ทั้งหมด?
   - A) ฮาร์ดดิสก์ไดรฟ์
   - B) RAM เท่านั้น 100%
   - C) การจัดเก็บด้วยแสง
   - D) เทปแม่เหล็ก

3. ฟีเจอร์ใดที่กำหนดเส้นทางทราฟฟิกผ่านเซิร์ฟเวอร์ VPN สองตัวที่แยกจากกัน?
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) เครือข่าย Nexus
   - D) IP แบบคงที่

4. ฟีเจอร์การพรางตัวใดที่ปลอมทราฟฟิก VPN ให้เหมือนข้อมูลเว็บปกติ?
   - A) Kill Switch
   - B) โหมด Camouflage
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. เครื่องมือ Surfshark Bypasser ทำหน้าที่อะไร?
   - A) Speed Booster
   - B) Split Tunneling
   - C) ตัวจัดการรหัสผ่าน
   - D) ตัวแปลง DNS

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. เซิร์ฟเวอร์แบบ RAM-only ลบข้อมูลการทำงานทั้งหมดทันทีเมื่อเซิร์ฟเวอร์รีบูต

○ จริง ○ เท็จ

7 คำถาม 7

7. โหมด Camouflage ป้องกันไม่ให้ ISP ตรวจพบว่าคุณใช้ VPN

○ จริง ○ เท็จ

8 คำถาม 8

8. CleanWeb 2.0 ทำงานภายในส่วนขยายเบราว์เซอร์เพื่อบล็อกป๊อปอัปขอความยินยอมเรื่องคุกกี้

○ จริง ○ เท็จ

9 คำถาม 9

9. Surfshark เก็บเวลาการเชื่อมต่อชั่วคราวและบันทึกปริมาณการใช้แบนด์วิดท์

○ จริง ○ เท็จ

10 คำถาม 10

10. เครือข่าย Nexus หมุนเวียนที่อยู่ IP ของผู้ใช้เป็นระยะโดยไม่ตัดการเชื่อมต่อ

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. โฆษณาเว็บที่น่ารำคาญ สคริปต์ติดตาม และลิงก์ฟิชชิงถูกบล็อกโดยตัวกรอง _____
2. กิจกรรมของผู้ใช้ไม่เหลือร่องรอยทางนิติวิทยาศาสตร์เพราะเซิร์ฟเวอร์ทำงานในหน่วยความจำแบบ _____
3. การส่งข้อมูลผ่านเซิร์ฟเวอร์ที่เข้ารหัสสองฮอปแยกกันทำได้ด้วยอุโมงค์แบบ _____
4. เพื่อซ่อนการใช้ VPN จากผู้ให้บริการอินเทอร์เน็ต ผู้ใช้เปิดโหมด _____
5. การอนุญาตให้แอปธนาคารข้ามอุโมงค์ VPN จัดการด้วยการตั้งค่า _____
6. สถาปัตยกรรม SDN รุ่นใหม่ที่เชื่อมกลุ่มเซิร์ฟเวอร์คือระบบ _____

คลังคำศัพท์

คลีนเว็บ | คาโมฟลาจ | คิลสวิตช์ | เน็กซัส | บายพาส | มัลติฮอป | แรมล้วน | ไวร์การ์ด

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่อง VPN และเครือข่าย

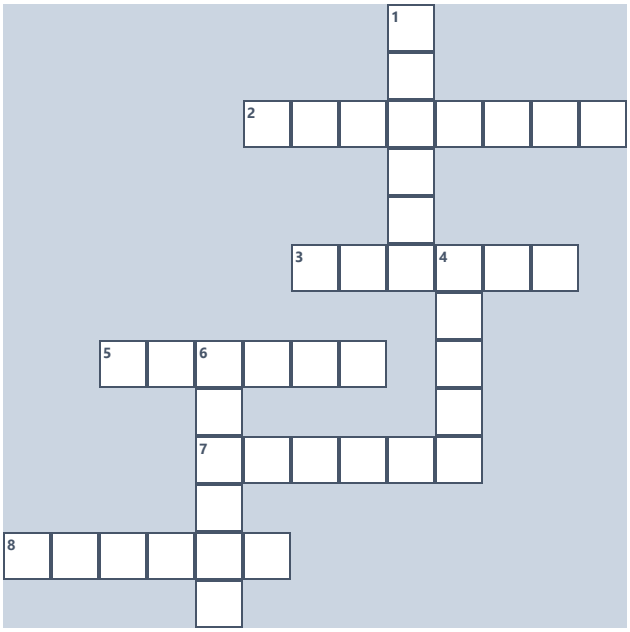
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. คลีนเว็บ**	**A**	ฟีเจอร์ความปลอดภัยอัตโนมัติที่บล็อกทราฟฟิกเครือข่ายเมื่อ VPN หลุด
☐	**2. แรมล้วน**	**B**	ฟังก์ชัน Split-tunneling ที่ให้แอปที่เลือกข้าม VPN ได้
☐	**3. มัลติฮอป**	**C**	ตัวกรองขั้นสูงที่บล็อกโฆษณา มัลแวร์ และแบนเนอร์ขอความยินยอมคุกกี้
☐	**4. คาโมฟลาจ**	**D**	ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ล้างข้อมูลทั้งหมดทุกครั้งที่ปิดและเปิดเครื่อง
☐	**5. บายพาส**	**E**	ฟีเจอร์ที่เปลี่ยนที่อยู่ IP ภายนอกของคุณเป็นประจำโดยไม่ขัดจังหวะอุโมงค์
☐	**6. คิลสวิตช์**	**F**	เทคโนโลยีอำพรางที่ซ่อนลายเซ็นของ VPN ให้ดูเหมือนทราฟฟิก HTTPS ปกติ
☐	**7. เน็กซัส**	**G**	ฟีเจอร์การกำหนดเส้นทางแบบ Double VPN ที่เข้ารหัสทราฟฟิกผ่านโหนดเซิร์ฟเวอร์สองโหนดที่แตกต่างกัน
☐	**8. การหมุนเวียน**	**H**	เครือข่ายที่กำหนดด้วยซอฟต์แวร์แบบกรรมสิทธิ์ที่เชื่อมเซิร์ฟเวอร์ทั้งหมดเป็นเมชเดียวกัน

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. เทคโนโลยีพรางที่ซ่อนลายเซ็น VPN ให้เหมือนทราฟฟิก HTTPS ปกติ (8)

3. ตัวกรองชั้นสูงที่บล็อกโฆษณา มัลแวร์ และแบนเนอร์ขอความยินยอมคุกกี้ (6)

5. ฟีเจอร์ความปลอดภัยอัตโนมัติที่บล็อกทราฟฟิกเครือข่ายเมื่อ VPN หลุด (6)

7. ฟังก์ชันแยกอุโมงค์ที่ให้บางแอปข้าม VPN ได้ (6)

8. ฟีเจอร์เส้นทาง VPN สองชั้นที่เข้ารหัสทราฟฟิกข้ามโหนดเซิร์ฟเวอร์สองตัวที่ต่างกัน (6)

แนวตั้ง

1. ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ล้างข้อมูลทั้งหมดทุกครั้งที่ปิดเปิดเครื่อง (6)

4. เครือข่ายกำหนดด้วยซอฟต์แวร์เฉพาะที่เชื่อมเซิร์ฟเวอร์ทั้งหมดเป็นเมชเดียว (5)

6. ฟีเจอร์ที่เปลี่ยนไอพีภายนอกของคุณเป็นประจำโดยไม่ขัดจังหวะอุโมงค์ (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: เทคโนโลยีพรางที่ซ่อนลายเซ็น VPN ให้เหมือนทราฟฟิก HTTPS ปกติ (8 ตัวอักษร):

3 แนวนอน: ตัวกรองขั้นสูงที่บล็อกโฆษณา มัลแวร์ และแบนเนอร์ขอความยินยอมคุกกี้ (6 ตัวอักษร):

5 แนวนอน: ฟีเจอร์ความปลอดภัยอัตโนมัติที่บล็อกทราฟฟิกเครือข่ายเมื่อ VPN หลุด (6 ตัวอักษร):

7 แนวนอน: ฟังก์ชันแยกอุโมงค์ที่ให้บางแอปข้าม VPN ได้ (6 ตัวอักษร):

8 แนวนอน: ฟีเจอร์เส้นทาง VPN สองชั้นที่เข้ารหัสทราฟฟิกข้ามโหนดเซิร์ฟเวอร์สองตัวที่ต่างกัน (6 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ล้างข้อมูลทั้งหมดทุกครั้งที่ปิดเปิดเครื่อง (6 ตัวอักษร):

4 แนวตั้ง: เครือข่ายกำหนดด้วยซอฟต์แวร์เฉพาะที่เชื่อมเซิร์ฟเวอร์ทั้งหมดเป็นเมชเดียว (5 ตัวอักษร):

6 แนวตั้ง: ฟีเจอร์ที่เปลี่ยนไอพีภายนอกของคุณเป็นประจำโดยไม่ขัดจังหวะอุโมงค์ (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ร	น	ต	อ	า	นี	า	น	นี	ส	ช	มี	ฟ	บ	า
า	ว	ส	ห	นี	า	ม	กี	บ	จ	า	า	รี	ต	ว
ย	ล้	ซ้	ง	ก	ค	จ	น	ตี	า	ว	ร	ตี	ว	า
ล	ม	ก	พี	อ	ไ	บ	ล้	ส	ล	ย	ด	า	อ	ย
ช	ร	น็	ฟ	ก	ค	ก	ล	ม	า	ป	พ	อ	คิ	อ
ม	แ	เ	มี	า	า	ล	ค	ล	ป	จ	า	า	ล	นี
ป	กี	พ	ร	ง	โ	า	ช	ลี	า	า	ลี	จ	ส	ดี
อ	า	น	ล	ผ	ม	ดี	ช	ก	น	ด	า	ต	วิ	า
ฮ	จ	า	ค	ก	ฟ	ดี	า	ช	ว	เ	ก	ด	ต	กี
ติ	ด	ท	ผ	ฟ	ล	ช	มี	ม	อ	ต	ว็	ฟ	ช์	ร
ล	ดี	า	ท	า	า	ส	ท	ข	ข	า	น	บ	ก	า
ม้	ล	า	ม	ร	จ	มี	า	ร	ช	ก	ด	ง	น	ร
ต	สี	ย	ข	มี	ดี	ด	ด	ว	บ	ฟ	อ	า	ร	ห
ห	รี	น	ผ	นี	ม	ผ	ดี	ข	กี	ส	บ	ลี	ง	ด
ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี

รายการคำศัพท์

คลีนเว็บ แรมล้วน มัลติฮอป คาโมฟลาจ บายพาส คิลสวิตช์ เน็กซัส สลับไอพี

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. คลีนเว็บ
B. แรมล้วน
C. มัลติฮอป
D. คาโมฟลาจ
E. บายพาส
F. คิลสวิตช์
G. เน็กซัส
H. สลับไอพี

คำนิยามและช่องจับคู่	
	1. เทคโนโลยีพรางที่ซ่อนลายเซ็น VPN ให้เหมือนทราฟฟิก HTTPS ปกติ
	2. ฟีเจอร์ความปลอดภัยอัตโนมัติที่บล็อกทราฟฟิกเครือข่ายเมื่อ VPN หลุด
	3. ตัวกรองขั้นสูงที่บล็อกโฆษณา มัลแวร์ และแบนเนอร์ขอความยินยอมคุกกี้
	4. ฟังก์ชันแยกอุโมงค์ที่ให้บางแอปข้าม VPN ได้
	5. ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ล้างข้อมูลทั้งหมดทุกครั้งที่ปิดเปิดเครื่อง
	6. ฟีเจอร์ที่เปลี่ยนไอพีภายนอกของคุณเป็นประจำโดยไม่ขัดจังหวะอุโมงค์
	7. ฟีเจอร์เส้นทาง VPN สองชั้นที่เข้ารหัสทราฟฟิกข้ามโหนดเซิร์ฟเวอร์สองตัวที่ต่างกัน
	8. เครือข่ายกำหนดด้วยซอฟต์แวร์เฉพาะที่เชื่อมเซิร์ฟเวอร์ทั้งหมดเป็นเมชเดียว

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของเครือข่ายส่วนตัวเสมือน (VPN) เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. น ค เ ว็ บ ลี
2. ป ม ั ต ิ อ ฮ ล
3. บ ย พ ส า า
4. ก ส ซ ์ เ น็
5. ล ้ ม น แ ว ร
6. า จ ม ล ค ฟ า โ
7. ต ค ิ ว ิ ซ ์ ส ล
8. บ พี ส อ ไ ล ้

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	ฟีเจอร์ด้านความปลอดภัยใน **Surfshark**			
2	สัญญาณที่บ่งบอกว่าการเชื่อมต่อ **VPN** ของคุณช้า			
3	โปรโตคอล **VPN** ที่คุณรู้จัก			
4	สิ่งที่การเข้ารหัสปกป้อง			
5	ภัยคุกคามบน **Wi-Fi** สาธารณะ			
6	ประเทศที่มีชื่อเสียงด้านกฎหมายความเป็นส่วนตัวที่เข้มแข็ง			
7	วิธีสร้างรหัสผ่านที่รัดกุม			
8	อุปกรณ์ที่คุณจะติดตั้ง **Surfshark**			
9	คำถามสำหรับฝ่ายสนับสนุนลูกค้าของ **Surfshark**			
10	การตั้งค่าที่คุณเปิดเพื่อความปลอดภัยเพิ่มเติม			
11	สิ่งที่ **Surfshark** ซ่อนจากเครือข่ายของคุณได้			
12	ประเภทของการรั่วไหลของ **VPN**			
13	ข้อมูลที่ **VPN** ไม่ควรเก็บ			
14	คำที่อธิบายแอป **VPN** ที่ดี			
15	สิ่งที่การตรวจสอบ (**audit**) ตรวจได้			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN และเครือข่าย

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การข้ามตัวกรองของมหาวิทยาลัยและที่ทำงาน



สถานการณ์: นักเรียนพบว่า Wi-Fi ของมหาวิทยาลัยบล็อกพอร์ต OpenVPN และ WireGuard มาตรฐานทั้งหมด

คำถามอภิปราย: ฟีเจอร์ Surfshark ใดที่ช่วยให้นักเรียนเชื่อมต่อได้โดยไม่ถูกผู้ดูแลเครือข่ายตรวจพบ?

กรณีศึกษาที่ 2: การสืบสวนเชิงสื่อสารมวลชนที่มีความเสี่ยงสูง



สถานการณ์: นักข่าวสืบสวนต้องการการปกป้องเพิ่มเติมจากการเฝ้าติดตามขณะค้นคว้าเอกสารองค์กรที่ละเอียดอ่อน

คำถามอภิปราย: Dynamic MultiHop ให้ความเป็นส่วนตัวที่เหนือกว่าการกำหนดเส้นทางผ่านเซิร์ฟเวอร์เดียวอย่างไร?

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

วิศวกรเครือข่ายรักษาความปลอดภัยของช่องทางกำหนดเส้นทางและอุโมงค์ของไคลเอนต์ ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความ 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

57	25	62	1	11	48	42		42	37	48	26		61	45	30	52

27	1	27	64	45	7		28	56	64	60	10	64

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q1: Surfshark CleanWeb คืออะไร?

CleanWeb เป็นฟีเจอร์ความปลอดภัยแบบบูรณาการที่บล็อกโฆษณา ตัวติดตาม มัลแวร์ และเว็บไซต์ฟิชชิง

Q2: เซิร์ฟเวอร์แบบ RAM อย่างเดียวคืออะไร?

เซิร์ฟเวอร์แบบ RAM-only ทำงานบนหน่วยความจำแบบ volatile ซึ่งหมายความว่าข้อมูลที่เก็บในหน่วยความจำจะถูกล้างทุกครั้งที่เซิร์ฟเวอร์รีบูต

Q3: Surfshark MultiHop คืออะไร?

MultiHop (Double VPN) กำหนดเส้นทางและเข้ารหัสการเชื่อมต่ออินเทอร์เน็ตของคุณผ่านตำแหน่งเซิร์ฟเวอร์ที่ต่างกันสองแห่ง

Q4: โหมดพรางตัว (Camouflage Mode) ทำงานอย่างไร?

โหมด Camouflage อำพรางทราฟฟิก VPN เพื่อไม่ให้ ISP ของคุณทราบว่าคุณใช้ VPN

Q5: ฟีเจอร์ Bypasser คืออะไร?

Bypasser เป็นเครื่องมือ split tunneling ของ Surfshark ที่ให้แอปหรือเว็บไซต์ที่เลือกข้าม VPN ได้

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q6: Surfshark มี Kill Switch หรือไม่?

ได้ Kill Switch จะตัดการเชื่อมต่ออินเทอร์เน็ตของคุณหาก VPN หลุดโดยไม่คาดคิด

Q7: Surfshark ใช้มาตรฐานการเข้ารหัสอะไร?

Surfshark ใช้ AES-256-GCM และ ChaCha20 รวมถึง AEGIS-256X2 บนโปรโตคอล Dausos ใหม่ของตน

Q8: นโยบาย no-logs ของ Surfshark เคยได้รับการตรวจสอบหรือไม่?

ใช่ Deloitte ตรวจสอบยืนยันนโยบายไม่เก็บบันทึกของ Surfshark ในปี 2023 และอีกครั้งในปี 2025

Q9: Surfshark Nexus คืออะไร?

Nexus เป็นสถาปัตยกรรม SDN ขั้นสูงที่เชื่อมต่อเซิร์ฟเวอร์ทั้งหมดเป็นเครือข่ายเดียวเพื่อการกำหนดเส้นทางที่ราบรื่นขึ้น

Q10: ฟีเจอร์ IP Rotator คืออะไร?

IP Rotator เปลี่ยนที่อยู่ IP ของคุณโดยอัตโนมัติทุกไม่กี่นาทีโดยไม่ตัดเซสชัน VPN ของคุณ

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q1: Dynamic MultiHop ต่างจาก Double VPN แบบดั้งเดิมอย่างไร?

Dynamic MultiHop ช่วยให้คุณปรับแต่งการผสมผสานเซิร์ฟเวอร์ขาเข้าและขาออกได้ทั่วโลก

Q2: CleanWeb 2.0 ใช้งานกับส่วนขยายเบราว์เซอร์ได้หรือไม่?

ใช่ CleanWeb 2.0 บล็อกโฆษณาวิดีโอ ป๊อปอัปขอความยินยอมคุกกี้ และแบนเนอร์แจ้งเตือนภายใน Chrome/ Firefox

Q3: Alternative ID ในชุดโปรแกรมความปลอดภัยคืออะไร?

Alternative ID สร้างนามแฝงส่วนตัว ที่อยู่อีเมล และหมายเลขโทรศัพท์ปลอมตัวที่ไม่ซ้ำกัน

Q4: Surfshark ป้องกัน DNS รั่วไหลได้อย่างไร?

Surfshark กำหนดเส้นทางคำขอโดเมนทั้งหมดผ่านเซิร์ฟเวอร์ DNS ส่วนตัวของตนเองบนแต่ละโหนด

Q5: Surfshark รองรับการเข้ารหัส ChaCha20 บนมือถือหรือไม่?

ใช่ WireGuard บน Android และ iOS ใช้ ChaCha20-Poly1305 เพื่อประสิทธิภาพที่เหนือกว่าบนมือถือ

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q6: โหมด NoBorders ใน Surfshark คืออะไร?

NoBorders ตรวจจับสภาพแวดล้อมเครือข่ายที่มีข้อจำกัดโดยอัตโนมัติและจัดหาเซิร์ฟเวอร์เฉพาะทางให้

Q7: ใครเป็นผู้ตรวจสอบความปลอดภัยของส่วนขยายเบราว์เซอร์ Surfshark?

บริษัทความปลอดภัยไซเบอร์อิสระ Cure53 ตรวจสอบส่วนขยายเบราว์เซอร์และระบบเซิร์ฟเวอร์เสร็จสิ้นแล้ว

Q8: Surfshark ป้องกันการรั่วไหลของ IPv6 อย่างไร?

Surfshark กำหนดเส้นทางทราฟฟิก IPv6 อย่างปลอดภัยหรือจำกัดอย่างปลอดภัยเพื่อป้องกันการรั่วไหลแบบไม่เข้ารหัส

Q9: เขตอำนาจศาลทางกฎหมายของ Surfshark ตั้งอยู่ที่ใด?

Surfshark ดำเนินงานภายใต้กฎหมายเนเธอร์แลนด์ โดยปฏิบัติตามมาตรฐานความเป็นส่วนตัวของยุโรปตาม GDPR อย่างเข้มงวด

Q10: Surfshark รองรับการยืนยันตัวตนสองปัจจัย (2FA) หรือไม่?

ใช่ และ Surfshark One เพิ่มล็อก 2FA เพื่อให้มีเพียงคุณเท่านั้นที่เปลี่ยนการตั้งค่าฟีเจอร์ได้

ส่วนที่ 11: ข้อเท็จจริง VPN ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับความเร็วการเข้ารหัส VPN การตรวจสอบโปรโตคอล การเชื่อมต่อบนมือถือ และการทำงานระยะไกลขององค์กร

1. ข้อมูลเชิงลึกเรื่อง VPN

1. Surfshark ระบุว่าเครือข่ายเซิร์ฟเวอร์ทั้งหมดกว่า 4,500 เครื่องทำงานบนฮาร์ดแวร์ RAM เท่านั้นที่ไม่มีดิสก์และไม่คงข้อมูล

2. ข้อมูลเชิงลึกเรื่อง VPN

2. Deloitte หนึ่งในบริษัท Big Four ตรวจสอบนโยบายไม่เก็บบันทึกของ Surfshark ในปี 2023 และอีกครั้งในเดือนพฤศจิกายน 2025

3. ข้อมูลเชิงลึกเรื่อง VPN

3. สถาปัตยกรรม Nexus ที่เป็นกรรมสิทธิ์เชื่อมต่อเซิร์ฟเวอร์ทั่วโลกทั้งหมดเป็นเครือข่ายที่กำหนดด้วยซอฟต์แวร์แบบไดนามิก

4. ข้อมูลเชิงลึกเรื่อง VPN

4. Rotating IP เปลี่ยนที่อยู่ IP ของคุณทุกประมาณห้านาทีโดยไม่ตัดการเชื่อมต่อ VPN

5. ข้อมูลเชิงลึกเรื่อง VPN

5. CleanWeb 2.0 บล็อกป๊อปอัปขอความยินยอมคุกกี้ที่รบกวนและโฆษณาวิดีโอโดยตรงในเบราว์เซอร์

6. ข้อมูลเชิงลึกเรื่อง VPN

6. Dynamic MultiHop ช่วยให้ผู้ใช้สร้างเส้นทางเข้ารหัสสองเซิร์ฟเวอร์แบบกำหนดเองข้าม 100 ประเทศ

7. ข้อมูลเชิงลึกด้าน VPN

7. Camouflage Mode ลบลายเซ็นส่วนหัวของ VPN ทำให้แยกทราฟฟิกออกจาก HTTPS ปกติไม่ได้

8. ข้อมูลเชิงลึกด้าน VPN

8. Alternative ID สร้างนามแฝงใช้แล้วทิ้งและอีเมลปลอมตัวเพื่อปกป้องผู้ใช้จากการรั่วไหลของฐานข้อมูล

9. ข้อมูลเชิงลึกด้าน VPN

9. Surfshark บังคับใช้การเข้ารหัสแบบสมมาตร AES-256-GCM ควบคู่กับ ChaCha20 บนโปรโตคอล WireGuard

10. ข้อมูลเชิงลึกเรื่อง VPN

10. โหมด NoBorders เปิดใช้งานอัตโนมัติบนเครือข่ายที่ถูกจำกัดเพื่อให้การเข้าถึงอุโมงค์ที่ยืดหยุ่น

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานทางเทคนิค ข้อกำหนดเฉพาะ และกรอบการกำกับดูแลระดับโลก

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **ตัวบล็อกเนื้อหาแบบรวมในตัว** การป้องกันโฆษณาและมัลแวร์ **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

CleanWeb คือตัวกรองความปลอดภัยแบบบูรณาการของ Surfshark ที่บล็อกโฆษณา โดเมนตัวติดตาม เว็บไซต์ฟิชชิง และสคริปต์ URL ที่เป็นอันตรายในระดับเครือข่าย แหล่งอ้างอิง: CleanWeb Security Specs.

2 **โครงสร้างพื้นฐาน RAM เท่านั้น 100%** สถาปัตยกรรม RAM **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

Surfshark ใช้เซิร์ฟเวอร์แบบ RAM เท่านั้น ดังนั้นข้อมูลที่เก็บในหน่วยความจำของเซิร์ฟเวอร์จะถูกลบเมื่อปิดหรือรีบูตเซิร์ฟเวอร์ การอ้างอิง: Cure53 Infrastructure Audit.

3 **อุโมงค์คู่ MultiHop** VPN แบบ MULTIHOP **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

MultiHop (Double VPN) เข้ารหัสการรับส่งข้อมูลผ่านโหนดเซิร์ฟเวอร์สองเครื่องที่แยกกันในต่างประเทศ เพื่อป้องกันการโจมตีแบบเชื่อมโยงการรับส่งข้อมูล อ้างอิง: Surfshark MultiHop Guide.

4 **การอำพรางด้วยโหมด Camouflage** การอำพราง **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

โหมด Camouflage ปรับเปลี่ยนส่วนหัวแพ็กเก็ต OpenVPN เพื่ออำพรางทราฟฟิก VPN ให้เหมือนทราฟฟิก HTTPS ทั่วไป จึงข้ามการบล็อกของไฟร์วอลล์ที่เข้มงวดได้ แหล่งอ้างอิง: Surfshark Stealth Whitepaper.

5 **Bypasser Split Tunneling** การทำอุโมงค์แยก (Split Tunneling) **คำตอบที่ถูกต้อง: B**

หมายเหตุสำหรับผู้สอน

Bypasser เป็นเครื่องมือ split tunneling ของ Surfshark ที่ให้ผู้ใช้เลือกแอปหรือเว็บไซต์เฉพาะเพื่อส่งตรงผ่านการเชื่อมต่อ ISP ปกติ อ้างอิง: Surfshark Client Features.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **การล้างข้อมูลในหน่วยความจำชั่วคราว** ความปลอดภัยของเซิร์ฟเวอร์ คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

เซิร์ฟเวอร์แบบ RAM-only ไม่เก็บข้อมูลใดๆ บนฮาร์ดดิสก์ถาวร การรีบูตฮาร์ดแวร์จะล้างหน่วยความจำการทำงานทั้งหมดทันที แหล่งอ้างอิง: RAM Server Architecture.

7 **การปกปิด ISP ด้วยโหมด Camouflage** การซ่อนทราฟฟิก คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

โหมด Camouflage ลบลายเซ็นโปรโตคอล OpenVPN ออก ป้องกันไม่ให้ ISP ตรวจพบว่าผู้ใช้เชื่อมต่ออยู่กับอุโมงค์ VPN แหล่งอ้างอิง: Deep Packet Inspection Guide.

8 **ส่วนขยายเบราว์เซอร์ CleanWeb 2.0** ส่วนขยายเบราว์เซอร์ คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

CleanWeb 2.0 ทำงานภายในส่วนขยายเบราว์เซอร์เพื่อบล็อกป๊อปอัปขอความยินยอมเรื่องคุกกี้ โฆษณาวิดีโอ และสคริปต์เปลี่ยนเส้นทางที่เป็นอันตรายแบบเรียลไทม์ แหล่งอ้างอิง: CleanWeb 2.0 Release Notes.

9 **ไม่เก็บบันทึกการเชื่อมต่อ** นโยบายไม่เก็บล็อก คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

Surfshark รักษานโยบายไม่เก็บบันทึกที่เข้มงวดซึ่งผ่านการตรวจสอบโดยอิสระ โดยไม่บันทึกที่อยู่ IP เวลาการเชื่อมต่อ หรือบันทึกแบนด์วิดท์ การอ้างอิง: Deloitte No-Logs Audit.

10 **การหมุนเวียน IP แบบไดนามิกของ Nexus** เครือข่าย NEXUS คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

เครือข่ายที่กำหนดโดยซอฟต์แวร์ Surfshark Nexus หมุนเวียนที่อยู่ IP ของผู้ใช้แบบไดนามิกทุกไม่กี่นาทีโดยไม่ตัดการเชื่อมต่อ VPN ที่ใช้งานอยู่ อ้างอิง: Surfshark Nexus Architecture.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

C 1. คลีนเว็บ	D 2. แรมล้วน	G 3. มัลติฮอป	F 4. คาโมฟลาจ
B 5. บายพาส	A 6. คิลสวิตช์	H 7. เน็กซัส	E 8. การหมุนเวียน

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 คลีนเว็บ	2 แรมล้วน	3 มัลติฮอป	4 คาโมฟลาจ
5 บายพาส	6 เน็กซัส		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 D – คาโมฟลาจ	2 F – คิลสวิตช์	3 A – คลีนเว็บ	4 E – บายพาส
5 B – แรมล้วน	6 H – สลับไอพี	7 C – มัลติฮอป	8 G – เน็กซัส

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย คลีนเว็บ แรมล้วน และ มัลติฮอป ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

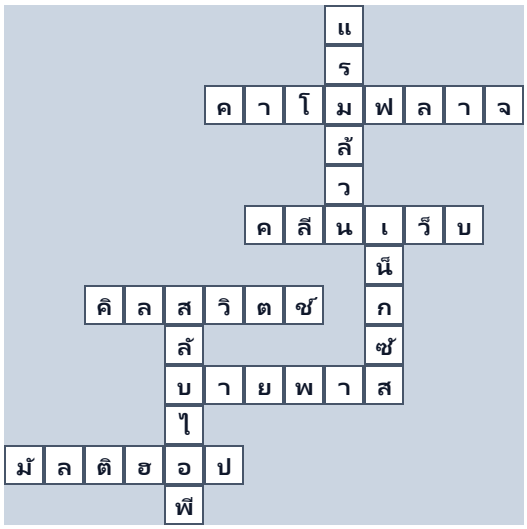
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ร	น	ต	อ	า	นี	า	น	นี	ส	ช	มี	ฟ	บ	า
า	ว	ส	ห	นี	า	ม	กี	บ	จ	า	า	รี	ต	ว
ย	ล้	ช้	ง	ก	ค	จ	น	ตี	า	ว	ร	ตี	ว	า
ล	ม	ก	พี	อ	ไ	บ	ล้	ส	ล	ย	ด	า	อ	ย
ช	ร	นิ	ฟ	ก	ค	ก	ล	ม	า	ป	พ	อ	คิ	อ
ม	แ	เ	มี	า	า	ล	ค	ล	ป	จ	า	า	ล	นี
ป	กี	พ	ร	ง	โ	า	ช	ลี	า	า	ลี	จ	ส	ดี
อ	า	น	ล	ผ	ม	ดี	ช	ก	น	ด	า	ต	วิ	า
ฮ	จ	า	ค	ก	ฟ	ดี	า	ช	ว	เ	ก	ด	ต	กี
ติ	ด	ท	ผ	ฟ	ล	ช	มี	ม	อ	ต	วิ	ฟ	ช์	ร
ล	ดี	า	ท	า	า	ส	ท	ข	ข	า	น	บ	ก	า
ม้	ล	า	ม	ร	จ	มี	า	ร	ช	ก	ด	ง	น	ร
ต	สี	ย	ข	มี	ดี	ด	ด	ว	บ	ฟ	อ	า	ร	ห
ห	รี	น	ผ	นี	ม	ผ	ดี	ข	กี	ส	บ	ลี	ง	ด
ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: คาโมฟลาจ เทคโนโลยีพรางที่ซ่อนลายเซ็น VPN ให้เหมือนทราฟฟิก HTTPS ปกติ (8 ตัวอักษร)

3 แนวนอน: คลีนเว็บ ตัวกรองขั้นสูงที่บล็อกโฆษณา มัลแวร์ และแบนเนอร์ขอความยินยอมคุกกี้ (6 ตัวอักษร)

5 แนวนอน: คิลสวิตช์ ฟีเจอร์ความปลอดภัยอัตโนมัติที่บล็อกทราฟฟิกเครือข่ายเมื่อ VPN หลุด (6 ตัวอักษร)

7 แนวนอน: บายพาส ฟังก์ชันแยกอุโมงค์ที่ให้บางแอปข้าม VPN ได้ (6 ตัวอักษร)

8 แนวนอน: มัลติฮอป ฟีเจอร์เส้นทาง VPN สองชั้นที่เข้ารหัสทราฟฟิกข้ามโหนดเซิร์ฟเวอร์สองตัวที่ต่างกัน (6 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: แรมล้วน ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ล้างข้อมูลทั้งหมดทุกครั้งที่ปิดเปิดเครื่อง (6 ตัวอักษร)

4 แนวตั้ง: เน็กซัส เครือข่ายกำหนดด้วยซอฟต์แวร์เฉพาะที่เชื่อมเซิร์ฟเวอร์ทั้งหมดเป็นเมชเดียว (5 ตัวอักษร)

6 แนวตั้ง: สลับไอพี ฟีเจอร์ที่เปลี่ยนไอพีภายนอกของคุณเป็นประจำโดยไม่ขัดจังหวะอุโมงค์ (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. นคเว็บลี — คลีนเว็บ
2. ปมัติอฮล — มัลติฮอป
3. บยพสาา — บายพาส
4. กสซ์เน็ — เน็กซัส
5. ล้มนแวร — แรมล้วน
6. าจมลคฟาโ — คาโมฟลาจ
7. ตคิวิซ์สล — คิลสวิตช์
8. บพีสอไล้ — สลับไอพี

เฉลยภารกิจรหัสลับ

"เน็กซัส สลับ ไอพี ปกป้อง ผู้ใช้"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การข้ามตัวกรองของมหาวิทยาลัยและที่ทำงาน

เฉลยสำหรับผู้สอน

เกณฑ์การให้คะแนนและแนวทางเฉลย

- การวิเคราะห์สถานการณ์: นักเรียนพบว่า Wi-Fi ในมหาวิทยาลัยบล็อกพอร์ต OpenVPN และ WireGuard มาตรฐานทั้งหมด
- คำถามชวนคิด: ฟีเจอร์ Surfshark ใดช่วยให้นักเรียนเชื่อมต่อได้โดยไม่ถูกผู้ดูแลเครือข่ายตรวจพบ?
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: เปิดใช้งานโหมดพรางตัว (Camouflage Mode) ของ OpenVPN ซึ่งซ่อนเมตาดาตาของ VPN เพื่อให้ไฟร์วอลล์เห็นเป็นการท่องเว็บ HTTPS ปกติ

B กรณีศึกษาที่ 2: การสืบสวนเชิงสื่อสารมวลชนที่มีความเสี่ยงสูง

เฉลยสำหรับผู้สอน

เกณฑ์การให้คะแนนและแนวทางเฉลย

- การวิเคราะห์สถานการณ์: นักข่าวสืบสวนต้องการการป้องกันการสอดแนมเพิ่มเติมขณะค้นคว้าบันทึกขององค์กรที่ละเอียดอ่อน
- คำถามชวนคิด: Dynamic MultiHop ให้ความเป็นส่วนตัวที่เหนือกว่าการกำหนดเส้นทางผ่านเซิร์ฟเวอร์เดียวได้อย่างไร?
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: Dynamic MultiHop กำหนดเส้นทางทราฟฟิกผ่านเซิร์ฟเวอร์ขาเข้าและขาออกในสองประเทศ จึงไม่มีเซิร์ฟเวอร์ใดเพียงตัวเดียวที่เปิดเผยผู้ใช้ได้