ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

รีวิว Surfshark

การวิเคราะห์ทางเทคนิคของ Surfshark VPN ที่มีสำนักงานใหญ่ในเนเธอร์แลนด์ การหมุนเวียน IP แบบไดนามิกของ SDN Nexus ตัวกรอง DNS CleanWeb 2.0 การเชื่อมต่ออุปกรณ์ไม่จำกัด และกลไกการหลีกเลี่ยงของ NoBorders

ภาพรวมการเรียนรู้เรื่องการรีวิว SURFSHARK

ผู้เรียน
สถานะนักเรียน
สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย
สถานะการเชื่อมต่อ
การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน
การป้องกันการรั่วไหล
การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการรีวิวทางเทคนิคของ Surfshark คุณจะได้สำรวจการหมุนเวียน IP แบบ Nexus ที่ใช้ SDN ตัวกรอง CleanWeb 2.0 การเชื่อมต่ออุปกรณ์ไม่จำกัด และการข้ามการเซ็นเซอร์ด้วย NoBorders

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/

เส้นทางการเรียนรู้ Surfshark ของคุณ

- วิเคราะห์สถาปัตยกรรมทางเทคนิคและมาตรฐานการเข้ารหัสของรีวิว Surfshark
- ตั้งค่าไคลเอนต์เพื่อป้องกันการรั่วไหลของทราฟฟิก IP, DNS และ WebRTC
- เปรียบเทียบโปรโตคอลอุโมงค์ที่เป็นกรรมสิทธิ์เฉพาะกับการใช้งานมาตรฐาน

คำชี้แจงการรีวิว SURFSHARK

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ เครือข่าย SDN Nexus และการบล็อกของ CleanWeb ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

ระบบเครือข่าย SDN NEXUS และตัวบล็อกเนื้อหา CLEANWEB (บทนำ)

Surfshark มีเครือข่าย Nexus ที่อิง SDN ซึ่งทำให้หมุนเวียน IP ขาออกแบบไดนามิกได้ บังคับใช้การเชื่อมต่ออุปกรณ์ไม่จำกัด ใช้โหนดเซิร์ฟเวอร์แบบ RAM เท่านั้นภายใต้เขตอำนาจรัฐของเนเธอร์แลนด์ และผสานตัวกรอง CleanWeb 2.0

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. **1. หน้าที่หลักของ CleanWeb 2.0 ของ Surfshark คืออะไร?**
   - A) บล็อกโฆษณา ตัวติดตาม ป๊อปอัปคุกกี้ และมัลแวร์
   - B) เข้ารหัสอีเมลขาออกและไดรฟ์บนคลาวด์
   - C) หมุนเวียนที่อยู่ IP ของเซิร์ฟเวอร์ทุกสิบนาที
   - D) ส่งต่อพอร์ตของเราเตอร์โดยอัตโนมัติ

2. **2. เทคโนโลยี SDN ของ Surfshark ใดที่ช่วยให้หมุนเวียน IP แบบไดนามิกได้?**
   - A) Surfshark Nexus
   - B) Secure Core
   - C) WireGuard Core
   - D) โหมด Camouflage

3. **3. Surfshark จำกัดจำนวนอุปกรณ์ที่เชื่อมต่อพร้อมกันได้เท่าใด?**
   - A) การเชื่อมต่อพร้อมกันไม่จำกัด
   - B) สูงสุดห้าอุปกรณ์
   - C) สูงสุดสิบอุปกรณ์
   - D) จำกัดให้ใช้กับเราเตอร์เพียงเครื่องเดียว

4. **4. โหมดใดของ Surfshark ที่ข้ามไฟร์วอลล์ในพื้นที่ที่มีการจำกัด?**
   - A) NoBorders Mode
   - B) โหมด CleanWeb
   - C) โหมด Nexus
   - D) โหมดข้าม

5. **5. ฟีเจอร์ฝั่งเซิร์ฟเวอร์ใดของ Surfshark ที่ป้องกันการจัดเก็บข้อมูลลงดิสก์?**
   - A) เซิร์ฟเวอร์ไร้ดิสก์ที่ใช้ RAM 100%
   - B) ไดรฟ์โซลิดสเตต (SSD) ที่เข้ารหัส
   - C) อาร์เรย์ RAID ความจุสูง
   - D) กลุ่มเซิร์ฟเวอร์เสมือนที่โฮสต์ในสหรัฐอเมริกา

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. CleanWeb 2.0 ทำงานเป็นส่วนขยายเบราว์เซอร์และตัวกรองฝั่งไคลเอนต์ที่ดักจับโฆษณา ตัวติดตาม และป๊อปอัปขอความยินยอมเรื่องคุกกี้

○ จริง ○ เท็จ

7 คำถาม 7

7. สถาปัตยกรรม Nexus ของ Surfshark เชื่อมเครือข่ายเซิร์ฟเวอร์ทั้งหมดเข้าเป็น SDN เดียวเพื่อเพิ่มประสิทธิภาพการกำหนดเส้นทางและเปิดใช้การหมุนเวียน IP

○ จริง ○ เท็จ

8 คำถาม 8

8. Surfshark จำกัดผู้ใช้ไว้ที่การเชื่อมต่ออุปกรณ์สูงสุดห้าเครื่อง ณ เวลาใดเวลาหนึ่ง

○ จริง ○ เท็จ

9 คำถาม 9

9. โหมด NoBorders ตรวจจับข้อจำกัดอินเทอร์เน็ตในพื้นที่โดยอัตโนมัติและแนะนำโหนดเซิร์ฟเวอร์เฉพาะที่ปรับให้เหมาะสม

○ จริง ○ เท็จ

10 คำถาม 10

10. Surfshark ดำเนินงานภายใต้เขตอำนาจรัฐของเนเธอร์แลนด์

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. เพื่อท่องเว็บโดยไม่เจอป๊อปอัปคุกกี้และโฆษณาที่รบกวน ผู้ใช้ควรเปิด _____ ในการตั้งค่าไคลเอนต์
2. Surfshark ให้เชื่อมต่ออุปกรณ์พร้อมกันแบบ _____ ภายใต้แผนพรีเมียมเดียว
3. สถาปัตยกรรมเซิร์ฟเวอร์แบบ SDN เฉพาะมีชื่อว่าเครือข่าย Surfshark _____
4. เพื่อข้ามการเซ็นเซอร์อินเทอร์เน็ตในพื้นที่โดยอัตโนมัติ ไคลเอนต์เปิดโหมด _____
5. เพื่อป้องกันการเก็บประวัติเซสชัน ผู้ให้บริการส่งทราฟฟิกผ่านเซิร์ฟเวอร์ไร้ดิสก์แบบ _____
6. ทราฟฟิก OpenVPN พรางเป็นทราฟฟิกเว็บมาตรฐานได้ด้วยโหมดพรางของ Surfshark คือ _____

คลังคำศัพท์

คลีนเว็บ | คาโมฟลาจ | เน็กซัส | โนบอร์เดอร์ส | บายพาส | ไม่จำกัด | แรมล้วน | ไวร์การ์ด

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่อง VPN และเครือข่าย

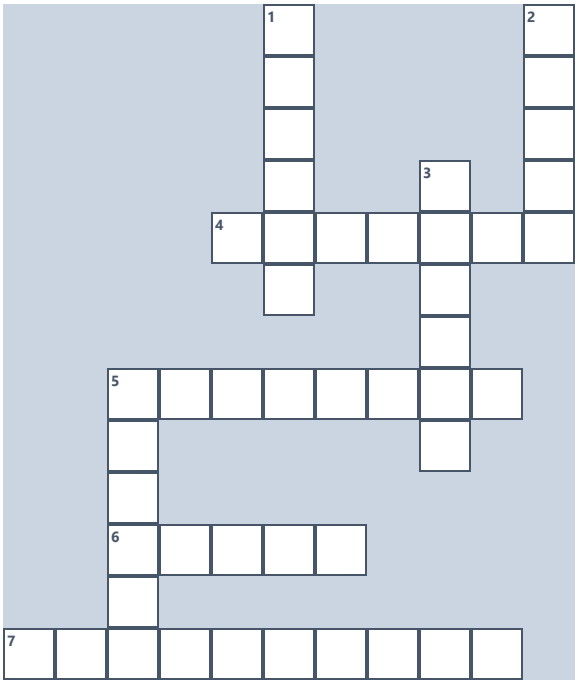
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. CleanWeb**	**A**	โปรโตคอลการเชื่อมต่อโอเพนซอร์สสมัยใหม่ความเร็วสูง
☐	**2. Nexus**	**B**	โหมดข้ามการเซ็นเซอร์ที่ปรับแต่งโหนดที่ถูกจำกัด
☐	**3. ไม่จำกัด**	**C**	เทคโนโลยีอำพรางที่ปกปิดทราฟฟิก VPN ให้เป็น HTTPS
☐	**4. NoBorders**	**D**	ตัวบล็อกโฆษณา ตัวติดตาม ป๊อปอัป และมัลแวร์ชั้นสูง
☐	**5. RAM-only**	**E**	การใช้งาน Split tunneling ที่กำหนดเส้นทางแอปพลิเคชันเฉพาะ
☐	**6. Camouflage**	**F**	เครือข่ายเซิร์ฟเวอร์ SDN ที่ทำให้หมุนเวียน IP และกระโดดข้ามเซิร์ฟเวอร์ได้
☐	**7. Bypasser**	**G**	ฮาร์ดแวร์เซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เก็บบันทึกแบบชั่วคราวเลย
☐	**8. WireGuard**	**H**	นโยบายการสมัครสมาชิกที่อนุญาตให้เชื่อมต่ออุปกรณ์ได้ไม่จำกัด

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

4. โปรโตคอลเชื่อมต่อโอเพนซอร์สความเร็วสูงสมัยใหม่ (7)

5. เทคโนโลยีพรางที่ปกปิดทราฟฟิก VPN ให้เป็น HTTPS (8)

6. เครือข่ายเซิร์ฟเวอร์ SDN ที่ทำให้หมุนเวียนไอพีและฮอปได้ (5)

7. โหมดข้ามการเซ็นเซอร์ที่ปรับให้เหมาะกับโหนดที่ถูกจำกัด (10)

แนวตั้ง

1. ฮาร์ดแวร์เซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เก็บล็อกในหน่วยความจำชั่วคราวเลย (6)

2. นโยบายการสมัครที่อนุญาตการเชื่อมต่ออุปกรณ์ได้ไม่จำกัด (5)

3. การใช้งานการแยกอุโมงค์ที่กำหนดเส้นทางแอปเฉพาะ (6)

5. ตัวบล็อกโฆษณา ตัวติดตาม ป๊อปอัป และมัลแวร์ชั้นสูง (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

4 แนวนอน: โปรโตคอลเชื่อมต่อโอเพนซอร์สความเร็วสูงสมัยใหม่ (7 ตัวอักษร):

5 แนวนอน: เทคโนโลยีพรางที่ปกปิดทราฟฟิก VPN ให้เป็น HTTPS (8 ตัวอักษร):

6 แนวนอน: เครือข่ายเซิร์ฟเวอร์ SDN ที่ทำให้หมุนเวียนไอพีและฮอปได้ (5 ตัวอักษร):

7 แนวนอน: โหมดข้ามการเซ็นเซอร์ที่ปรับให้เหมาะกับโหนดที่ถูกจำกัด (10 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ฮาร์ดแวร์เซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เก็บล็อกในหน่วยความจำชั่วคราวเลย (6 ตัวอักษร):

2 แนวตั้ง: นโยบายการสมัครที่อนุญาตการเชื่อมต่ออุปกรณ์ได้ไม่จำกัด (5 ตัวอักษร):

3 แนวตั้ง: การใช้งานการแยกอุโมงค์ที่กำหนดเส้นทางแอปเฉพาะ (6 ตัวอักษร):

5 แนวตั้ง: ตัวบล็อกโฆษณา ตัวติดตาม ป๊อปอัป และมัลแวร์ขั้นสูง (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช	มี	ส	ฟ	บ	า	า	ห	นี	า	ม	กี	จ	า	า
รี	ต	า	ว	ย	ง	ก	ค	ค	จ	น	ตี	ว	ร	ตี
ว	า	พ	ล	ล	ด	า	อ	ย	ลี	ช	ฟ	ก	ก	ล
ม	า	ย	น	ว	ล้	ม	ร	แ	ป	น	อ	อ	ม	มี
า	ล	า	ล	ป	โ	จ	า	นี	กี	พ	เ	ร	ง	า
ด	ช	บ	า	า	น	ลี	ค	จ	ส	ดี	า	ว็	น	ล
ร์	ผ	ดี	ช	ก	บ	ด	า	า	ต	ซ้	า	จ	บ	า
า	ค	ก	ดี	า	อ	ช	ว	ก	โ	ด	ก	กี	ด	ท
ก	ผ	ฟ	ช	มี	ร์	ม	อ	ต	ฟ	ม	ร	น็	ดี	า
ร์	ท	า	ส	ท	เ	ไ	ข	ข	า	น	ฟ	ก	เ	า
ว	ล	า	ม	ร	ด	ม่	มี	า	ร	ช	ก	ล	ด	ง
ไ	น	ร	ต	สี	อ	จำ	ย	ข	มี	ดี	ด	ด	า	ว
บ	ฟ	อ	า	ร	ร์	กั	ห	ห	รี	น	ผ	นี	ม	จ
ผ	ดี	ข	กี	ส	ส	ด	บ	ลี	ง	ด	ร	ด	ค	ผ
ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด	บ	ตี	น

รายการคำศัพท์

คลีนเว็บ เน็กซัส ไม่จำกัด โนบอร์เดอร์ส แรมล้วน คาโมฟลาจ บายพาส ไวร์การ์ด

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. คลีนเว็บ
B. เน็กซัส
C. ไม่จำกัด
D. โนบอร์เดอร์ส
E. แรมล้วน
F. คาโมฟลาจ
G. บายพาส
H. ไวร์การ์ด

คำนิยามและช่องจับคู่	
	1. ฮาร์ดแวร์เซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เก็บล็อกในหน่วยความจำชั่วคราวเลย
	2. ตัวบล็อกโฆษณา ตัวติดตาม ป๊อปอัป และมัลแวร์ขั้นสูง
	3. โหมดข้ามการเซ็นเซอร์ที่ปรับให้เหมาะกับโหนดที่ถูกจำกัด
	4. นโยบายการสมัครที่อนุญาตการเชื่อมต่ออุปกรณ์ได้ไม่จำกัด
	5. เครือข่ายเซิร์ฟเวอร์ SDN ที่ทำให้หมุนเวียนไอพีและฮอปได้
	6. การใช้งานการแยกอุโมงค์ที่กำหนดเส้นทางแอปเฉพาะ
	7. โปรโตคอลเชื่อมต่อโอเพนซอร์สความเร็วสูงสมัยใหม่
	8. เทคโนโลยีพรางที่ปกปิดทราฟฟิก VPN ให้เป็น HTTPS

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของเครือข่ายส่วนตัวเสมือน (VPN) เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. น ค เ ว็ บ ลี
2. ไ ด กั จำ ม่
3. แ ม ล้ น ว ร
4. ส พ ย า บ า
5. ก ส เ ซ้ น็
6. ร์ ร์ อ ด อ โ น เ ส บ
7. ค จ ฟ ล า า ม โ
8. ว ก ด ไ ร์ า ร์

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	บริการสตรีมมิงที่คุณรับชม			
2	บริการ VPN อื่นที่ไม่ใช่ Surfshark			
3	สิ่งที่ควรตรวจสอบก่อนซื้อ VPN			
4	คนที่คุณจะแนะนำ Surfshark ให้			
5	สถานการณ์ที่ kill switch ช่วยได้			
6	ข้อมูลที่ VPN ไม่ควรเก็บ			
7	โปรโตคอล VPN ที่คุณรู้จัก			
8	สถานที่ที่คุณจะเปิดใช้ Surfshark			
9	สัญญาณที่บ่งบอกว่าการเชื่อมต่อ VPN ของคุณช้า			
10	สิ่งที่ Surfshark ซ่อนจากเครือข่ายของคุณได้			
11	สิ่งที่คุณมองหาใน Surfshark			
12	อุปกรณ์ที่คุณจะติดตั้ง Surfshark			
13	แอปที่คุณจะใช้ร่วมกับ Surfshark			
14	คำศัพท์ด้านความปลอดภัยที่คุณเรียนรู้จากใบงานนี้			
15	ประเทศที่คุณอยากได้เซิร์ฟเวอร์ Surfshark			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN และเครือข่าย

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: ความปลอดภัยของการหมุนเวียน IP ของ Nexus



สถานการณ์: นักข่าวอิสระกำลังอัปโหลดบทสัมภาษณ์ที่ละเอียดอ่อน เพื่อป้องกันการติดตามโดยบุคคลที่สามที่อาจเฝ้าติดตาม IP ปลายทาง เขาเปิดใช้ Surfshark Nexus IP Rotation ซึ่งเปลี่ยน IP ขาออกประมาณทุกห้านาทีโดยไม่ตัดการเชื่อมต่อ

คำถามอภิปราย: ข้อได้เปรียบทางเทคนิคของการหมุนเวียน IP แบบ SDN เหนือการเชื่อมต่อ VPN แบบคงที่คืออะไร?

กรณีศึกษาที่ 2: การทดสอบการเชื่อมต่ออุปกรณ์ไม่จำกัด



สถานการณ์: ผู้ดูแลระบบไอทีใช้การสมัครใช้ Surfshark เดียวเพื่อรักษาความปลอดภัยอุปกรณ์ทดสอบทั้งหมดในห้องปฏิบัติการ โดยเชื่อมต่อสมาร์ทโฟนและแล็ปท็อปทดสอบ 45 เครื่องพร้อมกันกับเซิร์ฟเวอร์ภายใน

คำถามอภิปราย: สิทธิ์การใช้งานพร้อมกันแบบไม่จำกัดเป็นประโยชน์ต่อนักพัฒนาที่ทดสอบแอปหลายอุปกรณ์อย่างไร?

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		23	50	7	49	25		35	47	26	26

42	37	48	26		61	45	30	52

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q1: Surfshark CleanWeb 2.0 คืออะไร?

CleanWeb 2.0 เป็นฟีเจอร์ชั้นสูงที่บล็อกโฆษณา ตัวติดตาม มัลแวร์ และป๊อปอัปขอความยินยอมเรื่องคุกกี้โดยตรงในระดับเบราว์เซอร์ ช่วยเพิ่มความเร็วและความปลอดภัย

Q2: เครือข่าย Surfshark Nexus คืออะไร?

Nexus เป็นสถาปัตยกรรมเซิร์ฟเวอร์แบบ SDN ที่ส่งการรับส่งข้อมูลของคุณผ่านเครือข่ายเซิร์ฟเวอร์ทั้งหมดแทนที่จะเป็นอุโมงค์เดียว ทำให้มีฟีเจอร์อย่าง IP Rotation และ MultiHop

Q3: สามารถเชื่อมต่อ Surfshark พร้อมกันได้กี่อุปกรณ์?

Surfshark อนุญาตการเชื่อมต่ออุปกรณ์พร้อมกันไม่จำกัดภายใต้บัญชีสมาชิกที่ใช้งานอยู่เพียงบัญชีเดียว

Q4: โหมด NoBorders บน Surfshark คืออะไร?

NoBorders เป็นฟีเจอร์ที่เปิดใช้งานอัตโนมัติเมื่อไคลเอนต์ตรวจพบข้อจำกัดของเครือข่าย โดยให้รายการเซิร์ฟเวอร์ที่คัดสรรและปรับให้เหมาะสำหรับหลบการบล็อกในพื้นที่

Q5: Surfshark ใช้เซิร์ฟเวอร์แบบ RAM-only หรือไม่?

ใช่ เครือข่ายทั้งหมดของ Surfshark ทำงานบนเซิร์ฟเวอร์ที่ไม่มีดิสก์และใช้ RAM เท่านั้น ดังนั้นข้อมูลในหน่วยความจำจะถูกล้างเมื่อเซิร์ฟเวอร์รีบูต

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q6: Surfshark Bypasser คืออะไร?

Bypasser เป็นฟีเจอร์ split-tunneling ของ Surfshark ช่วยให้คุณเลือกแอปหรือเว็บไซต์เฉพาะเพื่อข้ามการเข้ารหัสของ VPN และส่งผ่าน ISP ในพื้นที่ของคุณ

Q7: Surfshark ใช้งานบนสมาร์ททีวีและเครื่องเกมคอนโซลได้หรือไม่?

ใช่ Surfshark มีบริการ Smart DNS ที่ให้คุณกำหนดค่า DNS บนสมาร์ททีวีและเครื่องคอนโซลเพื่อปลดบล็อกสื่อสตรีมมิง

Q8: โหมด Camouflage ของ Surfshark คืออะไร?

โหมด Camouflage คือฟีเจอร์อำพรางทราฟฟิกของ Surfshark โดยจะลบลายเซ็น VPN ออกจากการเชื่อมต่อของคุณ เพื่อไม่ให้ผู้ให้บริการอินเทอร์เน็ตของคุณทราบว่าคุณใช้ VPN

Q9: Surfshark มีเสิร์ชเอนจินรวมอยู่ด้วยหรือไม่?

ใช่ Surfshark มี Surfshark Search เสิร์ชเอนจินส่วนตัวที่ไม่มีโฆษณาและไม่ติดตามคำค้นหรือประวัติการค้นหาของคุณ [9]

Q10: Surfshark Alert คืออะไร?

Surfshark Alert เป็นเครื่องมือเฝ้าระวังดาร์กเว็บที่สแกนฐานข้อมูลเพื่อหาที่อยู่อีเมล รหัสผ่าน และรายละเอียดบัตรเครดิตที่รั่วไหล และแจ้งเตือนคุณเมื่อเกิดการรั่วไหล [10]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q1: โหมด Camouflage ของ Surfshark ซ่อนทราฟฟิก VPN ได้อย่างไร?

โหมด Camouflage ใช้การอำพราง OpenVPN เพื่อลบลายเซ็น VPN ออกจากส่วนหัวแพ็กเก็ต ทำให้ทราฟฟิกดูเหมือนการท่องเว็บ HTTPS ทั่วไป สำหรับเครื่องมือตรวจสอบแพ็กเก็ตเชิงลึก

Q2: ผลทางกฎหมายของการที่ Surfshark ดำเนินงานภายใต้เขตอำนาจของเนเธอร์แลนด์คืออะไร?

Surfshark ดำเนินงานภายใต้กฎหมายเนเธอร์แลนด์ เนเธอร์แลนด์เป็นประเทศในกลุ่ม 9-Eyes แต่กฎหมายไม่ได้กำหนดให้ผู้ให้บริการ VPN เก็บบันทึกข้อมูลผู้ใช้ ซึ่งทำให้ Surfshark รักษานโยบายไม่เก็บบันทึกที่ผ่านการตรวจสอบได้ [2]

Q3: ฟีเจอร์ split tunneling Bypasser ใน Surfshark ทำงานอย่างไร?

Bypasser แก้ไขตารางการกำหนดเส้นทางของระบบ ช่วยให้ผู้ใช้กำหนดแอปพลิเคชันหรือ URL เว็บไซต์ที่ส่งตรงผ่านเกตเวย์ ISP ในพื้นที่แทนอุโมงค์ VPN ที่เข้ารหัส

Q4: การเชื่อมต่อ WireGuard ของ Surfshark ใช้ไซเฟอร์การเข้ารหัสใด?

Surfshark รักษาความปลอดภัยทราฟฟิก WireGuard ด้วยรหัสกุญแจสมมาตร ChaCha20 พร้อมตัวยืนยันตัวตน Poly1305 ให้การเข้ารหัสความเร็วสูง

Q5: Nexus IP Rotator ทำงานโดยไม่ตัดการเชื่อมต่อ VPN ได้อย่างไร?

สถาปัตยกรรม SDN เชื่อมต่อไคลเอนต์กับเกตเวย์ในพื้นที่ เกตเวย์จะหมุนเวียน IP ขาออกในอีกชั้นหนึ่ง เพื่อให้การเข้ารหัสอุโมงค์ของไคลเอนต์ไม่ต้องเจรจาใหม่และยังคงการเชื่อมต่อไว้

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q6: สถาปัตยกรรม SDN ของ Surfshark Nexus ปรับการกำหนดเส้นทางให้เหมาะสมได้อย่างไร?

Nexus เชื่อมต่อเซิร์ฟเวอร์ทั้งหมดเป็นโครงข่ายเครือข่ายเดียวกัน แทนที่จะสร้างอุโมงค์ไปยังโหนดเดียว ไคลเอนต์เชื่อมต่อกับเกตเวย์ขาเข้า และ SDN จะกำหนดเส้นทางแพ็กเก็ตไปยังเกตเวย์ขาออกที่เหมาะสมที่สุดแบบไดนามิก ช่วยลดความหน่วง

Q7: เซิร์ฟเวอร์ RAM-only 100% ของ Surfshark มีข้อได้เปรียบด้านความปลอดภัยอะไร?

เซิร์ฟเวอร์แบบ RAM-only เก็บไฟล์ปฏิบัติการและคีย์เข้ารหัสทั้งหมดไว้ในหน่วยความจำแบบ volatile หากไฟดับหรือเซิร์ฟเวอร์ถูกยึด ข้อมูลที่เก็บในหน่วยความจำจะสูญหาย เหลือสิ่งให้กู้คืนได้น้อยมาก

Q8: โหมด NoBorders ตรวจจับเครือข่ายที่ถูกจำกัดอย่างไร?

แอปไคลเอนต์ทำการทดสอบการเชื่อมต่อไปยังจุดปลายทางสำคัญ หากตรวจพบการทิ้งแพ็กเก็ตแบบการเซ็นเซอร์หรือการเปลี่ยนเส้นทาง DNS จะเปลี่ยนเส้นทางไคลเอนต์ไปยังเซิร์ฟเวอร์เฉพาะทางโดยอัตโนมัติ

Q9: IKEv2 และ WireGuard บน Surfshark มีความแตกต่างด้านการเข้ารหัสอย่างไร?

IKEv2 ใช้ IPSec ที่มีการแลกเปลี่ยนคีย์แบบ Diffie-Hellman และการเข้ารหัส AES ขณะที่ WireGuard ใช้การเข้ารหัสลับสมัยใหม่ เช่น Noise Protocol Framework, Curve25519 และ ChaCha20-Poly1305

Q10: MultiHop ของ Surfshark ที่เป็น VPN สองชั้นรักษาความปลอดภัยเส้นทางการเชื่อมต่อได้อย่างไร?

MultiHop ส่งการรับส่งข้อมูลของคุณผ่านเซิร์ฟเวอร์ VPN สองเครื่องที่แยกกันในต่างประเทศ เซิร์ฟเวอร์แรกเข้ารหัสและกำหนดเส้นทางแพ็กเก็ต ส่วนเซิร์ฟเวอร์ที่สองถอดรหัสและส่งต่อ ทำให้การรับส่งข้อมูลสืบย้อนกลับมาหาคุณได้ยากขึ้นมาก

ส่วนที่ 11: ข้อเท็จจริง VPN ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับความเร็วการเข้ารหัส VPN การตรวจสอบโปรโตคอล การเชื่อมต่อบนมือถือ และการทำงานระยะไกลขององค์กร

1. ข้อมูลเชิงลึกเรื่อง VPN

Surfshark มีสำนักงานใหญ่ในเนเธอร์แลนด์และดำเนินงานภายใต้แนวทางทางกฎหมายและความเป็นส่วนตัวของเนเธอร์แลนด์ [1]

2. ข้อมูลเชิงลึกเรื่อง VPN

ผู้ให้บริการอนุญาตให้เชื่อมต่อพร้อมกันได้ไม่จำกัดจำนวนอุปกรณ์ โดยไม่กำหนดเพดานการเข้าสู่ระบบด้วยฮาร์ดแวร์ต่อบัญชีผู้ใช้

3. ข้อมูลเชิงลึกเรื่อง VPN

CleanWeb 2.0 บล็อกโฆษณา พิกเซลติดตาม มัลแวร์ และป๊อปอัปคุกกี้ในระดับเบราว์เซอร์และไคลเอนต์ [3]

4. ข้อมูลเชิงลึกเรื่อง VPN

สถาปัตยกรรม Surfshark Nexus เชื่อมเซิร์ฟเวอร์ทั้งหมดเข้าเป็นเครือข่ายที่กำหนดโดยซอฟต์แวร์ (Software-Defined Network) เพื่อให้หมุนเวียน IP ขาออกได้แบบไดนามิก [4]

5. ข้อมูลเชิงลึกเรื่อง VPN

โหมด NoBorders เปิดโดยอัตโนมัติเมื่อไคลเอนต์ตรวจพบข้อจำกัดของเครือข่ายในพื้นที่ และแสดงเซิร์ฟเวอร์ที่ปรับให้เหมาะสม [5]

6. ข้อมูลเชิงลึกเรื่อง VPN

เซิร์ฟเวอร์ Surfshark ทั้งหมดทำงานบนฮาร์ดแวร์ไร้ดิสก์ที่ใช้ RAM 100% หมายความว่าไม่มีไฟล์เซสชันถูกเขียนลงดิสก์

7. ข้อมูลเชิงลึกด้าน VPN

โหมด Camouflage อำพรางทราฟฟิก OpenVPN โดยลบส่วนหัว VPN ออก เพื่อให้ดูเหมือนการท่องเว็บที่ปลอดภัยตามปกติ [12]

8. ข้อมูลเชิงลึกด้าน VPN

แอปไคลเอนต์มี Kill Switch ที่ตัดการเข้าถึงอินเทอร์เน็ตของระบบหากการเชื่อมต่อ VPN ถูกขัดจังหวะ [11]

9. ข้อมูลเชิงลึกด้าน VPN

Bypasser เป็นเครื่องมือ split-tunneling เฉพาะของ Surfshark รองรับการยกเว้นทั้งแอปพลิเคชันและเว็บไซต์ [7]

10. ข้อมูลเชิงลึกเรื่อง VPN

VPN ใช้การเข้ารหัส ChaCha20 สำหรับ WireGuard ซึ่งเร็วและเบากว่า AES บนโปรเซสเซอร์มือถือ

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานทางเทคนิค ข้อกำหนดเฉพาะ และกรอบการกำกับดูแลระดับโลก

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

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

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

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

[4] Surfshark. (n.d.). Surfshark Nexus technology – elevating VPNs to the next level.
https://surfshark.com/features/nexus

[5] Surfshark. (n.d.). Avoid network restrictions with NoBorders VPN.
https://surfshark.com/features/noborders

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

[7] Surfshark. (n.d.). What is VPN split tunneling and how does it work?
https://surfshark.com/features/bypasser

[8] VPN.com. (n.d.). Surfshark Review: Unlimited Devices, Unbeatable Value.
https://www.vpn.com/vpn/surfshark/

[9] Surfshark. (n.d.). Hide your searches.
https://surfshark.com/search

[10] Surfshark. (n.d.). Surfshark Alert: protect your personal information.
https://surfshark.com/alert

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

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

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

CleanWeb บล็อกโฆษณา ตัวติดตาม มัลแวร์ และป๊อปอัปคุกกี้ ทั้งในแอปและในส่วนขยายเบราว์เซอร์ของ Surfshark

2 คำถาม 2 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

Nexus เชื่อมเซิร์ฟเวอร์ของ Surfshark เข้าเป็นเครือข่ายที่กำหนดด้วยซอฟต์แวร์เครือข่ายเดียว ซึ่งซับเคลื่อนฟีเจอร์อย่าง Rotating IP

3 คำถาม 3 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

ทุกแพ็กเกจของ Surfshark อนุญาตให้เชื่อมต่ออุปกรณ์พร้อมกันได้ไม่จำกัดในหนึ่งบัญชี

4 คำถาม 4 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

NoBorders เปิดโดยอัตโนมัติเมื่อแอปตรวจพบการจำกัดเครือข่ายและแนะนำเซิร์ฟเวอร์ที่ใช้งานได้ในที่นั้น

5 คำถาม 5 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

เซิร์ฟเวอร์ Surfshark ทั้งหมดเป็นแบบ RAM เท่านั้น จึงไม่มีการเขียนอะไรลงดิสก์ และข้อมูลจะถูกล้างทุกครั้งที่รีบูต

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: CleanWeb ใช้งานได้ทั้งในแอปและส่วนขยายเบราว์เซอร์ โดยบล็อกโฆษณา ตัวติดตาม และป๊อปอัปขอความยินยอมคุกกี้

7 **คำถาม 7** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: Nexus เชื่อมเซิร์ฟเวอร์ทั้งหมดเข้าเป็น SDN เดียว ซึ่งช่วยเพิ่มประสิทธิภาพการกำหนดเส้นทางและทำให้หมุนเวียน IP ได้

8 **คำถาม 8** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: Surfshark ไม่จำกัดจำนวนอุปกรณ์ ทุกแพ็กเกจอนุญาตการเชื่อมต่อพร้อมกันได้ไม่จำกัด

9 **คำถาม 9** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: เมื่อ NoBorders ตรวจพบการจำกัด จะแสดงรายการเซิร์ฟเวอร์ที่ทำงานได้ดีที่สุดภายใต้การจำกัดนั้น

10 **คำถาม 10** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: Surfshark B.V. จดทะเบียนที่อัมสเตอร์ดัมและดำเนินงานภายใต้กฎหมายดัตช์

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

D 1. CleanWeb	F 2. Nexus	H 3. ไม่จำกัด	B 4. NoBorders
G 5. RAM-only	C 6. Camouflage	E 7. Bypasser	A 8. WireGuard

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 คลีนเว็บ	2 ไม่จำกัด	3 เน็กซัส	4 โนบอร์เดอร์ส
5 แรมล้วน	6 คาโมฟลาจ		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 E – แรมล้วน	2 A – คลีนเว็บ	3 D – โนบอร์เดอร์ส	4 C – ไม่จำกัด
5 B – เน็กซัส	6 G – บายพาส	7 H – ไวร์การ์ด	8 F – คาโมฟลาจ

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย CleanWeb Nexus และ ไม่จำกัด ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

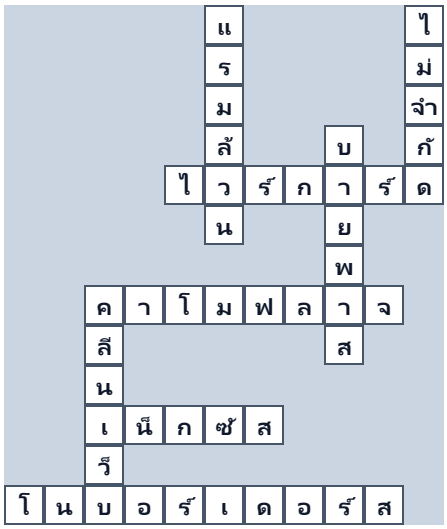
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	ส	ฟ	บ	า	า	ห	นี	า	ม	กี	จ	า	า
รี	ต	า	ว	ย	ง	ก	ค	ค	จ	น	ตี	ว	ร	ตี
ว	า	พ	ล	ล	ด	า	อ	ย	ลี	ช	ฟ	ก	ก	ล
ม	า	ย	น	ว	ล้	ม	ร	แ	ป	น	อ	อ	ม	มี
า	ล	า	ล	ป	โ	จ	า	นี	กี	พ	เ	ร	ง	า
ด	ช	บ	า	า	น	ลี	ค	จ	ส	ดี	า	ว็	น	ล
ร์	ผ	ดี	ช	ก	บ	ด	า	า	ต	ช้	า	จ	บ	า
า	ค	ก	ดี	า	อ	ช	ว	ก	โ	ด	ก	กี	ด	ท
ก	ผ	ฟ	ช	มี	ร์	ม	อ	ต	ฟ	ม	ร	น็	ดี	า
ร์	ท	า	ส	ท	เ	ไ	ข	ข	า	น	ฟ	ก	เ	า
ว	ล	า	ม	ร	ด	ม่	มี	า	ร	ช	ก	ล	ด	ง
ไ	น	ร	ต	สี	อ	จำ	ย	ข	มี	ดี	ด	ด	า	ว
บ	ฟ	อ	า	ร	ร์	กั	ห	ห	รี	น	ผ	นี	ม	จ
ผ	ดี	ข	กี	ส	ส	ด	บ	ลี	ง	ด	ร	ด	ค	ผ
ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด	บ	ตี	น

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

4 แนวนอน: ไวร์การ์ด โปรโตคอลเชื่อมต่อโอเพนซอร์สความเร็วสูงสมัยใหม่ (7 ตัวอักษร)

5 แนวนอน: คาโมฟลาจ เทคโนโลยีพรางที่ปกปิดทราฟฟิก VPN ให้เป็น HTTPS (8 ตัวอักษร)

6 แนวนอน: เน็กซัส เครือข่ายเซิร์ฟเวอร์ SDN ที่ทำให้หมุนเวียนไอพีและฮอปได้ (5 ตัวอักษร)

7 แนวนอน: โนบอร์เดอร์ส โหมดข้ามการเซ็นเซอร์ที่ปรับให้เหมาะกับโหนดที่ถูกจำกัด (10 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: แรมล้วน ฮาร์ดแวร์เซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เก็บล็อกในหน่วยความจำชั่วคราวเลย (6 ตัวอักษร)

2 แนวตั้ง: ไม่จำกัด นโยบายการสมัครที่อนุญาตการเชื่อมต่ออุปกรณ์ได้ไม่จำกัด (5 ตัวอักษร)

3 แนวตั้ง: บายพาส การใช้งานการแยกอุโมงค์ที่กำหนดเส้นทางแอปเฉพาะ (6 ตัวอักษร)

5 แนวตั้ง: คลีนเว็บ ตัวบล็อกโฆษณา ตัวติดตาม ป๊อปอัป และมัลแวร์ขั้นสูง (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. นคเว็บลี — คลีนเว็บ
2. ไดกัจำม่ — ไม่จำกัด
3. แมล้นวร — แรมล้วน
4. สพยาบา — บายพาส
5. กสเซ้น็ — เน็กซัส
6. ร์ร์อดอโนเสบ — โนบอร์เดอร์ส
7. คจฟลาามโ — คาโมฟลาจ
8. วกดไร์าร์ — ไวร์การ์ด

เฉลยภารกิจรหัสลับ

"เน็กซัส ทำงาน ระบบ สลับ ไอพี"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: ความปลอดภัยของการหมุนเวียน IP ของ Nexus

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: นักข่าวอิสระกำลังอัปโหลดบทสัมภาษณ์ที่ละเอียดอ่อน เพื่อป้องกันการติดตามโดยบุคคลที่สามที่อาจเฝ้าดู IP ปลายทาง เขาเปิดใช้ Surfshark Nexus IP Rotation ซึ่งเปลี่ยน IP ขาออกประมาณทุกห้านาทีโดยไม่ตัดการเชื่อมต่อ
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: การหมุนเวียน IP เปลี่ยนที่อยู่ IP ขาออกแบบไดนามิก ป้องกันไม่ให้ตัวติดตามรวบรวมบันทึกทราฟฟิกต่อเนื่องที่เชื่อมโยงกับ IP แบบคงที่เพียงหมายเลขเดียว

B กรณีศึกษาที่ 2: การทดสอบการเชื่อมต่ออุปกรณ์ไม่จำกัด

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ผู้ดูแลไอทีใช้การสมัคร Surfshark เดียวเพื่อรักษาความปลอดภัยอุปกรณ์ทดสอบทั้งหมดในห้องทดลอง โดยเชื่อมต่อสมาร์ทโฟนและแล็ปท็อปทดสอบ 45 เครื่องพร้อมกันกับเซิร์ฟเวอร์ภายใน
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ช่วยขจัดข้อจำกัดการเชื่อมต่อและข้อขัดแย้งในการเข้าสู่ระบบ ทำให้นักพัฒนาขยายสภาพแวดล้อมทดสอบได้โดยไม่ต้องจัดการหลายบัญชี