ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

รีวิว IPVanish

การวิเคราะห์ทางเทคนิคของ IPVanish VPN ที่มีสำนักงานใหญ่ในสหรัฐฯ เซิร์ฟเวอร์ที่เป็นเจ้าของเองเป็นส่วนใหญ่

ภาพรวมการเรียนรู้รีวิว IPVANISH

ผู้เรียน
สถานะนักเรียน
สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย
สถานะการเชื่อมต่อ
การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน
การป้องกันการรั่วไหล
การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการรีวิวทางเทคนิคของ IPVanish คุณจะได้สำรวจโครงสร้างพื้นฐานจริงที่เป็นเจ้าของเอง พร็อกซี SOCKS5 สำหรับทอร์เรนต์ P2P ประสิทธิภาพของ WireGuard และกฎระเบียบข้อมูลของเขตอำนาจศาลสหรัฐฯ

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/ipvanish/

เส้นทางการเรียนรู้ IPVanish ของคุณ

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

คำแนะนำรีวิว IPVANISH

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ พร็อกซี SOCKS5 และโครงสร้างพื้นฐานเซิร์ฟเวอร์ที่เป็นเจ้าของเอง ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

โครงสร้างพื้นฐานที่เป็นเจ้าของเองและพร็อกซี SOCKS5 P2P (บทนำ)

IPVanish โดดเด่นด้วยการเป็นเจ้าของและบริหารจัดการเครือข่ายเซิร์ฟเวอร์จริงส่วนใหญ่ของตน ซึ่งช่วยปรับปรุงประสิทธิภาพและความปลอดภัย มีโปรโตคอล WireGuard ความเร็วสูงและพร็อกซี SOCKS5 สำหรับทอร์เรนต์แบบ P2P แต่ดำเนินงานภายใต้เขตอำนาจศาล Five Eyes ของสหรัฐฯ

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. โปรโตคอลโอเพนซอร์สใดเป็นค่าเริ่มต้นเพื่อความเร็วสูงในแอปไคลเอนต์ IPVanish?
   - A) WireGuard
   - B) L2TP/IPSec
   - C) PPTP
   - D) Catapult Hydra

2. IPVanish ให้พร็อกซีเซิร์ฟเวอร์ประเภทใดเพื่อช่วยในการตั้งค่าทอร์เรนต์ P2P?
   - A) พร็อกซี SOCKS5
   - B) พร็อกซี HTTP
   - C) รีเลย์ Tor
   - D) Shadowsocks

3. บริษัทใดเป็นผู้ตรวจสอบการไม่เก็บบันทึกโดยอิสระครั้งแรกของ IPVanish ในปี 2022?
   - A) Leviathan Security Group
   - B) PwC
   - C) Deloitte
   - D) Cure53

4. นิติบุคคลขององค์กร IPVanish ดำเนินงานภายใต้เขตอำนาจศาลของประเทศใดเป็นหลัก?
   - A) สหรัฐอเมริกา
   - B) สวิตเซอร์แลนด์
   - C) ปานามา
   - D) หมู่เกาะเวอร์จินของอังกฤษ

5. แพ็กเกจพรีเมียมของ IPVanish อนุญาตให้เชื่อมต่อพร้อมกันได้กี่อุปกรณ์?
   - A) ไม่จำกัด
   - B) ห้า
   - C) สิบ
   - D) เจ็ด

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. IPVanish บริหารจัดการและเป็นเจ้าของโครงสร้างพื้นฐานเซิร์ฟเวอร์จริงส่วนใหญ่ของตน

○ จริง ○ เท็จ

7 คำถาม 7

7. ทราฟฟิกพร็อกซี SOCKS5 ถูกเข้ารหัสอย่างสมบูรณ์ระหว่างส่งผ่านเหมือนอุโมงค์ VPN มาตรฐาน

○ จริง ○ เท็จ

8 คำถาม 8

8. ไคลเอนต์เดสก์ท็อป IPVanish ไม่มีฟีเจอร์ Kill Switch ระดับระบบ

○ จริง ○ เท็จ

9 คำถาม 9

9. IPVanish ดำเนินงานจากสหรัฐอเมริกา ซึ่งเป็นสมาชิกข่าวกรอง Five Eyes

○ จริง ○ เท็จ

10 คำถาม 10

10. Split tunneling ใน IPVanish ช่วยให้ส่งทราฟฟิกของแอปออกนอกอุโมงค์ VPN ได้

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. โปรโตคอล _____ สมัยใหม่ถูกกำหนดเป็นค่าเริ่มต้นเพื่อประสิทธิภาพการกำหนดเส้นทางที่เหมาะสม
2. ทราฟฟิก P2P สามารถส่งผ่าน _____ ที่รวดเร็วเพื่อปกปิดตำแหน่งจริงของไคลเอนต์
3. การเชื่อมต่อกับโหนดที่อยู่ใกล้ทางภูมิศาสตร์ช่วยให้ได้ _____ จริงสูงสุด
4. เพื่อป้องกันข้อมูลรั่วไหล ผู้ใช้ควรตั้งค่าการควบคุม _____ ที่มีในตัว
5. การตรวจสอบความปลอดภัยอิสระรับรองคำมั่นของผู้ให้บริการเรื่อง _____
6. ต่างจากคู่แข่งบางราย IPVanish ไม่กำหนด _____ ใด ๆ ต่อบัญชี

คลังคำศัพท์

ขีดจำกัด | ความปลอดภัย | ความเร็ว | คิลสวิตช์ | ซ็อกส์ห้า | ที่อยู่ไอพี | ไม่เก็บล็อก | ไวร์การ์ด

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่อง VPN และเครือข่าย

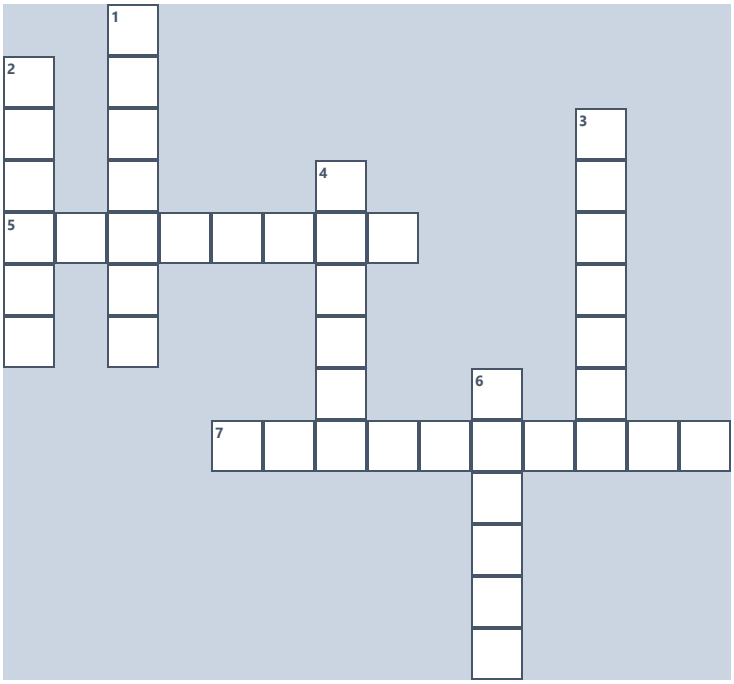
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. WireGuard**	**A**	กลไกป้องกันความล้มเหลวที่บล็อกทราฟฟิกอินเทอร์เน็ตหาก VPN ล้มเหลว
☐	**2. พร็อกซี SOCKS5**	**B**	โปรโตคอลโอเพนซอร์สที่ขึ้นชื่อเรื่องความเร็วและการเข้ารหัสสมัยใหม่
☐	**3. ความเร็วเซิร์ฟเวอร์**	**C**	ข้อจำกัดที่กำหนดจำนวนเซสชันอุปกรณ์ที่ใช้งานอยู่
☐	**4. Kill Switch**	**D**	ความสามารถด้านปริมาณงานของโหนดเซิร์ฟเวอร์ภายใต้ทราฟฟิกที่ใช้งานอยู่
☐	**5. ล็อกที่ผ่านการตรวจสอบ**	**E**	ตัวระบุเครือข่ายเฉพาะที่กำหนดให้อุปกรณ์บนอินเทอร์เน็ต
☐	**6. ขีดจำกัดอุปกรณ์**	**F**	สถานะการป้องกันโดยรวมของระบบอุโมงค์ที่เข้ารหัส
☐	**7. ที่อยู่ IP**	**G**	บันทึกที่ผ่านการตรวจสอบซึ่งยืนยันว่าไม่มีการติดตามกิจกรรมของผู้ใช้เลย
☐	**8. ความปลอดภัย**	**H**	ระบบกำหนดเส้นทางพร็อกซีที่ไม่เข้ารหัสซึ่งใช้ซ่อนตำแหน่งที่ตั้งของไคลเอนต์ P2P

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

5. บันทึกที่ผ่านการตรวจสอบยืนยันว่าไม่มีการติดตามกิจกรรมของผู้ใช้เลย (8)

7. สถานะการป้องกันโดยรวมของระบบอุโมงค์ที่เข้ารหัส (10)

แนวตั้ง

1. ความจุในการส่งผ่านข้อมูลของโหนดเซิร์ฟเวอร์ขณะมีทราฟฟิกจริง (7)

2. ตัวระบุเครือข่ายเฉพาะที่กำหนดให้อุปกรณ์บนอินเทอร์เน็ต (6)

3. โปรโตคอลโอเพนซอร์สที่มีชื่อเสียงด้านความเร็วและการเข้ารหัสสมัยใหม่ (7)

4. ระบบกำหนดเส้นทางพร็อกซีแบบไม่เข้ารหัสที่ใช้ปกปิดตำแหน่งของไคลเอนต์ P2P (6)

6. กลไกป้องกันความล้มเหลวที่บล็อกทราฟฟิกอินเทอร์เน็ตหาก VPN ขัดข้อง (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

5 แนวนอน: บันทึกที่ผ่านการตรวจสอบยืนยันว่าไม่มีการติดตามกิจกรรมของผู้ใช้เลย (8 ตัวอักษร):

7 แนวนอน: สถานะการป้องกันโดยรวมของระบบอุโมงค์ที่เข้ารหัส (10 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ความจุในการส่งผ่านข้อมูลของโหนดเซิร์ฟเวอร์ขณะมีทราฟฟิกจริง (7 ตัวอักษร):

2 แนวตั้ง: ตัวระบุเครือข่ายเฉพาะที่กำหนดให้อุปกรณ์บนอินเทอร์เน็ต (6 ตัวอักษร):

3 แนวตั้ง: โปรโตคอลโอเพนซอร์สที่มีชื่อเสียงด้านความเร็วและการเข้ารหัสสมัยใหม่ (7 ตัวอักษร):

4 แนวตั้ง: ระบบกำหนดเส้นทางพร็อกซีแบบไม่เข้ารหัสที่ใช้ปกปิดตำแหน่งของไคลเอนต์ P2P (6 ตัวอักษร):

6 แนวตั้ง: กลไกป้องกันความล้มเหลวที่บล็อกทราฟฟิกอินเทอร์เน็ตหาก VPN ขัดข้อง (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช	มี	ช์	ฟ	บ	า	า	ห	นี	า	ม	กี	จ	า	า
รี	ต	ต	ว	ย	ง	ก	ค	ค	จ	น	ตี	ว	ร	ตี
ว	า	วิ	ล	ล	ด	า	อ	ย	ว	ช	ฟ	ก	ก	ล
ม	า	ส	า	ห้	ส์	ก	อ	ซี	ป	า	อ	อ	ม	มี
า	ล	ล	ล	ป	ค	จ	า	พี	นี	กี	ม	พ	ร	ง
ด	า	คิ	ช	า	ว	า	ไ	ลี	อ	จ	ดี	เ	า	น
ร์	ล	ผ	ดี	ช	า	ก	ด	ม่	า	ไ	ต	า	ร็	จ
า	า	ค	ก	ดี	ม	า	ช	ว	เ	ก	ยู่	ด	กี	ว
ก	ด	ท	ผ	ฟ	ป	ช	มี	ม	อ	ก็	ต	อ	ฟ	ร
ร์	ดี	า	ท	า	ล	ขี	ส	ท	ข	ข	บ	า	ที่	น
ว	ก	า	ล	า	อ	ด	ม	ร	มี	า	ร	ล็	ช	ก
ไ	ด	ง	น	ร	ด	จำ	ต	สี	ย	ข	มี	ดี	อ	ด
ด	ว	บ	ฟ	อ	ภั	กั	า	ร	ห	ห	รี	น	ผ	ก
นี	ม	ผ	ดี	ข	ย	ด	กี	ส	บ	ลี	ง	ด	ร	ด
ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด	บ

รายการคำศัพท์

ไวร์การ์ด ซ็อกส์ห้า ความเร็ว คิลสวิตช์ ไม่เก็บล็อก ขีดจำกัด ที่อยู่ไอพี ความปลอดภัย

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. ไวร์การ์ด
B. ซ็อกส์ห้า
C. ความเร็ว
D. คิลสวิตช์
E. ไม่เก็บล็อก
F. ซีดจำกัด
G. ที่อยู่ไอพี
H. ความปลอดภัย

คำนิยามและช่องจับคู่	
	1. ระบบกำหนดเส้นทางพรือกซีแบบไม่เข้ารหัสที่ใช้ปกปิดตำแหน่งของไคลเอนต์ P2P
	2. สถานะการป้องกันโดยรวมของระบบอุโมงค์ที่เข้ารหัส
	3. ข้อจำกัดที่กำหนดจำนวนเซสชันอุปกรณ์ที่ใช้งานอยู่
	4. ความจุในการส่งผ่านข้อมูลของโหนดเซิร์ฟเวอร์ขณะมีทราฟฟิกจริง
	5. โปรโตคอลโอเพนซอร์สที่มีชื่อเสียงด้านความเร็วและการเข้ารหัสสมัยใหม่
	6. ตัวระบุเครือข่ายเฉพาะที่กำหนดให้อุปกรณ์บนอินเทอร์เน็ต
	7. กลไกป้องกันความล้มเหลวที่บล็อกทราฟฟิกอินเทอร์เน็ตหาก VPN ขัดข้อง
	8. บันทึกที่ผ่านการตรวจสอบยืนยันว่าไม่มีการติดตามกิจกรรมของผู้ใช้เลย

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของเครือข่ายส่วนตัวเสมือน (VPN) เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ก ร์ ไ า ด ร์ ว _____
2. ค า ว ร็ เ ม ว _____
3. ก็ ม่ ไ บ ล็ ก อ เ _____
4. พี ไ ยู่ อ ที่ อ _____
5. ส์ ก า ซ็ ห้ อ _____
6. ต วิ ค ิ ส ช์ ล _____
7. ก้ ด ขี จ่ า ด _____
8. ภ์ ม ล ย ค ป ว อ ด า _____

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	คำที่อธิบายแอป VPN ที่ดี			
2	สิ่งที่ IPVanish ซ่อนจากเครือข่ายของคุณได้			
3	สถานที่ที่คุณจะเปิดใช้ IPVanish			
4	โปรโตคอล VPN ที่คุณรู้จัก			
5	คำถามสำหรับฝ่ายสนับสนุนลูกค้าของ IPVanish			
6	ประเทศที่คุณอยากได้เซิร์ฟเวอร์ IPVanish			
7	บริการ VPN อื่นที่ไม่ใช่ IPVanish			
8	สถานการณ์ที่ kill switch ช่วยได้			
9	เหตุผลที่ควรเลือก IPVanish			
10	สัญญาณที่บ่งบอกว่าการเชื่อมต่อ VPN ของคุณช้า			
11	สิ่งที่คุณทำทางออนไลน์ทุกวัน			
12	คนที่คุณจะแนะนำ IPVanish ให้			
13	สิ่งที่ควรตรวจสอบก่อนซื้อ VPN			
14	คำศัพท์ด้านความปลอดภัยที่คุณเรียนรู้จากใบงานนี้			
15	สิ่งที่คุณมองหาใน IPVanish			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN และเครือข่าย

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การตั้งค่ามีเดียเซ็นเตอร์



สถานการณ์: ลูกค้าต้องการรักษาความปลอดภัยเครื่องเล่นสื่อ Android Fire TV โดยใช้ IPVanish เพื่อสตรีมอย่างปลอดภัยพร้อมรักษาอัตราส่งข้อมูลให้เร็ว

คำถามอภิปราย: เหตุใดโปรโตคอล WireGuard จึงเป็นที่นิยมมากกว่า OpenVPN สำหรับฮาร์ดแวร์สตรีมมิงที่มีทรัพยากรจำกัด?

กรณีศึกษาที่ 2: พร็อกซีเครือข่ายทอร์เรนต์



สถานการณ์: ผู้อัปโหลด P2P ต้องการซ่อนตำแหน่งของตนโดยไม่มีภาระของการเข้ารหัสข้อมูลเต็มรูปแบบ โดยใช้การตั้งค่า SOCKS5

คำถามอภิปราย: จงเปรียบเทียบข้อดีข้อเสียด้านความปลอดภัยและความเร็วระหว่างการใช้พร็อกซี SOCKS5 กับอุโมงค์ IPVanish VPN เต็มรูปแบบ

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

61	45	30	52	39	49	25	51	10		26	48	7	4	48	26

61	33	63	57	1	62	26	37	62	45	1		57	2	64	33	7	39	20

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q1: โปรโตคอลเริ่มต้นใน IPVanish คืออะไร?

กำหนดเส้นทางผ่าน WireGuard ความเร็วสูงเป็นค่าเริ่มต้น

Q2: IPVanish เป็นเจ้าของฮาร์ดแวร์เซิร์ฟเวอร์ของตนเองหรือไม่?

ได้ เป็นเจ้าของและบริหารเครือข่ายเซิร์ฟเวอร์จริงส่วนใหญ่เอง

Q3: IPVanish ตั้งอยู่ที่ไหน?

ตั้งอยู่ในสหรัฐอเมริกา จึงอยู่ภายใต้กฎหมายสหรัฐฯ

Q4: เชื่อมต่อพร้อมกันได้กี่อุปกรณ์?

IPVanish เสนอการเชื่อมต่อพร้อมกันได้ไม่จำกัดจำนวนอุปกรณ์ต่อบัญชี

Q5: เก็บบันทึกการเชื่อมต่อใดๆ หรือไม่?

ไม่ บังคับใช้นโยบายไม่เก็บล็อกอย่างเข้มงวดซึ่งผ่านการรับรองโดยการตรวจสอบอิสระ [6]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q6: IPVanish มีบริการพร็อกซีหรือไม่?

ได้ มีพร็อกซี SOCKS5 ฟรีสำหรับการดาวน์โหลดทอร์เรนต์

Q7: มี kill switch รวมอยู่ด้วยหรือไม่?

ใช่ มี kill switch บน Windows, macOS, Android และ iOS

Q8: ฉันหลบเลี่ยงการบล็อกตามภูมิศาสตร์ด้วย IPVanish ได้หรือไม่?

ได้ เครือข่ายเซิร์ฟเวอร์ทั่วโลกช่วยให้เข้าถึงห้องสมุดที่ถูกจำกัดได้

Q9: รองรับ split tunneling หรือไม่?

ได้ มีการแยกอุโมงค์ รวมถึงบน Windows และ Android

Q10: ใช้รหัสเข้ารหัสแบบใด?

รักษาความปลอดภัยการเชื่อมต่อด้วยการเข้ารหัส AES-256 และ ChaCha20

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q1: พร็อกซี SOCKS5 ถูกกำหนดค่าอย่างไร?

ตั้งค่าในไคลเอนต์ทอร์เรนต์เพื่อซ่อน IP ของผู้ใช้โดยไม่มีภาระจากการเข้ารหัส

Q2: การเป็นเจ้าของฮาร์ดแวร์เซิร์ฟเวอร์ช่วยเพิ่มความปลอดภัยอย่างไร?

ลดความเสี่ยงจากการเช่าเซิร์ฟเวอร์ของบุคคลที่สาม และให้ผู้ให้บริการควบคุมการกำหนดค่าเซิร์ฟเวอร์ได้โดยตรง

Q3: เขตอำนาจศาลของสหรัฐฯ มีผลกระทบต่อความเป็นส่วนตัวอย่างไร?

แม้กฎหมายสหรัฐอเมริกาจะไม่กำหนดให้เก็บรักษาข้อมูล แต่ก็อนุญาตให้ใช้หนังสือแจ้งความมั่นคงแห่งชาติและหมายค้นได้

Q4: kill switch ป้องกัน IP รั่วไหลได้อย่างไร?

บล็อกอะแดปเตอร์อินเทอร์เน็ตทั้งหมดหากการเชื่อมต่อ VPN หลุดโดยไม่คาดคิด

Q5: WireGuard ใช้การเข้ารหัสแบบใด?

WireGuard ใช้การเข้ารหัสด้วยกุญแจสมมาตร ChaCha20 และการยืนยันตัวตนด้วย Poly1305 [7]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q6: นโยบาย zero-logs ได้รับการตรวจสอบยืนยันอย่างไร?

Leviathan Security Group ตรวจสอบในปี 2022 และ Schellman ในปี 2025 โดยทั้งคู่ไม่พบล็อกของผู้ใช้ [3]

Q7: จัดการคำค้นหา DNS ผ่าน IPv6 อย่างไร?

กำหนดเส้นทางคำขอ DNS และ IPv6 ทั้งหมดผ่านเนมเซิร์ฟเวอร์ส่วนตัวของตนโดยอัตโนมัติ

Q8: IPVanish มีฟีเจอร์พรางทราฟฟิก (obfuscation) หรือไม่?

ได้ ฟีเจอร์ Scramble ช่วยอำพรางทราฟฟิก OpenVPN เพื่อข้ามไฟร์วอลล์

Q9: split tunneling ทำงานบนอุปกรณ์มือถืออย่างไร?

ช่วยให้แอปที่เลือกข้ามอุโมงค์ VPN และเชื่อมต่อโดยตรง

Q10: รองรับการกำหนดค่าบนเราเตอร์หรือไม่?

ใช่ สามารถโหลดการกำหนดค่า OpenVPN และ WireGuard ลงบนเราเตอร์ DD-WRT ด้วยตนเองได้ [1]

ส่วนที่ 11: ข้อเท็จจริง VPN ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับความเร็วการเข้ารหัส VPN การตรวจสอบโปรโตคอล การเชื่อมต่อบนมือถือ และการทำงานระยะไกลขององค์กร

1. ข้อมูลเชิงลึกเรื่อง VPN

IPVanish เป็นเจ้าของโครงสร้างพื้นฐานเซิร์ฟเวอร์ส่วนใหญ่ของตนเอง แทนที่จะเช่าจากบุคคลที่สาม [3]

2. ข้อมูลเชิงลึกเรื่อง VPN

IPVanish ดำเนินงานมาตั้งแต่ปี 2012 และเป็นของ Ziff Davis ซึ่งเดิมรู้จักกันในชื่อ J2 Global [2]

3. ข้อมูลเชิงลึกเรื่อง VPN

พร็อกซี SOCKS5 ซ่อนที่อยู่ IP สาธารณะของไคลเอนต์ แต่ไม่ได้เข้ารหัสแพ็กเก็ตข้อมูล

4. ข้อมูลเชิงลึกเรื่อง VPN

WireGuard เป็นโปรโตคอลเริ่มต้น โดยมี OpenVPN และ IKEv2/IPSec ให้ใช้ในแอปด้วย [2]

5. ข้อมูลเชิงลึกเรื่อง VPN

OpenVPN Scramble มาตรฐานเพิ่มชั้นการปกปิดแบบ XOR ให้กับส่วนหัวของแพ็กเก็ตเพื่อหลีกเลี่ยงไฟร์วอลล์

6. ข้อมูลเชิงลึกเรื่อง VPN

นโยบายการเชื่อมต่อพร้อมกันแบบไม่จำกัดช่วยให้ผู้ใช้ปกป้องอุปกรณ์ทั้งหมดในบ้านได้พร้อมกัน [2]

7. ข้อมูลเชิงลึกด้าน VPN

การตรวจสอบโดย Leviathan Security Group (2022) และ Schellman (2025) ยืนยันคำกล่าวอ้างเรื่อง no-logs [3]

8. ข้อมูลเชิงลึกด้าน VPN

แอป Android รองรับการตั้งค่า VPN แบบเปิดตลอดเวลา ซึ่งป้องกันการเข้าถึงอินเทอร์เน็ตหากอุโมงค์ขาดการเชื่อมต่อ

9. ข้อมูลเชิงลึกด้าน VPN

การเชื่อมต่อ OpenVPN ใช้ได้ทั้ง UDP เพื่อความเร็วหรือ TCP เพื่อการกำหนดเส้นทางที่เสถียรผ่านไฟร์วอลล์

10. ข้อมูลเชิงลึกเรื่อง VPN

มีแชตสดสนับสนุนตลอด 24/7 พร้อมการสนับสนุนทางโทรศัพท์ในเวลาทำการวันธรรมดาที่กำหนด [5]

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานทางเทคนิค ข้อกำหนดเฉพาะ และกรอบการกำกับดูแลระดับโลก

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] VPN.com. (2026). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **ค่าเริ่มต้น WireGuard** WIREGUARD คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

WireGuard ถูกกำหนดค่าเป็นค่าเริ่มต้นเพื่อความเร็วในการกำหนดเส้นทางที่เหมาะสมที่สุด การอ้างอิง: IPVanish Features.

2 **พร็อกซี SOCKS5** พร็อกซี SOCKS5 คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

พร็อกซี SOCKS5 ปกปิดตำแหน่งของไคลเอนต์โดยไม่มีภาระจากการเข้ารหัส การอ้างอิง: IPVanish Support.

3 **คำถาม 3** คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

Leviathan Security Group ดำเนินการตรวจสอบการไม่เก็บบันทึกครั้งแรกของ IPVanish ในปี 2022 และ Schellman ตามมาในปี 2025 [3]

4 **เขตอำนาจศาลสหรัฐฯ** สหรัฐอเมริกา คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

IPVanish ตั้งอยู่ในสหรัฐอเมริกา ภายใต้กฎของพันธมิตร Five Eyes การอ้างอิง: IPVanish Review.

5 **อุปกรณ์ไม่จำกัด** ไม่จำกัด คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

IPVanish อนุญาตให้เชื่อมต่อพร้อมกันได้ไม่จำกัดจำนวนอุปกรณ์ การอ้างอิง: IPVanish Support.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **ฮาร์ดแวร์เซิร์ฟเวอร์** เป็นเจ้าของเครือข่าย — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

IPVanish เป็นเจ้าของและบริหารจัดการเครือข่ายเซิร์ฟเวอร์จริงส่วนใหญ่ของตน การอ้างอิง: IPVanish Support.

7 **คำถาม 7** — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

เท็จ: พร็อกซี SOCKS5 ซ่อนที่อยู่ IP ของคุณแต่ไม่ได้เข้ารหัสข้อมูล

8 **คำถาม 8** — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

เท็จ: IPVanish มี kill switch ในแอปเดสก์ท็อปและมือถือ

9 **เขตอำนาจศาลสหรัฐฯ** FIVE EYES สหรัฐฯ — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

IPVanish ตั้งอยู่ในสหรัฐฯ จึงอยู่ภายใต้กฎการสอดแนมของ Five Eyes การอ้างอิง: IPVanish Review.

10 **อุโมงค์แบบแยก** เส้นทางแยก — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

Split tunneling ส่งทราฟฟิกของแอปเฉพาะออกนอกอุโมงค์ที่ปลอดภัย การอ้างอิง: IPVanish Support.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

B 1. WireGuard	H 2. พร็อกซี SOCKS5	D 3. ความเร็วเซิร์ฟเวอร์	A 4. Kill Switch
G 5. ล็อกที่ผ่านการตรวจสอบ	C 6. ขีดจำกัดอุปกรณ์	E 7. ที่อยู่ IP	F 8. ความปลอดภัย

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ไวร์การ์ด	2 ซ็อกส์ห้า	3 ความเร็ว	4 คิลสวิตช์
5 ไม่เก็บล็อก	6 ขีดจำกัด		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 B – ซ็อกส์ห้า	2 H – ความปลอดภัย	3 F – ขีดจำกัด	4 C – ความเร็ว
5 A – ไวร์การ์ด	6 G – ที่อยู่ไอพี	7 D – คิลสวิตช์	8 E – ไม่เก็บล็อก

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย WireGuard พร็อกซี SOCKS5 และ ความเร็วเซิร์ฟเวอร์ ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

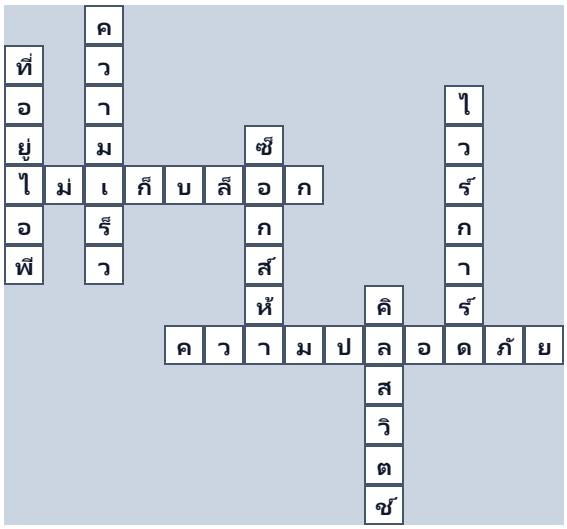
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	ช์	ฟ	บ	า	า	ห	นี	า	ม	กี	จ	า	า
รี	ต	ต	ว	ย	ง	ก	ค	ค	จ	น	ตี	ว	ร	ตี
ว	า	วิ	ล	ล	ด	า	อ	ย	ว	ช	ฟ	ก	ก	ล
ม	า	ส	า	ห้	ส์	ก	อ	ซ็	ป	า	อ	อ	ม	มี
า	ล	ล	ล	ป	ค	จ	า	พี	นี	กี	ม	พ	ร	ง
ด	า	คิ	ช	า	ว	า	ไ	ลี	อ	จ	ตี	เ	า	น
ร์	ล	ผ	ดี	ช	า	ก	ด	ม่	า	ไ	ต	า	ร็	จ
า	า	ค	ก	ตี	ม	า	ช	ว	เ	ก	ยู่	ด	กี	ว
ก	ด	ท	ผ	ฟ	ป	ช	มี	ม	อ	ก็	ต	อ	ฟ	ร
ร์	ดี	า	ท	า	ล	ขี	ส	ท	ข	ข	บ	า	ที่	น
ว	ก	า	ล	า	อ	ด	ม	ร	มี	า	ร	ล็	ช	ก
ไ	ด	ง	น	ร	ด	จำ	ต	สี	ย	ข	มี	ดี	อ	ด
ด	ว	บ	ฟ	อ	ภั	ก้	า	ร	ห	ห	รี	น	ผ	ก
นี	ม	ผ	ดี	ข	ย	ด	กี	ส	บ	ลี	ง	ด	ร	ด
ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด	บ

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

5 แนวนอน: ไม่เก็บล็อก บันทึกที่ผ่านการตรวจสอบยืนยันว่าไม่มีการติดตามกิจกรรมของผู้ใช้เลย (8 ตัวอักษร)

7 แนวนอน: ความปลอดภัย สถานะการป้องกันโดยรวมของระบบอุโมงค์ที่เข้ารหัส (10 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: ความเร็ว ความฉุในการส่งผ่านข้อมูลของโหนดเซิร์ฟเวอร์ขณะมีทราฟฟิกจริง (7 ตัวอักษร)

2 แนวตั้ง: ที่อยู่ไอพี ตัวระบุเครือข่ายเฉพาะที่กำหนดให้อุปกรณ์บนอินเทอร์เน็ต (6 ตัวอักษร)

3 แนวตั้ง: ไวร์การ์ด โปรโตคอลโอเพนซอร์สที่มีชื่อเสียงด้านความเร็วและการเข้ารหัสสมัยใหม่ (7 ตัวอักษร)

4 แนวตั้ง: ซ็อกส์ห้า ระบบกำหนดเส้นทางพร็อกซีแบบไม่เข้ารหัสที่ใช้ปกปิดตำแหน่งของไคลเอนต์ P2P (6 ตัวอักษร)

6 แนวตั้ง: คิลสวิตช์ กลไกป้องกันความล้มเหลวที่บล็อกทราฟฟิกอินเทอร์เน็ตหาก VPN ขัดข้อง (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. กร์ไาดร์ว — ไวร์การ์ด
2. คาวร็เมว — ความเร็ว
3. ก็มไบล็กอเ — ไม่เก็บล็อก
4. พ์ไยู่อที่อ — ที่อยู่ไอพี
5. ส์กาซ็ห้อ — ซ็อกส์ห้า
6. ตวิคิสช์ล — คิลสวิตช์
7. กัดขีจำด — ขีดจำกัด
8. ภัมลยคปวอดา — ความปลอดภัย

เฉลยภารกิจรหัสลับ

"ไอพีวานิช บังคับ ไม่เก็บล็อก เข้มงวด"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การตั้งค่ามีเดียเซ็นเตอร์

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ลูกค้าต้องการรักษาความปลอดภัยเครื่องเล่นมีเดีย Android Fire TV โดยใช้ IPVanish เพื่อสตรีมอย่างปลอดภัยพร้อมคงปริมาณงานที่รวดเร็ว
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: แนวทางการให้คะแนน: อธิบายว่า WireGuard มีโค้ดขนาดเล็กกว่า ทำงานในเคอร์เนลสเปซ และใช้รอบ CPU น้อยกว่า จึงเพิ่มความเร็วบนฮาร์ดแวร์สเปกเบาได้สูงสุด

B กรณีศึกษาที่ 2: พร็อกซีเครือข่ายทอร์เรนต์

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ผู้อัปโหลด P2P ต้องการซ่อนตำแหน่งของตนโดยไม่มีภาระจากการเข้ารหัสข้อมูลเต็มรูปแบบ โดยใช้การกำหนดค่า SOCKS5
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: แนวทางการให้คะแนน: ระบุว่า SOCKS5 ซ่อนที่อยู่ IP โดยไม่เข้ารหัสทราฟฟิก ให้ความเร็วสูงกว่า แต่ไม่มีความเป็นส่วนตัวเลยเมื่อเทียบกับการตรวจสอบแพ็กเก็ตโดย ISP