ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

ความปลอดภัยของ NordVPN

การตรวจสอบฟีเจอร์ความปลอดภัยของ NordVPN รวมถึงโปรโตคอล NordLynx, Double VPN, Onion Over VPN, Threat Protection, การตรวจสอบนโยบายไม่เก็บบันทึก และการเข้ารหัส AES-256

ภาพรวมการเรียนรู้ความปลอดภัย NORDVPN

ผู้เรียน
สถานะนักเรียน
สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย
สถานะการเชื่อมต่อ
การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน
การป้องกันการรั่วไหล
การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับฟีเจอร์ความปลอดภัยของ NordVPN คุณจะได้สำรวจ NordLynx เฉพาะของตน โหนด RAM ที่ไม่มีดิสก์ การเชื่อมต่อ Double VPN แบบต่อเนื่อง และการตรวจสอบนโยบายไม่เก็บล็อกโดยอิสระ

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/nordvpn/khwam-plodphai/

เส้นทางการเรียนรู้ความปลอดภัยของ NordVPN ของคุณ

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

คำแนะนำคู่มือความปลอดภัย NORDVPN

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ โปรโตคอลเข้ารหัสเฉพาะของผู้ให้บริการและโหนดเซิร์ฟเวอร์ที่ใช้ RAM เท่านั้น ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

โปรโตคอล NORDLYNX เฉพาะของบริษัทและการลดช่องโหว่

โปรโตคอล NordLynx เฉพาะของ NordVPN ผสาน WireGuard เข้ากับระบบ NAT สองชั้น ออกแบบเพื่อความเร็วโดยไม่จัดเก็บข้อมูลผู้ใช้ เซิร์ฟเวอร์ทำงานบนฮาร์ดแวร์ RAM ที่ไม่มีดิสก์ และ PwC กับ Deloitte ได้ยืนยันนโยบายไม่เก็บล็อกของ NordVPN มาแล้วหกครั้ง

(บทนำ)

โปรโตคอล NordLynx เฉพาะของ NordVPN ผสาน WireGuard เข้ากับระบบ NAT สองชั้น ออกแบบเพื่อความเร็วโดยไม่จัดเก็บข้อมูลผู้ใช้ เซิร์ฟเวอร์ทำงานบนฮาร์ดแวร์ RAM ที่ไม่มีดิสก์ และ PwC กับ Deloitte ได้ยืนยันนโยบายไม่เก็บล็อกของ NordVPN มาแล้วหกครั้ง

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. โปรโตคอลการเชื่อมต่อเฉพาะของ **NordVPN** คืออะไร?
   - A) OpenVPN
   - B) NordLynx
   - C) IKEv2
   - D) Lightway

2. สถาปัตยกรรมใดที่รันเซิร์ฟเวอร์บน **RAM** ชั่วคราวเท่านั้น?
   - A) Dual NAT
   - B) Meshnet
   - C) ระดับ RAM แบบไม่มีดิสก์
   - D) Split Tunneling

3. ฟีเจอร์ใดที่บล็อกโฆษณา ตัวติดตาม และโดเมนมัลแวร์?
   - A) Double VPN
   - B) NordLynx
   - C) Threat Protection
   - D) Onion Over VPN

4. **Double VPN** เพิ่มความปลอดภัยในการส่งข้อมูลอย่างไร?
   - A) เชื่อมเซิร์ฟเวอร์สองเครื่อง
   - B) เพิ่มแบนด์วิดท์เป็นสองเท่า
   - C) บีบอัดแพ็กเก็ต
   - D) ข้ามภาษี ISP

5. บริษัทอิสระใดตรวจสอบนโยบายไม่เก็บบันทึกของ **NordVPN**?
   - A) BDO
   - B) KPMG
   - C) Ernst & Young
   - D) Deloitte / PwC

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. NordLynx สร้างขึ้นโดยตรงบนโปรโตคอล WireGuard

○ จริง ○ เท็จ

7 คำถาม 7

7. Threat Protection Pro ต้องมีการเชื่อมต่อ VPN ที่ใช้งานอยู่จึงจะทำงานได้

○ จริง ○ เท็จ

8 คำถาม 8

8. IP เฉพาะให้ผู้ใช้หนึ่งคนมีที่อยู่ที่ไม่มีใครใช้ร่วมด้วย

○ จริง ○ เท็จ

9 คำถาม 9

9. App Kill Switch บล็อกทราฟฟิกทั่วทั้งระบบหากอุโมงค์หลุด

○ จริง ○ เท็จ

10 คำถาม 10

10. NordVPN เลือกใช้เซิร์ฟเวอร์ RAM แบบไม่มีดิสก์แทนเซิร์ฟเวอร์ที่ใช้ฮาร์ดไดรฟ์

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. โปรโตคอลเชื่อมต่อแบบกำหนดเองที่อิง **WireGuard** ถูก **NordVPN** ตั้งชื่อว่า _____
2. ข้อมูลถูกปกป้องจากการยึดฮาร์ดแวร์ในพื้นที่ด้วยโหนดไร้ดิสก์แบบ _____
3. มัลแวร์และตัวติดตามที่รุกล้ำถูกบล็อกด้วยฟีเจอร์ในตัวคือ _____
4. การส่งทราฟฟิกผ่านโหนดเข้ารหัสสองตัวทำได้ผ่านอุโมงค์ _____
5. **PwC** และ **Deloitte** ยืนยันนโยบาย _____ ที่เข้มงวดและไม่เก็บข้อมูลของ **NordVPN**
6. การเข้าถึงอินเทอร์เน็ตถูกตัดทันทีเมื่ออุโมงค์หลุดด้วยระบบป้องกันความล้มเหลว _____
7. สร้างการเชื่อมต่อปลอดภัยแบบเครือข่ายภายในข้ามอุปกรณ์ได้ด้วยการกำหนดเส้นทางแบบ _____
8. ความปลอดภัยของเพย์โหลดข้อมูลบังคับใช้ด้วยการเข้ารหัส **AES-256** และ **ChaCha20** ซึ่งเป็น _____

คลังคำศัพท์

คิลสวิตช์	ไซเฟอร์	นอร์ดลิงซ์	ป้องกันภัยนอร์ดลิงซ์	เมชเน็ตแรมล้วน	ไม่เก็บล็อก	แรมล้วน	วีพีเอ็นคู่

เขียนคำตอบของคุณที่นี่:

1.
2.
3.
4.
5.
6.
7.
8.

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่อง VPN และเครือข่าย

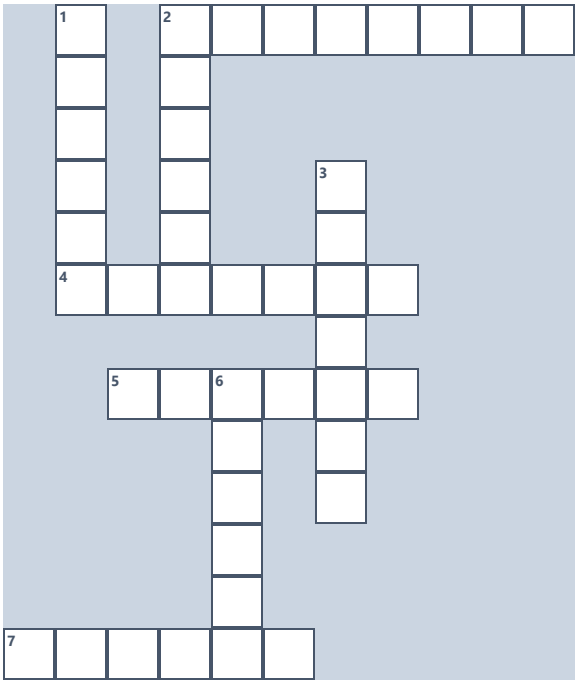
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. นอร์ดลิงซ์**	**A**	เครื่องมือกำหนดเส้นทางแบบกระจายศูนย์เพื่อเชื่อมต่ออุปกรณ์โดยตรง
☐	**2. โหนด RAM**	**B**	ชุดความปลอดภัยในเครื่องที่บล็อกตัวติดตาม โฆษณา และมัลแวร์
☐	**3. ป้องกันภัย**	**C**	อัลกอริทึมการเข้ารหัสที่ใช้ปกป้องข้อมูลเพย์โหลด
☐	**4. วีพีเอ็นคู่**	**D**	ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ไม่เก็บข้อมูลใดๆ เมื่อรีสตาร์ท
☐	**5. ไม่เก็บล็อก**	**E**	การเชื่อมเซิร์ฟเวอร์ VPN สองเครื่องเพื่อเข้ารหัสข้อมูลสองครั้ง
☐	**6. คิลสวิตช์**	**F**	โปรโตคอลเฉพาะของ NordVPN ที่สร้างบนมาตรฐาน WireGuard
☐	**7. เมชเน็ตซ์**	**G**	มาตรฐานการเก็บรักษาข้อมูลที่เข้มงวดซึ่งผ่านการตรวจสอบโดยหน่วยงานภายนอก
☐	**8. ไซเฟอร์**	**H**	ฟีเจอร์ความปลอดภัยที่ตัดทราฟฟิกเมื่อ VPN หลุด

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. มาตรฐานการเก็บข้อมูลที่เข้มงวดซึ่งผ่านการตรวจสอบจากภายนอก (8)

4. โปรโตคอลเฉพาะของ NordVPN ที่สร้างบนมาตรฐาน WireGuard (7)

5. การเชื่อมเซิร์ฟเวอร์ VPN สองตัวเข้าด้วยกันเพื่อเข้ารหัสข้อมูลสองครั้ง (6)

7. ฟีเจอร์ความปลอดภัยที่ตัดทราฟฟิกเมื่อ VPN หลุด (6)

แนวตั้ง

1. ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ไม่เก็บข้อมูลเมื่อรีสตาร์ต (6)

2. อัลกอริทึมเข้ารหัสลับที่ใช้รักษาความปลอดภัยของเพย์โหลดข้อมูล (6)

3. ชุดความปลอดภัยในเครื่องที่บล็อกตัวติดตาม โฆษณา และมัลแวร์ (7)

6. เครื่องมือกำหนดเส้นทางแบบกระจายศูนย์เพื่อเชื่อมต่ออุปกรณ์โดยตรง (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: มาตรฐานการเก็บข้อมูลที่เข้มงวดซึ่งผ่านการตรวจสอบจากภายนอก (8 ตัวอักษร):

4 แนวนอน: โปรโตคอลเฉพาะของ NordVPN ที่สร้างบนมาตรฐาน WireGuard (7 ตัวอักษร):

5 แนวนอน: การเชื่อมเซิร์ฟเวอร์ VPN สองตัวเข้าด้วยกันเพื่อเข้ารหัสข้อมูลสองครั้ง (6 ตัวอักษร):

7 แนวนอน: ฟีเจอร์ความปลอดภัยที่ตัดทราฟฟิกเมื่อ VPN หลุด (6 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ไม่เก็บข้อมูลเมื่อรีสตาร์ต (6 ตัวอักษร):

2 แนวตั้ง: อัลกอริทึมเข้ารหัสลับที่ใช้รักษาความปลอดภัยของเพย์โหลดข้อมูล (6 ตัวอักษร):

3 แนวตั้ง: ชุดความปลอดภัยในเครื่องที่บล็อกตัวติดตาม โฆษณา และมัลแวร์ (7 ตัวอักษร):

6 แนวตั้ง: เครื่องมือกำหนดเส้นทางแบบกระจายศูนย์เพื่อเชื่อมต่ออุปกรณ์โดยตรง (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 แ จ น ตี ว ร ตี
ว า วิ ล ล ด า อ ย ร ซ ฟ ก ก ล
ม า ส คู่ น อ็ เ พี วี ป ม อ อ ม มี
า ล ล ล ป ไ จ า ต นี กี ล้ พ ร ง
ย า คิ ซ า ม่ า น ลี น็ จ ดี ว า น
ภั ล ผ ดี ซ เ ก ด อ า เ ต า น จ
น า ค ก ดี ก็ า ซ ว ร์ ก ช ด กี ด
กั ท ผ ฟ ซ บ มี ม อ ต ด ฟ ม ร ดี
ง า ท า ส ล็ ไ ท ข ข า ลิ น เ ก
อ า ล า ม อ ซ ร มี า ร ช ง ก ด
ป้ ง น ร ต ก เ สี ย ข มี ดี ด ซ์ ด
ว บ ฟ อ า ร ฟ ห ห รี น ผ นี ม ผ
ดี ข กี ส บ ลี อ ง ด ร ด ค ผ ห ดี
ป ร กี นี า ต ร์ จ ห ดี ด บ ตี น สี

รายการคำศัพท์

นอร์ดลิงซ์ แรมล้วน ป้องกันภัย วีพีเอ็นคู่ ไม่เก็บล็อก คิลสวิตช์ เมชเน็ต ไซเฟอร์

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. นอร์ดลิงซ์
B. แรมล้วน
C. ป้องกันภัย
D. วีพีเอ็นคู่
E. ไม่เก็บล็อก
F. คิลสวิตช์
G. เมชเน็ต
H. ไซเฟอร์

คำนิยามและช่องจับคู่
1. อัลกอริทึมเข้ารหัสลับที่ใช้รักษาความปลอดภัยของเพย์โหลดข้อมูล
2. ฟีเจอร์ความปลอดภัยที่ตัดทราฟฟิกเมื่อ VPN หลุด
3. เครื่องมือกำหนดเส้นทางแบบกระจายศูนย์เพื่อเชื่อมต่ออุปกรณ์โดยตรง
4. ชุดความปลอดภัยในเครื่องที่บล็อกตัวติดตาม โฆษณา และมัลแวร์
5. การเชื่อมเซิร์ฟเวอร์ VPN สองตัวเข้าด้วยกันเพื่อเข้ารหัสข้อมูลสองครั้ง
6. โปรโตคอลเฉพาะของ NordVPN ที่สร้างบนมาตรฐาน WireGuard
7. มาตรฐานการเก็บข้อมูลที่เข้มงวดซึ่งผ่านการตรวจสอบจากภายนอก
8. ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ไม่เก็บข้อมูลเมื่อรีสตาร์ต

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของเครือข่ายส่วนตัวเสมือน (VPN) เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ด ง น ล ิ ซ ์ ร ์ อ
2. ป ้ ง ย ก ั น ก ั อ
3. ก ็ ม ่ ไ บ ล ็ ก อ เ
4. ต เ ช ห น ็ เ ม
5. ล ้ ม น แ ว ร
6. น อ ็ ว ี เ ค ู่ พ ี
7. ต ค ิ ว ิ ซ ์ ส ล
8. เ ร ์ ไ อ ฟ ซ

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	สัญญาณที่บ่งบอกว่าการเชื่อมต่อ VPN ของคุณช้า			
2	วิธีสร้างรหัสผ่านที่รัดกุม			
3	แอปที่คุณจะใช้ร่วมกับ NordVPN			
4	เหตุผลที่ควรเลือก NordVPN			
5	ประเทศที่คุณอยากได้เซิร์ฟเวอร์ NordVPN			
6	ประเภทของการรั่วไหลของ VPN			
7	โปรโตคอล VPN ที่คุณรู้จัก			
8	สิ่งที่การตรวจสอบ (audit) ตรวจได้			
9	สิ่งที่คุณมองหาใน NordVPN			
10	ประเทศที่มีชื่อเสียงด้านกฎหมายความเป็นส่วนตัวที่เข้มแข็ง			
11	คำถามสำหรับฝ่ายสนับสนุนลูกค้าของ NordVPN			
12	ฟีเจอร์ด้านความปลอดภัยใน NordVPN			
13	ภัยคุกคามบน Wi-Fi สาธารณะ			
14	การตั้งค่าที่คุณเปิดเพื่อความปลอดภัยเพิ่มเติม			
15	สิ่งที่การเข้ารหัสปกป้อง			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN และเครือข่าย

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การปรับใช้การเข้ารหัสสองชั้น



สถานการณ์: นักข่าวต้องส่งเอกสารที่ละเอียดอ่อนมากจากประเทศที่เซ็นเซอร์เข้มงวด

คำถามอภิปราย: พวกเขาควรใช้โปรไฟล์เซิร์ฟเวอร์ NordVPN ใดเพื่อเพิ่มความปลอดภัยของการเข้ารหัสให้สูงสุด?

กรณีศึกษาที่ 2: การป้องกันมัลแวร์บนเครือข่ายที่ใช้ร่วมกัน



สถานการณ์: บริษัททางไกลต้องการป้องกันไม่ให้พนักงานดาวน์โหลดไฟล์อันตรายผ่าน Wi-Fi สาธารณะ

คำถามอภิปราย: พวกเขาควรเปิดฟีเจอร์ใดในไคลเอนต์ NordVPN ไว้ตลอดเวลา?

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

25	45	35	67	20	37	51	7	11	67		60	10	64

61	39	35	67	1	49	35	67	20		60	25	21	48	39

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q1: NordLynx คืออะไร?

โปรโตคอลเฉพาะของ NordVPN ที่สร้างบน WireGuard ปรับให้เหมาะกับความเร็วและความปลอดภัย

Q2: NordVPN เก็บบันทึกหรือไม่?

ไม่ NordVPN รักษานโยบายไม่เก็บล็อกอย่างเข้มงวดซึ่งผ่านการตรวจสอบโดย Deloitte และ PwC [2]

Q3: Threat Protection คืออะไร?

เครื่องมือในตัวที่บล็อกโฆษณา ตัวติดตาม และสแกนการดาวน์โหลดหามัลแวร์

Q4: Double VPN คืออะไร?

ฟีเจอร์ที่ส่งทราฟฟิกของคุณผ่านเซิร์ฟเวอร์ VPN สองเครื่องแยกกันเพื่อการเข้ารหัสสองชั้น

Q5: kill switch ทำงานอย่างไร?

บล็อกอุปกรณ์ของคุณไม่ให้เข้าถึงอินเทอร์เน็ตหากการเชื่อมต่อ VPN หลุด

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q6: เซิร์ฟเวอร์ NordVPN ไม่มีดิสก์ (diskless) หรือไม่?

ใช่ NordVPN ดำเนินการเครือข่ายเซิร์ฟเวอร์ที่ไม่มีดิสก์และใช้ RAM เท่านั้นเพื่อปกป้องข้อมูลผู้ใช้

Q7: NordVPN มีฐานอยู่ที่ไหน?

NordVPN ตั้งอยู่ในปานามา ซึ่งไม่มีกฎหมายบังคับเก็บรักษาข้อมูล

Q8: ใช้ไซเฟอร์การเข้ารหัสใด?

AES-256 ใช้กับ OpenVPN/IKEv2 ส่วน ChaCha20 ใช้กับ NordLynx

Q9: Onion Over VPN คืออะไร?

ฟีเจอร์ที่ส่งทราฟฟิกผ่าน NordVPN แล้วจึงผ่านเครือข่าย Tor

Q10: NordVPN ป้องกันการรั่วไหลหรือไม่?

ใช่ NordVPN มีการป้องกัน DNS leak; VPN.com ไม่พบ DNS leak ในการทดสอบ [7]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q1: NordLynx แก้ปัญหาความเป็นส่วนตัวอย่างไร?

ใช้ระบบ NAT สองชั้นเพื่อกำหนด IP ชั่วคราวที่ปลอดภัยโดยไม่เก็บข้อมูลผู้ใช้บนเซิร์ฟเวอร์ [8]

Q2: ฮาร์ดแวร์แบบ RAM อย่างเดียวปลอดภัยเพียงใด?

เนื่องจาก RAM สูญเสียข้อมูลทั้งหมดเมื่อรีบูต การยึดเซิร์ฟเวอร์จึงไม่ได้บันทึกทราฟฟิกย้อนหลังใดๆ

Q3: App Kill Switch คืออะไร?

ต่างจาก kill switch ของอินเทอร์เน็ต ตัวนี้จะยุติเฉพาะแอปที่ระบุเมื่อ VPN หลุด

Q4: เซิร์ฟเวอร์ NordVPN ตั้งอยู่ในศูนย์ข้อมูลร่วม (collocated) หรือไม่?

ใช่ NordVPN กำลังเพิ่มจำนวนเซิร์ฟเวอร์แบบ collocated ซึ่งหมายความว่าเป็นเจ้าของฮาร์ดแวร์โดยตรง

Q5: การตรวจสอบความปลอดภัยดำเนินการอย่างไร?

PwC ตรวจสอบการตั้งค่าไม่เก็บบันทึกของบริษัทในปี 2018 และ 2020 ส่วน Deloitte ตรวจสอบทุกปีตั้งแต่ 2022 [3]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q6: Threat Protection Lite คืออะไร?

ชื่อเดิมของตัวบล็อกแบบ DNS ซึ่งปัจจุบันเรียกว่าการป้องกันสแกมและฟิชชิง

Q7: Meshnet รักษาความปลอดภัยของการกำหนดเส้นทางอย่างไร?

สร้างอุโมงค์เข้ารหัสแบบจุดต่อจุดระหว่างอุปกรณ์ของผู้ใช้โดยใช้คีย์ NordLynx

Q8: NordVPN รองรับการพรางทราฟฟิก (obfuscation) หรือไม่?

ได้ เซิร์ฟเวอร์แบบอำพรางข้ามไฟร์วอลล์ได้โดยพรางทราฟฟิก VPN ให้เป็นแพ็กเก็ต HTTPS

Q9: มีการป้องกันการรั่วไหลของ WebRTC หรือไม่?

WebRTC อาจเปิดเผย IP ในเบราว์เซอร์ ให้เชื่อมต่อ VPN ไว้ตลอดและรันการทดสอบการรั่วไหลเพื่อยืนยัน

Q10: เขตอำนาจของปานามาช่วยได้อย่างไร?

ปานามาอยู่นอกพันธมิตร 5/9/14-Eyes และไม่มีกฎหมายบังคับให้เก็บข้อมูล

ส่วนที่ 11: ข้อเท็จจริง VPN ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับความเร็วการเข้ารหัส VPN การตรวจสอบโปรโตคอล การเชื่อมต่อบนมือถือ และการทำงานระยะไกลขององค์กร

1. ข้อมูลเชิงลึกเรื่อง VPN

NordLynx เป็นโปรโตคอลเฉพาะของ NordVPN ที่สร้างโดยตรงรอบโค้ดแกนหลักของ WireGuard [1]

2. ข้อมูลเชิงลึกเรื่อง VPN

เขตอำนาจของปานามาไม่มีกฎหมายบังคับเก็บข้อมูล จึงช่วยรักษาความเป็นส่วนตัวของผู้ใช้

3. ข้อมูลเชิงลึกเรื่อง VPN

Deloitte ตรวจสอบและยืนยันการดำเนินงานแบบไม่เก็บบันทึกของ NordVPN อย่างเป็นอิสระ [9]

4. ข้อมูลเชิงลึกเรื่อง VPN

Threat Protection Pro ทำงานบนอุปกรณ์เพื่อบล็อกไฟล์อันตราย โฆษณา และตัวติดตาม [4]

5. ข้อมูลเชิงลึกเรื่อง VPN

Double VPN ส่งแพ็กเก็ตผ่านสองโหนด โดยเข้ารหัสเพย์โหลดข้อมูลสองครั้ง

6. ข้อมูลเชิงลึกเรื่อง VPN

ฮาร์ดแวร์เซิร์ฟเวอร์แบบ RAM-only ป้องกันการจัดเก็บบันทึกการทำงานหรือคีย์ไว้อย่างถาวร [5]

7. ข้อมูลเชิงลึกด้าน VPN

NordVPN ใช้รหัส AES-256-GCM และ ChaCha20 เพื่อปกป้องการรับส่งข้อมูลของผู้ใช้

8. ข้อมูลเชิงลึกด้าน VPN

เซิร์ฟเวอร์แบบอำพรางปกปิดส่วนหัวแพ็กเก็ต VPN เพื่อหลบไฟร์วอลล์ระดับประเทศที่เข้มงวด

9. ข้อมูลเชิงลึกด้าน VPN

Meshnet สร้างเครือข่ายเพียร์ทูเพียร์ที่เข้ารหัสโดยใช้การกำหนดค่า NordLynx ภายในเครื่อง

10. ข้อมูลเชิงลึกเรื่อง VPN

Kill switch ระดับแอปจะยุติกระบวนการเบื้องหลังที่เลือกไว้หากอุโมงค์หลุด

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานทางเทคนิค ข้อกำหนดเฉพาะ และกรอบการกำกับดูแลระดับโลก

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] NordVPN. (2026). NordLynx protocol for fast, secure VPN connections.
https://nordvpn.com/blog/nordlynx-protocol-wireguard/

[2] NordVPN. (2026). A leading no-log VPN for online privacy in 2026.
https://nordvpn.com/features/no-log-vpn/

[3] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[4] NordVPN Support. (n.d.). What is NordVPN's Scam, Phishing, and Malware protection?
https://support.nordvpn.com/hc/en-us/articles/19508765521425-What-is-Threat-Protection-Pro-and-Threat-Protection

[5] NordVPN. (2024). Why does NordVPN use RAM-based servers?
https://nordvpn.com/blog/ram-based-servers/

[6] NordVPN. (2026). Buy a VPN with card, crypto, or PayPal: Monthly and yearly plans.
https://nordvpn.com/pricing/

[7] VPN.com. (n.d.). NordVPN Review: Speed, Pricing & Features.
https://www.vpn.com/vpn/nordvpn/

[8] NordVPN. (2020). NordVPN Is Rolling Out NordLynx -- New Generation VPN Protocol That Makes VPN Connection Faster Than Ever. PR Newswire.
https://www.prnewswire.com/news-releases/nordvpn-is-rolling-out-nordlynx--new-generation-vpn-protocol-that-makes-vpn-connection-faster-than-ever-301046715.html

[9] NordVPN. (2024). NordVPN verifies its no-logs claim for the fourth time. PR Newswire.
https://www.prnewswire.com/news-releases/nordvpn-verifies-its-no-logs-claim-for-the-fourth-time-302031533.html

[10] NordVPN. (2023). NordVPN has completed independent infrastructure and app security audits. PR Newswire.
https://www.prnewswire.com/news-releases/nordvpn-has-completed-independent-infrastructure-and-app-security-audits-301760758.html

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

[12] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **คำถาม 1**

คำตอบที่ถูกต้อง: B

หมายเหตุสำหรับผู้สอน

NordLynx เป็นโปรโตคอลของ NordVPN เองที่สร้างบน WireGuard ร่วมกับระบบ NAT สองชั้น

2 **คำถาม 2**

คำตอบที่ถูกต้อง: C

หมายเหตุสำหรับผู้สอน

เซิร์ฟเวอร์ RAM แบบไม่มีดิสก์เก็บทุกอย่างไว้ในหน่วยความจำชั่วคราว ซึ่งจะถูกล้างเมื่อตัดไฟ

3 **คำถาม 3**

คำตอบที่ถูกต้อง: C

หมายเหตุสำหรับผู้สอน

Threat Protection บล็อกโฆษณา ตัวติดตาม และโดเมนอันตราย และเวอร์ชัน Pro ยังสแกนไฟล์ที่ดาวน์โหลดด้วย

4 **คำถาม 4**

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

Double VPN เชื่อมเซิร์ฟเวอร์ VPN สองเครื่องต่อกัน ทำให้ทราฟฟิกถูกเข้ารหัสสองครั้งก่อนไปถึงเว็บ

5 **คำถาม 5**

คำตอบที่ถูกต้อง: D

หมายเหตุสำหรับผู้สอน

PwC Switzerland (ปี 2018, 2020) และ Deloitte (ปี 2022–2025) ตรวจสอบยืนยันนโยบายไม่เก็บบันทึกของ NordVPN [2]

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6**

คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: NordLynx สร้างบน WireGuard โดยเพิ่มระบบ NAT สองชั้นเพื่อความเป็นส่วนตัว

7 **คำถาม 7**

คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: Threat Protection Pro ทำงานได้แม้ปิด VPN อยู่

8 **คำถาม 8**

คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: IP เฉพาะถูกกำหนดให้ผู้ใช้เพียงคนเดียว ต่างจากที่อยู่ IP ของ VPN แบบใช้ร่วมกัน

9 **คำถาม 9**

คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: App Kill Switch ปิดเฉพาะแอปที่เลือก ส่วน Internet Kill Switch บล็อกทราฟฟิกทั้งหมด

10 **คำถาม 10**

คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: NordVPN ระบุว่าเลือกใช้เซิร์ฟเวอร์ RAM แบบไม่มีดิสก์ ซึ่งไม่เก็บข้อมูลหลังปิดเครื่อง

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

F 1. นอร์ดลิงซ์	D 2. โหนด RAM	B 3. ป้องกันภัย	E 4. วีพีเอ็นคู่
G 5. ไม่เก็บล็อก	H 6. คิลสวิตช์	A 7. เมชเน็ตซ์	C 8. ไซเฟอร์

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 นอร์ดลิงซ์	2 แรมล้วน	3 ป้องกันภัย	4 วีพีเอ็นคู่
5 ไม่เก็บล็อก	6 คิลสวิตช์	7 เมชเน็ต	8 ไซเฟอร์

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 H – ไซเฟอร์	2 F – คิลสวิตช์	3 G – เมชเน็ต	4 C – ป้องกันภัย
5 D – วีพีเอ็นคู่	6 A – นอร์ดลิงซ์	7 E – ไม่เก็บล็อก	8 B – แรมล้วน

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย นอร์ดลิงซ์ โหนด RAM และ ป้องกันภัย ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

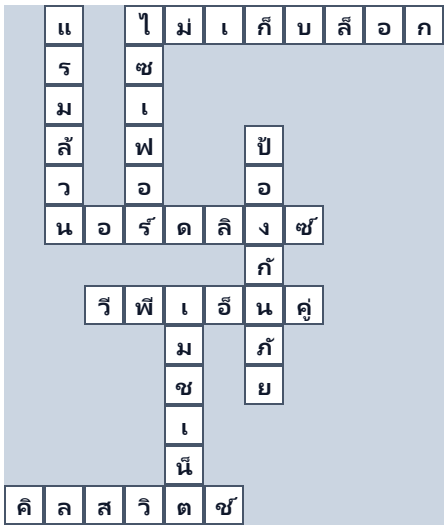
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

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	แ	จ	น	ตี	ว	ร	ตี
ว	า	วิ	ล	ล	ด	า	อ	ย	ร	ช	ฟ	ก	ก	ล
ม	า	ส	คู่	น	อ็	เ	พี	วี	ป	ม	อ	อ	ม	มี
า	ล	ล	ล	ป	ไ	จ	า	ต	นี	กี	ล้	พ	ร	ง
ย	า	คิ	ช	า	ม่	า	น	ลี	นิ	จ	ตี	ว	า	น
ภั	ล	ผ	ตี	ช	เ	ก	ด	อ	า	เ	ต	า	น	จ
น	า	ค	ก	ตี	ก็	า	ช	ว	ร์	ก	ช	ด	กี	ด
กั	ท	ผ	ฟ	ช	บ	มี	ม	อ	ต	ด	ฟ	ม	ร	ตี
ง	า	ท	า	ส	ล็	ไ	ท	ข	ข	า	ลิ	น	เ	ก
อ	า	ล	า	ม	อ	ช	ร	มี	า	ร	ช	ง	ก	ด
ป้	ง	น	ร	ต	ก	เ	สี	ย	ข	มี	ตี	ด	ช์	ด
ว	บ	ฟ	อ	า	ร	ฟ	ห	ห	รี	น	ผ	นี	ม	ผ
ตี	ข	กี	ส	บ	ลี	อ	ง	ด	ร	ต	ค	ผ	ห	ตี
ป	ร	กี	นี	า	ต	ร์	จ	ห	ตี	ด	บ	ตี	น	สี

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: ไม่เก็บล็อก มาตรฐานการเก็บข้อมูลที่เข้มงวดซึ่งผ่านการตรวจสอบจากภายนอก (8 ตัวอักษร)

4 แนวนอน: นอร์ดลิงซ์ โปรโตคอลเฉพาะของ NordVPN ที่สร้างบนมาตรฐาน WireGuard (7 ตัวอักษร)

5 แนวนอน: วีพีเอ็นคู่ การเชื่อมเซิร์ฟเวอร์ VPN สองตัวเข้าด้วยกันเพื่อเข้ารหัสข้อมูลสองครั้ง (6 ตัวอักษร)

7 แนวนอน: คิลสวิตช์ ฟีเจอร์ความปลอดภัยที่ตัดทราฟฟิกเมื่อ VPN หลุด (6 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: แรมล้วน ฮาร์ดแวร์เซิร์ฟเวอร์หน่วยความจำชั่วคราวที่ไม่เก็บข้อมูลเมื่อรีสตาร์ต (6 ตัวอักษร)

2 แนวตั้ง: ไซเฟอร์ อัลกอริทึมเข้ารหัสลับที่ใช้รักษาความปลอดภัยของเพย์โหลดข้อมูล (6 ตัวอักษร)

3 แนวตั้ง: ป้องกันภัย ชุดความปลอดภัยในเครื่องที่บล็อกตัวติดตาม โฆษณา และมัลแวร์ (7 ตัวอักษร)

6 แนวตั้ง: เมชเน็ต เครื่องมือกำหนดเส้นทางแบบกระจายศูนย์เพื่อเชื่อมต่ออุปกรณ์โดยตรง (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ดงนลิซ์ร์อ — นอร์ดลิงซ์
2. ป้งยกันกัอ — ป้องกันภัย
3. ก็ม่ไบล็กอเ — ไม่เก็บล็อก
4. ตเซน็เม — เมซเน็ต
5. ล้มนแวร — แรมล้วน
6. นฮ็วีเคู่พี — วีพีเอ็นคู่
7. ตคิวิซ์สล — คิลสวิตซ์
8. เร์ไอฟซ — ไซเฟอร์

เฉลยภารกิจรหัสลับ

"นอร์ดลิงซ์ ใช้ ไวร์การ์ด ในตัว"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การปรับใช้การเข้ารหัสสองชั้น

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: นักข่าวต้องส่งเอกสารที่ละเอียดอ่อนอย่างยิ่งจากประเทศที่เซ็นเซอร์เข้มงวด
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: เปิดใช้โปรไฟล์ Double VPN เพื่อเข้ารหัสข้อมูลผ่านโหนดเซิร์ฟเวอร์สองตัวที่แยกกัน

B กรณีศึกษาที่ 2: การป้องกันมัลแวร์บนเครือข่ายที่ใช้ร่วมกัน

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: บริษัทระยะไกลต้องการป้องกันไม่ให้พนักงานดาวน์โหลดไฟล์อันตรายผ่าน Wi-Fi สาธารณะ
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: เปิดฟีเจอร์ Threat Protection ไว้เพื่อสแกนการดาวน์โหลดและบล็อกมัลแวร์