ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

VPN ระดับองค์กร

การใช้การเข้าถึงเครือข่ายแบบ Zero Trust โหนดเกตเวย์เฉพาะ และการควบคุมผู้ดูแลระบบส่วนกลางขององค์กร

ภาพรวมการเรียนรู้เครือข่าย VPN ระดับองค์กร

ผู้เรียน

สถานะนักเรียน

สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย

สถานะการเชื่อมต่อ

การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน

การป้องกันการรั่วไหล

การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับเครือข่าย VPN ระดับองค์กร คุณจะได้สำรวจสถาปัตยกรรมซีโร่ทรัสต์ เกตเวย์ IP คงที่เฉพาะ คอนโซลผู้ดูแลระบบ การจัดเตรียม และอุโมงค์ IPsec แบบไซต์ถึงไซต์

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/vpn-di-thi-sut-samrap-thurakit/enterprise/

เส้นทางการเรียนรู้เครือข่าย VPN องค์กรของคุณ

- ใช้กรอบงาน Zero Trust Network Access (ZTNA)
- ตั้งค่า IP เกตเวย์เซิร์ฟเวอร์เฉพาะสำหรับตัวกรองรายการที่อนุญาต
- จัดการแผงผู้ดูแลระบบส่วนกลางขององค์กรและรายชื่อที่นั่งของผู้ใช้
- ตรวจสอบล็อกการเข้าถึงเครือข่ายและประวัติการเชื่อมต่อของผู้ใช้
- ตั้งค่ากฎ Single Sign-On (SSO) และการยืนยันตัวตนหลายปัจจัย
- ตั้งค่าอุโมงค์ IPsec แบบไซต์ต่อไซต์ระหว่างสาขา

คำแนะนำเครือข่าย VPN ระดับองค์กร

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ Zero Trust และ IPsec แบบ site-to-site ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

สถาปัตยกรรมซีโร่ทรัสต์และเกตเวย์เฉพาะ (บทนำ)

VPN ระดับองค์กรปกป้องสินทรัพย์ขององค์กรด้วยการเปลี่ยนไปใช้กรอบ Zero Trust Network Access (ZTNA) และการใช้ไวต์ลิสต์กับเกตเวย์ IP แบบคงที่เฉพาะ ผู้จัดการไอทีใช้คอนโซลผู้ดูแลระบบส่วนกลางเพื่อจัดการอุโมงค์ IPsec แบบ site-to-site และลิงก์การลงชื่อเข้าใช้ครั้งเดียว (SSO)

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. โมเดลความปลอดภัยใดที่กำลังเข้ามาแทนที่ VPN ระดับองค์กรแบบเดิม?
   - A) Zero Trust
   - B) Multi-hop
   - C) เพียร์ทูเพียร์
   - D) เกตเวย์เดียว

2. ต้องใช้ฟีเจอร์ใดเพื่อจำกัดการเข้าถึงฐานข้อมูลให้เฉพาะเซิร์ฟเวอร์ของบริษัท?
   - A) IP เฉพาะ
   - B) การกำหนดเส้นทางแบบไดนามิก
   - C) Split tunnel
   - D) พร็อกซี DNS

3. โปรโตคอลใดเป็นมาตรฐานสำหรับอุโมงค์ไซต์ทูไซต์ขององค์กร?
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. เครื่องมือกลางใดที่ช่วยให้ผู้ดูแลระบบจัดการที่นั่งของพนักงานได้?
   - A) คอนโซลผู้ดูแลระบบ
   - B) คีย์รีจิสทรี
   - C) เฟิร์มแวร์เราเตอร์
   - D) บันทึกระบบ

5. มาตรฐานการยืนยันตัวตนใดที่ช่วยให้ลงชื่อเข้าใช้ผ่าน Okta หรือ Microsoft Entra ID ได้?
   - A) Single Sign-On
   - B) รหัสลับที่ใช้ร่วมกัน
   - C) การยืนยันตัวตน EPP
   - D) คีย์ WEP

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. Zero Trust Network Access อนุญาตให้เข้าเครือข่ายหลังจากตรวจสอบความน่าเชื่อถือของอุปกรณ์อย่างต่อเนื่องแล้วเท่านั้น

○ จริง ○ เท็จ

7 คำถาม 7

7. เกตเวย์ IP เฉพาะส่งทราฟฟิกของพนักงานปะปนกับผู้ใช้ทั่วไปแบบสุ่ม

○ จริง ○ เท็จ

8 คำถาม 8

8. คอนโซลผู้ดูแลระบบแบบรวมศูนย์ช่วยให้ผู้จัดการไอทีเพิกถอนที่นั่งของพนักงานแต่ละคนได้ทันที

○ จริง ○ เท็จ

9 คำถาม 9

9. IPsec เป็นโปรโตคอลน้ำหนักเบาที่ไม่รองรับอุโมงค์เครือข่ายแบบไซต์ต่อไซต์

○ จริง ○ เท็จ

10 คำถาม 10

10. Single Sign-On ช่วยให้พนักงานยืนยันตัวตนอย่างปลอดภัยโดยใช้ผู้ให้บริการข้อมูลระบุตัวตนขององค์กร

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. สถาปัตยกรรมความปลอดภัยสมัยใหม่แทนที่อุโมงค์แบบเดิมด้วยการเข้าถึงแบบ _____
2. เพื่อจำกัดการเข้าถึงฐานข้อมูล บริษัทกำหนดที่อยู่เกตเวย์แบบ _____
3. สาขาของบริษัทเชื่อมต่ออย่างปลอดภัยด้วยอุโมงค์แบบไซต์ทูไซต์ที่ใช้ _____
4. ผู้ดูแลไอทีจัดสรรไลเซนส์ผู้ใช้ของพนักงานภายใน _____ ส่วนกลาง
5. การผสาน Okta ช่วยให้พนักงานยืนยันตัวตนผ่าน _____ ขององค์กรได้
6. เพื่อปกป้องการเข้าสู่ระบบ พอร์ทัลองค์กรบังคับใช้การยืนยันตัวตนแบบ _____

คลังคำศัพท์

เกตเวย์ | จัดสรรสิทธิ์ | ซีโรทรัสต์ | แผงผู้ดูแล | หลายปัจจัย | เอสเอสโอ | ไอพีเฉพาะ | ไอพีเซก

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดสำคัญ

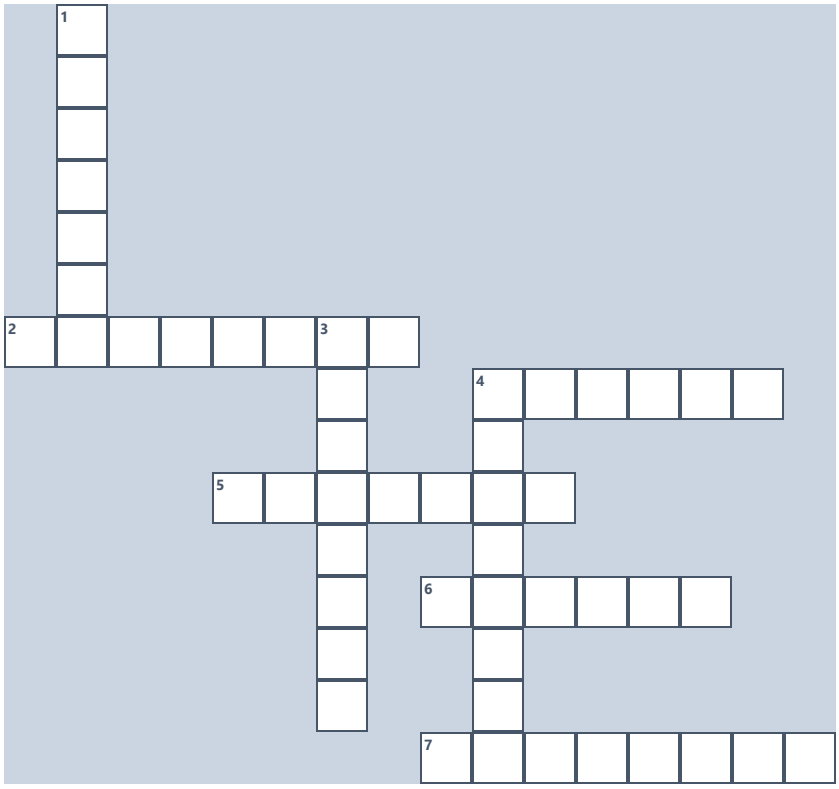
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. ซีโร่ทรัสต์**	**A**	การจัดสรรใบอนุญาตการเข้าถึง VPN ของพนักงาน
☐	**2. IP เฉพาะ**	**B**	การเชื่อมโยงตัวตนของ Okta และ Entra ID
☐	**3. IPSEC**	**C**	ความปลอดภัยการเข้าสู่ระบบที่ต้องใช้โทเค็นเพิ่มเติม
☐	**4. คอนโซลผู้ดูแล**	**D**	ที่อยู่เกตเวย์ไวต์ลิสต์แบบสแตติก
☐	**5. ลงชื่อเข้าใช้ครั้งเดียว**	**E**	มาตรฐานอุโมงค์แบบไซต์ต่อไซต์
☐	**6. หลายปัจจัย**	**F**	โหนดกำหนดเส้นทางทางเข้าของเครือข่าย
☐	**7. เกตเวย์**	**G**	พอร์ทัลสำหรับผู้จัดการไอทีส่วนกลางในการจัดการที่นั่ง
☐	**8. จัดเตรียม**	**H**	กรอบการทำงานที่ตรวจสอบความน่าเชื่อถืออย่างต่อเนื่อง

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. ความปลอดภัยของการเข้าสู่ระบบที่ต้องใช้โทเค็นเพิ่มเติม (8)

4. โหนดกำหนดเส้นทางที่เป็นทางเข้าเครือข่าย (6)

5. กรอบการตรวจสอบความน่าเชื่อถือแบบต่อเนื่อง (7)

6. มาตรฐานอุโมงค์แบบไซต์ทูไซต์ (6)

7. ที่อยู่เกตเวย์แบบคงที่สำหรับรายการอนุญาต (8)

แนวตั้ง

1. พอร์ทัลส่วนกลางสำหรับผู้จัดการไอทีบริหารที่นั่ง (7)

3. การจัดสรรไลเซนส์การเข้าถึง VPN ให้พนักงาน (8)

4. การเชื่อมโยงตัวตนกับ Okta และ Entra ID (8)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: ความปลอดภัยของการเข้าสู่ระบบที่ต้องใช้โทเค็นเพิ่มเติม (8 ตัวอักษร):

4 แนวนอน: โหนดกำหนดเส้นทางที่เป็นทางเข้าเครือข่าย (6 ตัวอักษร):

5 แนวนอน: กรอบการตรวจสอบความน่าเชื่อถือแบบต่อเนื่อง (7 ตัวอักษร):

6 แนวนอน: มาตรฐานอุโมงค์แบบไซต์ทูไซต์ (6 ตัวอักษร):

7 แนวนอน: ที่อยู่เกตเวย์แบบคงที่สำหรับรายการอนุญาต (8 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: พอร์ทัลส่วนกลางสำหรับผู้จัดการไอทีบริหารที่นั่ง (7 ตัวอักษร):

3 แนวตั้ง: การจัดสรรไลเซนส์การเข้าถึง VPN ให้พนักงาน (8 ตัวอักษร):

4 แนวตั้ง: การเชื่อมโยงตัวตนกับ Okta และ Entra ID (8 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

แ	ผ	ง	ผู้	ดู	แ	ล	า	า	ลี	จ	ดี	า	น	ล
ผ	ดี	ซ	ก	ด	า	ต	า	จ	า	ซี	ค	ก	ดี	า
ซ	ว	ก	ด	กี	ด	ท	ผ	ฟ	ซ	โ	มี	ม	อ	ต
ฟ	ธิ์	ท	สิ	ร	ร	ส	ด	จั	ร	ร	ดี	า	ท	า
ย	ส	ท	ข	ข	ไ	า	น	ก	า	ท	ล	า	ม	ร
จั	มี	า	ร	ช	อ	ก	เ	ด	ง	ร้	น	ร	ต	สี
จ	ย	ข	มี	ดี	พี	ด	ด	อ	ว	ส	บ	ฟ	อ	า
ปั	ร	ห	ห	รี	เ	น	ไ	ผ	ส	ต์	นี	ม	ผ	ดี
ย	ข	กี	ส	บ	ฉ	ลี	ง	อ	ด	เ	ร	ด	ค	ผ
า	ห	ดี	ป	ร	พ	กี	นี	า	พี	ต	อ	จ	ห	ดี
ล	ด	บ	ตี	น	า	สี	ลี	ว	ลี	เ	า	ส	ค	า
ห	า	ล	ห	ป	ะ	ส	ช	ตี	ลี	ล	ซ	มี	โ	ข
ต	ดี	เ	ก	ต	เ	ว	ย์	ดี	ห	ร	ม	ก	า	อ
ฟ	น	ซ	ข	ช	ร	ม	า	ต	ต	ว	ย	พ	ล	พ
บ	ค	ท	ฟ	ล	รี	ร	า	า	า	ต	พ	ท	ร	จ

รายการคำศัพท์

ซีโรทรัสต์ ไอพีเฉพาะ ไอพีเซก แผงผู้ดูแลจัดสรรสิทธิ์ เอสเอสโอ หลายปัจจัย เกตเวย์

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. ซีโรทรัสต์
B. ไอพีเฉพาะ
C. ไอพีเซก
D. แผงผู้ดูแล
E. เอสเอสโอ
F. หลายปัจจัย
G. เกตเวย์
H. จัดสรรสิทธิ์

คำนิยามและช่องจับคู่
1. ที่อยู่เกตเวย์แบบคงที่สำหรับรายการอนุญาต
2. โหนดกำหนดเส้นทางที่เป็นทางเข้าเครือข่าย
3. การจัดสรรไลเซนส์การเข้าถึง VPN ให้พนักงาน
4. ความปลอดภัยของการเข้าสู่ระบบที่ต้องใช้โทเค็นเพิ่มเติม
5. มาตรฐานอุโมงค์แบบไซต์ทูไซต์
6. กรอบการตรวจสอบความน่าเชื่อถือแบบต่อเนื่อง
7. การเชื่อมโยงตัวตนกับ Okta และ Entra ID
8. พอร์ทัลส่วนกลางสำหรับผู้จัดการไอทีบริหารที่นั่ง

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดสำคัญของใบงานนี้ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ท ส ซี ร์ ต์ ร โ
2. ก ไ พี ซ เ อ
3. เ อ เ อ ส อ โ ส
4. ย์ เ ต ว เ ก
5. ฉ พ อ ะ เ ไ า พี
6. แ ง ดู แ ผู้ ล ผ
7. ห ย ป์ จ จ ล ย า
8. ร ด ร ธิ์ จ์ ท ส ิ ส

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	เครื่องมือที่บริษัทใช้ทุกวัน			
2	สิ่งที่ VPN ซ่อนได้			
3	บทบาทในแผนก IT			
4	คำที่อธิบาย Zero Trust			
5	วิธีเข้าสู่ระบบอย่างปลอดภัย			
6	เหตุผลที่ควรให้พนักงานใช้ VPN			
7	สิ่งที่ต้องทำหลังเกิดการละเมิดความปลอดภัย			
8	เหตุผลที่ควรใช้ VPN ขณะเดินทาง			
9	กฎสำหรับการทำงานจากระยะไกลอย่างปลอดภัย			
10	ข้อมูลที่บริษัทต้องปกป้อง			
11	สิ่งที่อาจรบกวนการประชุมทางวิดีโอ			
12	อุปกรณ์ที่ใช้ VPN ได้			
13	โปรแกรมสำนักงานที่คุณรู้จัก			
14	สถานที่ที่พนักงานทำงาน			
15	อุปกรณ์ที่พนักงานอาจมี			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN และเครือข่าย

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การย้ายไปใช้ Zero Trust



สถานการณ์: องค์กรต้องการรักษาความปลอดภัยของเซิร์ฟเวอร์ภายในโดยตรวจสอบใบรับรองความสอดคล้องของอุปกรณ์ สถานะไฟร์วอลล์ และตำแหน่งของผู้ใช้อย่างต่อเนื่อง แทนที่จะไว้วางใจทุกคนภายในเครือข่าย

คำถามอภิปราย: ผู้อำนวยการด้านความปลอดภัยไอทีควรนำกรอบแนวคิดใดมาใช้เพื่อให้บรรลุเป้าหมายนี้?

กรณีศึกษาที่ 2: การจำกัดเกตเวย์



สถานการณ์: บริษัทโฮสต์ฐานข้อมูลการเงินส่วนตัวบนคลาวด์ ต้องการบล็อกการเข้าถึงแผงผู้ดูแลระบบจากอินเทอร์เน็ตสาธารณะทั้งหมด โดยอนุญาตการเข้าสู่ระบบเฉพาะจากอุปกรณ์ปลายทางของบริษัทที่ผ่านการยืนยัน

คำถามอภิปราย: ผู้ดูแลฐานข้อมูลควรตั้งค่าเครือข่ายแบบใดบนไฟร์วอลล์ของคลาวด์?

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

11	52	59	35	23	35	48	42	21	67		21	35	39	8	42	45	26

23	55	1		45	55	27	1	35	19	67

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q1: VPN สำหรับองค์กรคืออะไร?

อุโมงค์เครือข่ายที่ปลอดภัยซึ่งออกแบบมาสำหรับธุรกิจ ช่วยให้ผู้ทำงานระยะไกลเข้าถึงเครือข่ายองค์กรได้พร้อมการจัดการแบบรวมศูนย์

Q2: Zero Trust ต่างจาก VPN แบบดั้งเดิมอย่างไร?

VPN แบบดั้งเดิมไว้วางใจทุกคนภายในอุโมงค์ ในขณะที่ Zero Trust ตรวจสอบทุกอุปกรณ์และการเชื่อมต่อของผู้ใช้อย่างต่อเนื่อง

Q3: Dedicated IP ใน VPN สำหรับธุรกิจคืออะไร?

ที่อยู่ IP คงที่ที่สงวนไว้สำหรับธุรกิจของคุณเท่านั้น ช่วยให้คุณอนุญาตเฉพาะ IP นี้ (whitelist) เพื่อเข้าถึงฐานข้อมูลคลาวด์อย่างปลอดภัย

Q4: ทำไม SSO จึงสำคัญสำหรับ VPN ธุรกิจ?

Single Sign-On ช่วยให้พนักงานใช้ข้อมูลรับรององค์กร (เช่น Okta หรือ Microsoft Entra ID) เพื่อเข้าสู่ระบบอย่างปลอดภัย

Q5: VPN แบบ site-to-site คืออะไร?

อุโมงค์ที่เชื่อมสำนักงานจริงสองแห่ง (เช่น สาขากับสำนักงานใหญ่) ผ่านอินเทอร์เน็ตสาธารณะโดยใช้ IPsec

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q6: คอนโซลผู้ดูแลระบบ (admin console) มีหน้าที่อะไร?

แดชบอร์ดสำหรับผู้ดูแลระบบ IT เพื่อเพิ่มหรือลบที่นั่งของพนักงาน กำหนดเกตเวย์ และตรวจสอบการเชื่อมต่อที่ใช้งานอยู่

Q7: MFA รักษาความปลอดภัยให้ VPN ธุรกิจอย่างไร?

ด้วยการกำหนดให้ใช้รหัสเพิ่มเติม (เช่น โทเคนจากแอปยืนยันตัวตน) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากรหัสผ่านที่ถูกเจาะ

Q8: ฉันตรวจสอบประวัติการเชื่อมต่อของพนักงานได้หรือไม่?

ได้ VPN ขององค์กรบันทึกเวลาการเชื่อมต่อ ระยะเวลา และ IP ที่ได้รับมอบหมาย เพื่อการตรวจสอบตามข้อกำหนด

Q9: ZTNA คืออะไร?

Zero Trust Network Access โมเดลความปลอดภัยที่อนุญาตการเข้าถึงเฉพาะแอปพลิเคชันที่ระบุ แทนที่จะเป็นทั้งเครือข่าย

Q10: โหนดเกตเวย์มีบทบาทอย่างไร?

ทำหน้าที่เป็นจุดเข้าที่ปลอดภัยสำหรับทราฟฟิกระยะไกล ส่งข้อมูลตรงไปยังเซิร์ฟเวอร์องค์กรส่วนตัว

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q1: IPsec ปกป้องการสื่อสารขององค์กรแบบไซต์ถึงไซต์ได้อย่างไร?

IPsec เข้ารหัสทราฟฟิกที่ชั้นเครือข่ายโดยใช้ Encapsulating Security Payload (ESP) เพื่อให้ข้อมูลเป็นความลับและคงความสมบูรณ์

Q2: เหตุใดความปลอดภัยแบบเดิมที่อิงขอบเขตเครือข่ายจึงใช้ไม่ได้ผลกับพนักงานทำงานระยะไกล?

เพราะพนักงานเข้าถึงข้อมูลจากหลายสถานที่และหลายอุปกรณ์ ทำให้ขอบเขตไฟร์วอลล์เครือข่ายเดียวล้าสมัย

Q3: ผู้จัดการ IT นำการจัดเตรียมอัตโนมัติ (automated provisioning) ไปใช้อย่างไร?

ด้วยการแมปโปรโตคอล SCIM ระหว่างผู้ให้บริการยืนยันตัวตน (Okta) และคอนโซลผู้ดูแลระบบ VPN เพื่อซิงโครไนซ์ไดเรกทอรีผู้ใช้

Q4: split tunneling มีประโยชน์อย่างไรในสภาพแวดล้อมองค์กร?

กำหนดเส้นทางทราฟฟิก SaaS ในพื้นที่ (เช่น Microsoft 365) นอกอุโมงค์ VPN รักษาแบนด์วิดท์เกตเวย์ขององค์กรไว้สำหรับฐานข้อมูลส่วนตัว

Q5: การตรวจสอบสถานะอุปกรณ์ตรวจสอบความปลอดภัยของอุปกรณ์ปลายทางอย่างไร?

ไคลเอนต์ VPN สแกนอุปกรณ์ก่อนเชื่อมต่อเพื่อตรวจสอบว่าไฟร์วอลล์เปิดอยู่ ไวรัสป้องกันกำลังทำงาน และแพตช์ระบบปฏิบัติการเป็นปัจจุบัน

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q6: NAT traversal มีบทบาทอย่างไรในการตั้งค่า VPN ธุรกิจ?

NAT-T ห่อหุ้มแพ็กเก็ต IPsec ใน UDP เพื่อให้ผ่านเราเตอร์ตามบ้านและไฟร์วอลล์ได้โดยการเชื่อมต่อไม่หลุด

Q7: ธุรกิจป้องกันคอขวดแบนด์วิดท์ของเกตเวย์ได้อย่างไร?

ด้วยการติดตั้งโหนดเกตเวย์ระดับภูมิภาคหลายโหนดและกระจายทราฟฟิกผู้ใช้ขาเข้าไปยังโหนดเหล่านั้นด้วยตัวกระจายโหลด

Q8: ทำไมจึงนิยมใช้รายการอนุญาต IP แบบคงที่มากกว่าแบบไดนามิก?

ไวต์ลิสต์แบบสแตติกป้องกันไม่ให้ IP ภายนอกที่ไม่ได้รับอนุญาตพยายามทำแฮนด์เชคการเชื่อมต่อ ช่วยลดพื้นที่การโจมตีได้อย่างมาก

Q9: การพิสูจน์ตัวตนด้วยใบรับรองมีบทบาทอะไรใน VPN ระดับองค์กร?

ตรวจสอบใบรับรองดิจิทัลที่ไม่ซ้ำกันซึ่งติดตั้งบนอุปกรณ์ที่บริษัทจัดการ บล็อกคอมพิวเตอร์ส่วนตัวที่ไม่ได้รับการจัดการ

Q10: ZTNA ลดความเสี่ยงของการเคลื่อนที่ในแนวขวางได้อย่างไร?

ด้วยการแยกเซสชันของผู้ใช้ให้เข้าถึงเฉพาะทรัพยากรที่ได้รับอนุญาต ป้องกันแฮกเกอร์เคลื่อนที่ไปทั่วเครือข่ายหากโหนดหนึ่งถูกเจาะ

ส่วนที่ 11: ข้อเท็จจริง VPN ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับความเร็วการเข้ารหัส VPN การตรวจสอบโปรโตคอล การเชื่อมต่อบนมือถือ และการทำงานระยะไกลขององค์กร

1. ข้อมูลเชิงลึกเรื่อง VPN

สถาปัตยกรรมซีโร่ทรัสต์ตรวจสอบสถานะความปลอดภัยของทุกอุปกรณ์ที่พยายามเชื่อมต่อเครือข่ายอย่างต่อเนื่อง

2. ข้อมูลเชิงลึกเรื่อง VPN

เกตเวย์ IP เฉพาะช่วยให้ธุรกิจล็อกฐานข้อมูลบนคลาวด์ได้ด้วยการใช้ไวต์ลิสต์กับที่อยู่แบบคงที่

3. ข้อมูลเชิงลึกเรื่อง VPN

IPsec เป็นโปรโตคอลมาตรฐานอุตสาหกรรมสำหรับกำหนดค่าอุโมงค์เครือข่ายสำนักงานแบบไซต์ต่อไซต์ที่ปลอดภัย

4. ข้อมูลเชิงลึกเรื่อง VPN

คอนโซลผู้ดูแลระบบช่วยให้ฝ่าย IT จัดเตรียม จัดการ และตรวจสอบที่นั่งการเข้าถึง VPN ของพนักงาน

5. ข้อมูลเชิงลึกเรื่อง VPN

Single Sign-On ผสานการเข้าถึง VPN เข้ากับผู้ให้บริการข้อมูลระบุตัวตนขององค์กร เช่น Okta และ Entra ID

6. ข้อมูลเชิงลึกเรื่อง VPN

การยืนยันตัวตนหลายปัจจัยบล็อกความพยายามเชื่อมต่อโดยไม่ได้รับอนุญาตที่มาจากคีย์รหัสผ่านที่ถูกขโมย

7. ข้อมูลเชิงลึกด้าน VPN

Split tunneling เพิ่มประสิทธิภาพแบนด์วิดท์ขององค์กรโดยแยกทราฟฟิก SaaS สาธารณะออกจากอุโมงค์ที่เข้ารหัส

8. ข้อมูลเชิงลึกด้าน VPN

การตรวจสอบสถานะอุปกรณ์ยืนยันการตั้งค่าความปลอดภัยในเครื่องก่อนให้สิทธิ์เข้าถึงเซิร์ฟเวอร์ขององค์กร

9. ข้อมูลเชิงลึกด้าน VPN

การซิงโครไนซ์ไดเรกทอรี SCIM ช่วยทำให้การควบคุมการเข้าถึงสำหรับการรับพนักงานใหม่และการออกจากงานเป็นไปโดยอัตโนมัติ

10. ข้อมูลเชิงลึกเรื่อง VPN

Zero Trust Network Access จำกัดการเข้าถึงของผู้ใช้ไว้เฉพาะแอปพลิเคชันที่ได้รับอนุญาต ป้องกันการเคลื่อนที่ด้านข้างในเครือข่าย

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานทางเทคนิค ข้อกำหนดเฉพาะ และกรอบการกำกับดูแลระดับโลก

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **ซีโร่ทรัสต์** โมเดล ZTNA **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

โมเดลซีโร่ทรัสต์ตรวจสอบการปฏิบัติตามข้อกำหนดของอุปกรณ์อย่างต่อเนื่องก่อนเข้าสู่เครือข่าย การอ้างอิง: NIST Zero Trust.

2 **IP เฉพาะ** IP แบบคงที่ **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

IP เฉพาะช่วยให้ใช้ไวต์ลิสต์กับเกตเวย์เพื่อบล็อกทราฟฟิกสาธารณะได้ แหล่งอ้างอิง: Dedicated IP Guide.

3 **มาตรฐาน IPsec** อุโมงค์ IPSEC **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

IPsec เป็นโปรโตคอลมาตรฐานที่ใช้สำหรับอุโมงค์ไซต์ต่อไซต์ของสาขา การอ้างอิง: IPsec Tunneling.

4 **การจัดสรรไอที** คอนโซลผู้ดูแลระบบ **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

แดชบอร์ดผู้ดูแลระบบแบบรวมศูนย์ช่วยให้ผู้จัดการไอทีจัดสรรใบอนุญาตที่นั่งได้ แหล่งอ้างอิง: CISA Guidelines.

5 **คำถาม 5** **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

มาตรฐานการยืนยันตัวตนใดที่ช่วยให้ลงชื่อเข้าใช้ผ่าน Okta หรือ Microsoft Entra ID ได้? → Single Sign-On

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **ซีโร่ทรัสต์** การตรวจสอบ ZTNA — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

โมเดลซีโร่ทรัสต์ตรวจสอบการปฏิบัติตามข้อกำหนดของอุปกรณ์อย่างต่อเนื่องก่อนเข้าสู่เครือข่าย การอ้างอิง: NIST Zero Trust.

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

หมายเหตุสำหรับผู้สอน

IP เฉพาะสงวนไว้สำหรับธุรกิจเดียว ทราฟฟิกจึงไม่ปะปนกับผู้ใช้รายอื่น

8 **การจัดสรรไอที** ที่นั่งผู้ดูแลระบบไอที — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

แดชบอร์ดผู้ดูแลระบบแบบรวมศูนย์ช่วยให้ผู้จัดการไอทีจัดสรรใบอนุญาตที่นั่งได้ แหล่งอ้างอิง: CISA Guidelines.

9 **มาตรฐาน IPsec** ไซต์ถึงไซต์ — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

IPsec เป็นโปรโตคอลมาตรฐานที่ใช้สำหรับอุโมงค์ไซต์ต่อไซต์ของสาขา การอ้างอิง: IPsec Tunneling.

10 **ลิงก์ Okta SSO** การลือกอินด้วย SSO — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

Single Sign-On ผสานการเข้าสู่ระบบ VPN เข้ากับไดเรกทอรีขององค์กร เช่น Okta การอ้างอิง: Okta SSO.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

H 1. ซีโร่ทรัสต์	D 2. IP เฉพาะ	E 3. IPSEC	G 4. คอนโซลผู้ดูแล
B 5. ลงชื่อเข้าใช้ครั้งเดียว	C 6. หลายปัจจัย	F 7. เกตเวย์	A 8. จัดเตรียม

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ซีโรทรัสต์	2 ไอพีเฉพาะ	3 ไอพีเซก	4 แผงผู้ดูแล
5 เอสเอสโอ	6 หลายปัจจัย		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 B – ไอพีเฉพาะ	2 G – เกตเวย์	3 H – จัดสรรสิทธิ์	4 F – หลายปัจจัย
5 C – ไอพีเซก	6 A – ซีโรทรัสต์	7 E – เอสเอสโอ	8 D – แผงผู้ดูแล

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย ซีโร่ทรัสต์ IP เฉพาะ และ IPSEC ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

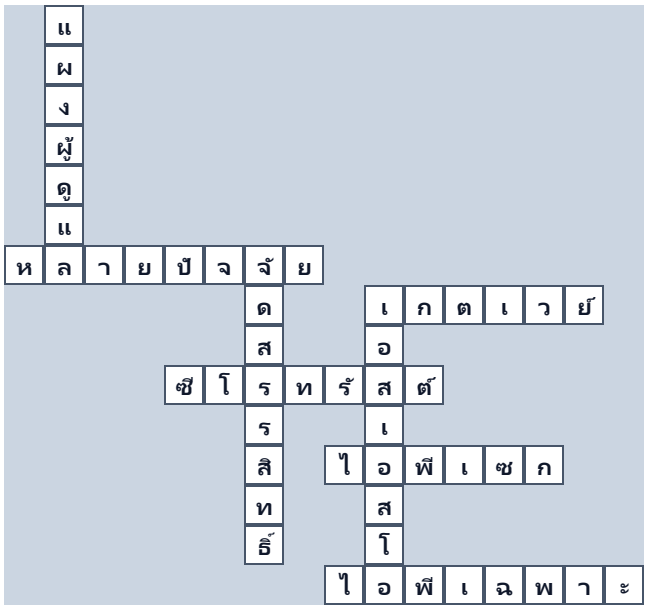
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

แ	ผ	ง	ผู้	ดู	แ	ล	า	า	ลี	จ	ดี	า	น	ล
ผ	ดี	ซ	ก	ด	า	ต	า	จ	า	ซี	ค	ก	ดี	า
ซ	ว	ก	ด	กี	ด	ท	ผ	ฟ	ซ	โ	มี	ม	อ	ต
ฟ	ธิ์	ท	สิ	ร	ร	ส	ด	จั	ร	ร	ดี	า	ท	า
ย	ส	ท	ข	ข	ไ	า	น	ก	า	ท	ล	า	ม	ร
จั	มี	า	ร	ช	อ	ก	เ	ด	ง	รั	น	ร	ต	สี
จ	ย	ข	มี	ดี	พี	ด	ด	อ	ว	ส	บ	ฟ	อ	า
ปั	ร	ห	ห	รี	เ	น	ไ	ผ	ส	ต์	นี	ม	ผ	ดี
ย	ข	กี	ส	บ	ฉ	ลี	ง	อ	ด	เ	ร	ด	ค	ผ
า	ห	ดี	ป	ร	พ	กี	นี	า	พี	ต	อ	จ	ห	ดี
ล	ด	บ	ตี	น	า	สี	ลี	ว	ลี	เ	า	ส	ค	า
ห	า	ล	ห	ป	ะ	ส	ช	ดี	ลี	ล	ซ	มี	โ	ข
ต	ดี	เ	ก	ต	เ	ว	ย์	ดี	ห	ร	ม	ก	า	อ
ฟ	น	ซ	ข	ช	ร	ม	า	ต	ต	ว	ย	พ	ล	พ
บ	ค	ท	ฟ	ล	รี	ร	า	า	า	ต	พ	ท	ร	จ

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: หลายปัจจัย ความปลอดภัยของการเข้าสู่ระบบที่ต้องใช้โทเคนเพิ่มเติม (8 ตัวอักษร)

4 แนวนอน: เกตเวย์ โหนดกำหนดเส้นทางที่เป็นทางเข้าเครือข่าย (6 ตัวอักษร)

5 แนวนอน: ซีโรทรัสต์ กรอบการตรวจสอบความน่าเชื่อถือแบบต่อเนื่อง (7 ตัวอักษร)

6 แนวนอน: ไอพีเซก มาตรฐานอุโมงค์แบบไซต์ทูไซต์ (6 ตัวอักษร)

7 แนวนอน: ไอพีเฉพาะ ที่อยู่เกตเวย์แบบคงที่สำหรับรายการอนุญาต (8 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: แผงผู้ดูแล พอร์ทัลส่วนกลางสำหรับผู้จัดการไอทีบริหารที่นั่ง (7 ตัวอักษร)

3 แนวตั้ง: จัดสรรสิทธิ์ การจัดสรรไลเซนส์การเข้าถึง VPN ให้พนักงาน (8 ตัวอักษร)

4 แนวตั้ง: เอสเอสโอ การเชื่อมโยงตัวตนกับ Okta และ Entra ID (8 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ทสซีรัต์รโ → ซีโรทรัสต์
2. กไพีซเอ → ไอพีเซก
3. เอเอสอโส → เอสเอสโอ
4. ย์เตวเก → เกตเวย์
5. ฉพอะเไาพี → ไอพีเฉพาะ
6. แงดูแผู้ลผ → แผงผู้ดูแล
7. หยปัจจัลยา → หลายปัจจัย
8. รดรธิ์จัทสิส → จัดสรรสิทธิ์

เฉลยภารกิจรหัสลับ

"ซีโรทรัสต์ ตรวจสอบ ทุก อุปกรณ์"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การย้ายไปใช้ Zero Trust

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: องค์กรต้องการรักษาความปลอดภัยของเซิร์ฟเวอร์ภายในโดยตรวจสอบใบรับรองการปฏิบัติตามข้อกำหนดของอุปกรณ์ สถานะไฟร์วอลล์ และตำแหน่งของผู้ใช้อย่างต่อเนื่อง แทนที่จะเชื่อถือทุกคนที่อยู่ภายในเครือข่าย
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ผู้อำนวยการควรย้ายไปใช้โมเดล Zero Trust Network Access (ZTNA) ซึ่งบังคับใช้การตรวจสอบความปลอดภัยตามบริบทอย่างต่อเนื่อง

B กรณีศึกษาที่ 2: การจำกัดเกตเวย์

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: บริษัทโฮสต์ฐานข้อมูลการเงินส่วนตัวบนคลาวด์ ต้องการบล็อกการเข้าถึงแผงผู้ดูแลระบบจากอินเทอร์เน็ตสาธารณะทั้งหมด โดยอนุญาตให้ล็อกอินเฉพาะจากอุปกรณ์ปลายทางของบริษัทที่ผ่านการยืนยัน
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ผู้ดูแลระบบควรกำหนดค่าเกตเวย์ Dedicated IP บน VPN ระดับองค์กร และอนุญาต (whitelist) ที่อยู่คงที่นี้บนไฟร์วอลล์ของฐานข้อมูลคลาวด์