นาย พัชระ อัลอุมารี รหัสนักศึกษา 6651630177

Assignment #8

อธิบายหลักการทำงาน IPsec

หลักการทำงานของ IPsec (Internet Protocol Security)

IPsec (Internet Protocol Security) เป็นชุดของโปรโตคอลที่ใช้สำหรับ การรักษาความปลอดภัยของการสื่อสารผ่านเครือข่าย IP โดยรองรับ การเข้ารหัส (Encryption), การตรวจสอบความถูกต้อง (Authentication), และการรักษาความสมบูรณ์ของข้อมูล (Integrity)

IPsec ใช้สำหรับ VPN (Virtual Private Network) และการสื่อสารที่ต้องการความปลอดภัย เช่น การส่งข้อมูลระหว่างองค์กร การปกป้องเครือข่ายอินเทอร์เน็ต เป็นต้น

1. องค์ประกอบหลักของ IPsec

IPsec มีองค์ประกอบหลัก 3 ส่วน:

1. **Authentication Header (AH)**
   - ใช้สำหรับ **การตรวจสอบความถูกต้องของแพ็กเก็ต (Authentication)**
   - ป้องกัน **การแก้ไขข้อมูล (Integrity Protection)**
   - **ไม่รองรับการเข้ารหัส** (ข้อมูลยังอ่านได้ แต่ป้องกันการเปลี่ยนแปลง)
2. **Encapsulating Security Payload (ESP)**
   - รองรับทั้ง **การเข้ารหัส (Encryption) และการตรวจสอบความถูกต้อง (Authentication)**
   - **ปกปิดข้อมูล (Confidentiality)** และป้องกันการเปลี่ยนแปลงของข้อมูล
   - ESP เป็นที่นิยมมากกว่า AH เพราะรองรับ **การเข้ารหัสข้อมูล**
3. **Security Association (SA)**
   - เป็นข้อตกลงระหว่าง 2 อุปกรณ์ที่ต้องการสื่อสารกันอย่างปลอดภัย
   - ระบุ **อัลกอริธึมเข้ารหัส, คีย์ที่ใช้, ระยะเวลาที่ใช้คีย์นั้น** เป็นต้น
   - SA ถูกจัดการโดย **Internet Key Exchange (IKE)** ซึ่งเป็นโปรโตคอลที่ช่วยในการแลกเปลี่ยนคีย์เข้ารหัส

2. โหมดการทำงานของ IPsec

IPsec มี **2 โหมดหลัก** ที่ใช้ขึ้นอยู่กับประเภทของการใช้งาน:

1. Transport Mode

- ใช้สำหรับ **End-to-End Security** (การรักษาความปลอดภัยระหว่างอุปกรณ์ปลายทาง เช่น PC ↔ PC)
- **เฉพาะ Payload (ข้อมูลภายในแพ็กเก็ต) ถูกเข้ารหัส** แต่ IP Header ยังคงมองเห็นได้
- ใช้ใน **การป้องกันข้อมูลที่วิ่งภายในเครือข่ายองค์กร**

2. Tunnel Mode

- ใช้สำหรับ **Gateway-to-Gateway Security** (เช่น VPN ระหว่างองค์กร)
- **ทั้ง IP Header และ Payload ถูกเข้ารหัส** และถูกห่อหุ้มด้วย IP Header ใหม่
- ปลอดภัยกว่ารูปแบบ Transport Mode เพราะปกปิดที่อยู่ปลายทางจริง

3. กระบวนการทำงานของ IPsec

IPsec ทำงานผ่าน 2 กระบวนการหลัก ได้แก่ **Key Exchange (IKE) และ Data Transfer**

1. **Internet Key Exchange (IKE)**

   เป็นกระบวนการแลกเปลี่ยนคีย์เข้ารหัสและสร้าง Security Association (SA) ประกอบด้วย 2 เฟส:

   IKE Phase 1 (สร้าง Secure Channel)

   1. **Authentication:** ตรวจสอบตัวตนของอุปกรณ์
   2. **Key Exchange:** แลกเปลี่ยนคีย์เข้ารหัส (ใช้ Diffie-Hellman)
   3. **Negotiation:** ตกลงอัลกอริธึมเข้ารหัสและค่าความปลอดภัย
   4. **Secure Channel:** สร้างช่องทางที่เข้ารหัสเพื่อใช้ใน IKE Phase 2

   IKE Phase 2 (สร้าง Security Association - SA)

   1. **สร้าง IPsec SA** สำหรับ ESP หรือ AH
   2. **กำหนดระยะเวลาและเงื่อนไขการใช้งานคีย์เข้ารหัส**
   3. **เริ่มการสื่อสารที่ปลอดภัย**

2. **Data Transfer (การรับส่งข้อมูล)**

หลังจาก SA ถูกสร้างขึ้น:

- IPsec จะเข้ารหัสแพ็กเก็ตข้อมูลโดยใช้ ESP หรือ AH
- แพ็กเก็ตที่ถูกเข้ารหัสจะถูกส่งไปยังปลายทาง
- เมื่อปลายทางได้รับข้อมูล จะใช้คีย์ถอดรหัสและตรวจสอบความถูกต้อง

4. อัลกอริธึมที่ใช้ใน IPsec

IPsec รองรับหลายอัลกอริธึมที่ใช้สำหรับการเข้ารหัสและตรวจสอบข้อมูล เช่น:

ฟังก์ชัน	**อัลกอริธึมที่ใช้**
Encryption (การเข้ารหัส)	AES, 3DES, Blowfish
Authentication (การตรวจสอบ)	HMAC-SHA-256, HMAC-MD5
Key Exchange (การแลกเปลี่ยนคีย์)	Diffie-Hellman, RSA

5. การใช้งาน IPsec ในชีวิตจริง

1. **VPN (Virtual Private Network)**
   - ใช้ IPsec Tunnel Mode เพื่อสร้าง VPN ระหว่างสำนักงาน
   - ปกป้องข้อมูลที่ส่งผ่านอินเทอร์เน็ต
2. **Secure Remote Access**
   - องค์กรใช้ IPsec VPN เพื่อให้พนักงานเข้าถึงระบบจากระยะไกลอย่างปลอดภัย
3. **Site-to-Site VPN**
   - ใช้ IPsec เชื่อมโยงเครือข่ายของ 2 สาขาเข้าด้วยกัน
4. **Network Layer Security**
   - ใช้ IPsec เพื่อปกป้องการสื่อสารระหว่างอุปกรณ์ภายในองค์กร

6. ข้อดีของ IPsec

1. ความปลอดภัยสูง

- รองรับ **Encryption, Authentication, และ Integrity**

2. รองรับ VPN ได้ดี

- สามารถใช้สร้าง VPN ที่ปลอดภัยทั้งสำหรับ Remote Access และ Site-to-Site

3. ปกป้องข้อมูลใน Layer 3 (Network Layer)

- ป้องกันการโจมตีเช่น **Man-in-the-Middle (MITM), IP Spoofing**

4. รองรับหลายอัลกอริธึม

- สามารถเลือกใช้อัลกอริธึมที่เหมาะสมกับระดับความปลอดภัย

7. ข้อเสียของ IPsec

1. Overhead สูง

- การเข้ารหัสและถอดรหัสต้องใช้ทรัพยากร CPU และเพิ่มขนาดแพ็กเก็ต

2. การตั้งค่าซับซ้อน

- ต้องกำหนดค่า Security Association, Key Exchange และ Policy

3. อาจเกิดปัญหากับ NAT

- ESP ไม่รองรับ NAT ได้ดีนัก อาจต้องใช้ NAT-Traversal

IPsec เป็นโปรโตคอลที่ให้ความปลอดภัยกับการสื่อสารผ่านเครือข่าย IP โดยใช้การเข้ารหัสและการตรวจสอบข้อมูล

รองรับ 2 โหมด คือ Transport Mode (เข้ารหัสเฉพาะข้อมูล) และ Tunnel Mode (เข้ารหัสทั้งแพ็กเก็ต)

ใช้ใน VPN, Secure Remote Access, และ Network Security

มีข้อดีด้านความปลอดภัยสูง แต่มี Overhead และการตั้งค่าที่ซับซ้อน