อุปกรณ์เชื่อมต่อเครือข่ายคอมพิวเตอร์ (Network Connectivity Devices)

ความหมายและบทบาทหลัก

อุปกรณ์เชื่อมต่อเครือข่ายคือฮาร์ดแวร์ที่ใช้เชื่อมต่อโหนด (คอมพิวเตอร์ เซิร์ฟเวอร์ อุปกรณ์ IOT ฯลฯ) ให้ สามารถสื่อสารกันและส่งต่อข้อมูลระหว่างกันได้ โดยทำหน้าที่ต่างระดับของโมเดล OSI (Layer 1-Layer 3 เป็นต้น)

การใช้งาน / ตัวอย่าง

ใช้ Switch ภายในออฟฟิศเพื่อเชื่อมคอมพิวเตอร์หลายเครื่อง

ใช้ Router เชื่อมสำนักงานใหญ่กับอินเทอร์เน็ตและกำหนด policy การจราจร

ใช้ Load balancer กับเว็บเซิร์ฟเวอร์เพื่อรองรับผู้ใช้งานจำนวนมาก

ประเภทหลักและคำอธิบาย

1. Network Interface Card (NIC) / Ethernet Adapter

ต่อเครื่องคอมพิวเตอร์กับสื่อกายภาพ (UTP, Fiber)

สนับสนุนความเร็วต่าง ๆ (10/100/1000 Mbps, 10 Gbps ขึ้นไป)

มีเวอร์ชันสำหรับ Wi-Fi (Wireless NIC)

2. Hub

อุปกรณ์ Layer 1 ที่ทำหน้าที่กระจายสัญญาณแบบเรียบ (broadcast)

ใช้งานน้อยลงเพราะเกิด collision เยอะ

ข้อควรระวังและแนวปฏิบัติที่แนะนำ

เลือกอุปกรณ์ให้เหมาะกับปริมาณทราฟฟิกและฟีเจอร์ที่ต้องการ (เช่น VLAN, PoE, 10GbE)

ใช้ Managed Switch สำหรับองค์กรที่ต้องการควบคุม/มอนิเตอร์

กำหนดแผนการสำรอง (redundancy) เช่น Spanning Tree, LACP, dual-homing

อัปเดตเฟิร์มแวร์และตั้งค่ารหัสผ่านเริ่มต้นทันทีหลังติดตั้ง

อุปกรณ์รักษาความปลอดภัย (Network Security Devices)

ความหมายและบทบาทโดยรวม

อุปกรณ์รักษาความปลอดภัยคือฮาร์ดแวร์/ ซอฟต์แวร์ที่วางเป็นชั้นป้องกันให้เครือข่ายและ ข้อมูลจากภัยคุกคามภายนอก/ภายใน เช่น การ โจมตีทางเครือข่าย มัลแวร์ การบุกรุก และการรั่ว ไหลของข้อมูล หน้าที่หลักคือ ป้องกัน ตรวจจับ ตอบสนอง และรายงาน เหตุการณ์ด้านความ ปลอดภัย

ประเภทหลักของอุปกรณ์และการทำงาน

ทำหน้าที่กรองทราฟฟิกตามนโยบาย (policy) เช่น อนุญาต/ปฏิเสธพอร์ต โปรโตคอล หรือที่อยู่ IP

มีหลายรูปแบบ: packet-filtering, stateful firewall, next-gen firewall (NGFW) ที่รวม DPI, URL filtering, application control

ตัวอย่างการใช้งาน: บล็อกพอร์ตที่ไม่ใช้, NAT, การแยกเครือข่าย (zone)

ปัญหาที่พบบ่อย

false positives ใน IDS/IPS → ต้อง tune rule

sets

single point of failure ถ้าใช้ UTM ตัวเดียว → ต้องมี redundancy

configuration errors ที่เปิดพอร์ต management ให้สาธารณะ → ควรจำกัดด้วย ACL และการเข้าถึง เฉพาะ IP/management VLAN

ประเภทหลักของอุปกรณ์และการทำงาน

1. Firewall

ทำหน้าที่กรองทราฟฟิกตามนโยบาย (policy) เช่น อนุญาต/ปฏิเสธพอร์ต โปรโตคอล หรือที่อยู่ IP

มีหลายรูปแบบ: packet-filtering, stateful firewall, next-gen firewall (NGFW) ที่รวม DPI, URL filtering, application control

ตัวอย่างการใช้งาน: บล็อกพอร์ตที่ไม่ใช้, NAT, การแยกเครือข่าย (zone)

2. IDS/IPS (Intrusion Detection/Prevention System)

IDS = ตรวจจับเหตุการณ์ที่ผิดปกติและแจ้งเตือน (alert)

IPS = ตรวจจับและบล็อกการโจมตีแบบเรียลไทม์

ใช้ signature-based, anomaly-based หรือ hybrid detection

อุปกรณ์เครือข่ายไร้สาย
(Wireless Networking Devices)

ความหมายและบทบาทโดยรวม

อุปกรณ์เครือข่ายไร้สายคือฮาร์ดแวร์และ ซอฟต์แวร์ที่ทำให้เครื่องลูกข่ายเชื่อมต่อเครือข่าย โดยไม่ใช้สาย – โดยมากหมายถึง Wi-Fi (IEEE 802.11) แต่รวมถึงเทคโนโลยีอื่น ๆ เช่น Bluetooth, Zigbee สำหรับอุปกรณ์ IoT

แนวปฏิบัติที่แนะนำ

ใช้ WPA2/WPA3-Enterprise สำหรับองค์กรใหญ่ หากเป็นสาธารณะให้ใช้ Guest SSID แยก VLAN

ทำ Site Survey ก่อนติดตั้งและหลังเปลี่ยนสภาพแวดล้อม (เช่น ติดตั้งเครื่องจักรใหม่)

แยก management network และจำกัดการเข้าถึงด้วย ACL / VPN

ตั้งค่า monitoring (SNMP, logs, RADIUS accounting) เพื่อติดตามปัญหาและการใช้งาน

วางแผน capacity & redundancy (หลาย AP, controller redundancy) และอัปเดตเฟิร์มแวร์อย่างสม่ำเสมอ

อุปกรณ์หลักและหน้าที่

1. Access Point (AP)

จุดเชื่อมต่อสำหรับอุปกรณ์ไร้สาย ทำหน้าที่รับ/ส่งสัญญาณวิทยุและเชื่อมต่อกับ LAN

มีแบบ Standalone (อิสระ) และแบบ Controller-managed (centralized management)

มาตรฐานและย่านความถี่

IEEE 802.11 family: 802.11b/g/n (2.4 GHz), 802.11a/ac (5 GHz), 802.11ax (Wi-Fi 6), 802.11ax + 6GHz (Wi-Fi 6E)

2.4 GHz: ช่วงครอบคลุมดีแต่ช่องสัญญาณจำกัดและแออัด

5 GHz: ความเร็วสูงขึ้น ช่องสัญญาณเยอะกว่าและรบกวนน้อยกว่า

ความเข้าใจเรื่อง channel width (20/40/80/160 MHz) สำคัญต่อ throughput และ interference