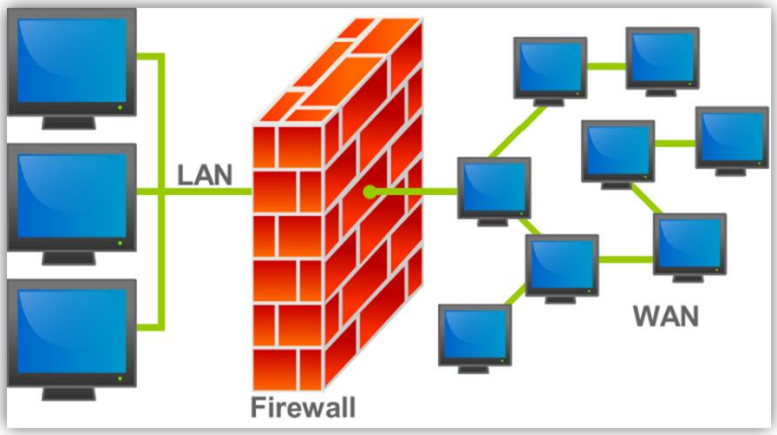
บทเรียนคอมพิวเตอร์ช่วยสอน เรื่อง อุปกรณ์ระบบเครือข่าย

เรื่อง อุปกรณ์รักษาความปลอดภัย (Security device)

ในระบบเครือข่ายนั้นมีผู้ใช้เป็นจำนวนมากทำให้มีรูปแบบการใช้งานที่หลากหลายทั้งผู้ที่ประสงค์ดีและประสงค์ร้าย ทำให้เกิดการบริการข้อมูลทั่วไปและอาชญากรรมทางด้านเครือข่ายคอมพิวเตอร์ จึงต้องมีอุปกรณ์ที่ใช้รักษาความปลอดภัยในระบบเครือข่ายด้วย ดังนี้

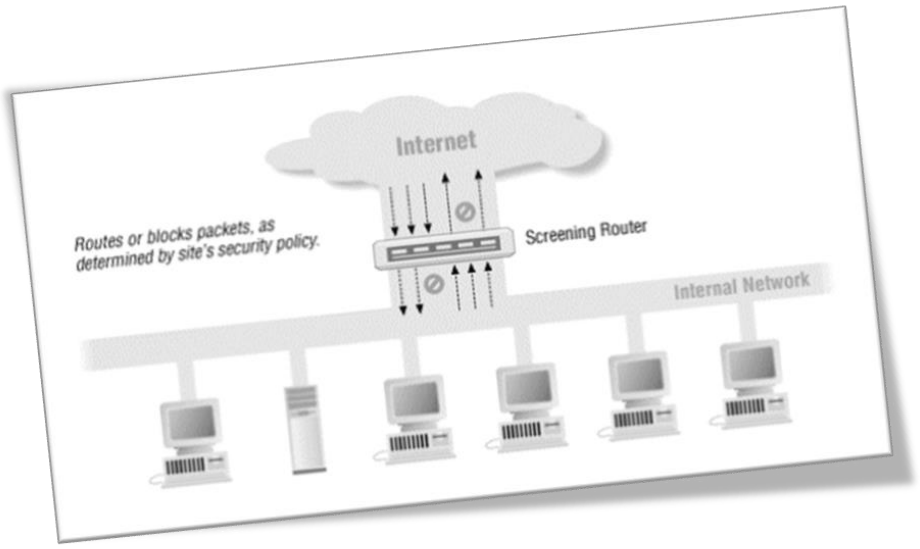
1. **ไฟร์วอลล์**

ไฟร์วอลล์ (Firewall) หมายถึง ซอฟต์แวร์หรือฮาร์ดแวร์ที่ทำหน้าที่ตรวจสอบและควบคุมระบบข้อมูลที่มาจากอินเทอร์เน็ตหรือเครือข่าย โดยสามารถกำหนดว่าอนุญาตให้ใครเข้าถึงข้อมูล

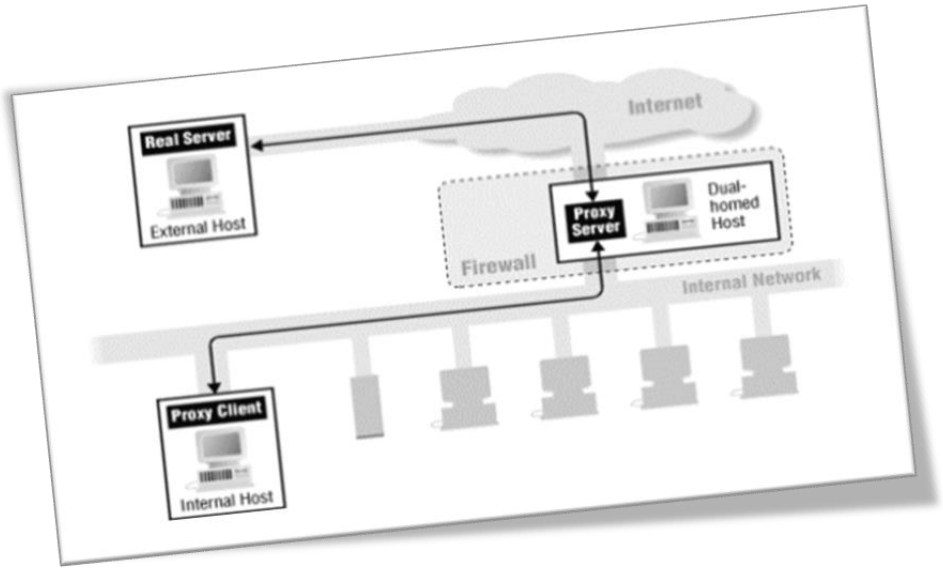


ไฟร์วอลล์สามารถแบ่งออกมาตามลักษณะการทำงาน ได้ 3 ประเภท คือ

1. Packet Filtering Firewall เราเตอร์ที่ทำการหาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎ (rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้



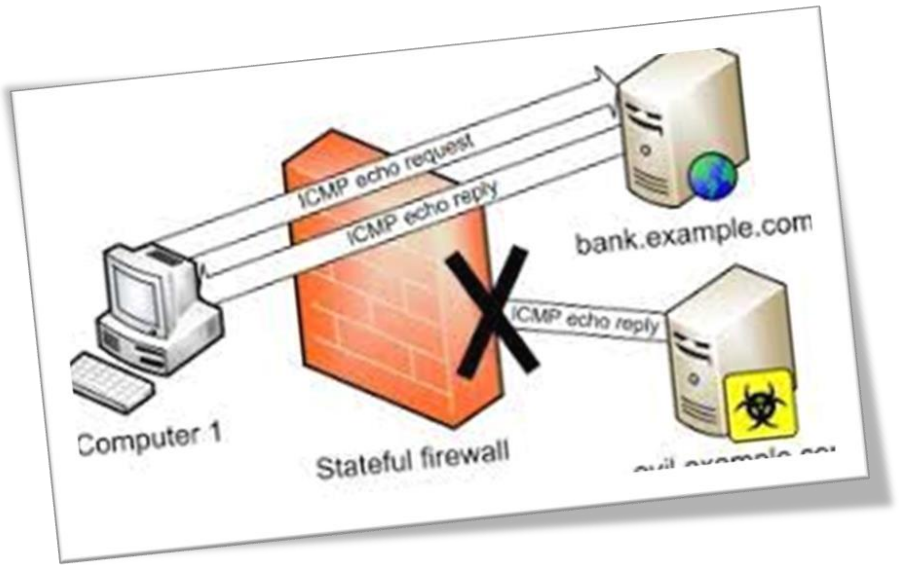
2. Application Firewall หรือ Proxy ซึ่งถูกออกแบบมาเพื่อแก้จุดบกพร่องของ Packet Filtering Firewall โดย Application Firewall จะทำหน้าที่เหมือนคนกลางที่คอยติดต่อระหว่างด้านในกับด้านนอกเครือข่าย



Proxy หรือ Application Gateway เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)

เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก ไคลเอนต์จะทำการติดต่อไปยัง Proxy ก่อน ไคลเอนต์จะเจรจา (negotiate) กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่

3. Stateful Firewall ประเภทนี้เป็นการตรวจสอบสถานะไม่ใช่เพียงแค่ตรวจสอบ Packet แต่ยังติดตามว่า Packet นั้นเคยเข้ามาในเครือข่ายนี้แล้ว หรือเข้ามาครั้งแรก โดยจะนำเอาข้อมูลของ Packet และข้อมูลที่ได้จาก Packet ก่อนหน้านี้มาพิจารณารวมกัน ซึ่งประเภทนี้จะมีความปลอดภัยมากกว่าการตรวจสอบเส้นทาง หรือการกรอง Packet เพียงอย่างเดียว



2. AAA Server

AAA หมายถึง Authenticate, Authorization และ Accounting เป็นการเพิ่มความปลอดภัย ในการใช้งานแบบ Remote Access VPN ซึ่งจะมีการตรวจสอบดังนี้ คือ

1. คุณเป็นใคร Who you are (Authentication)

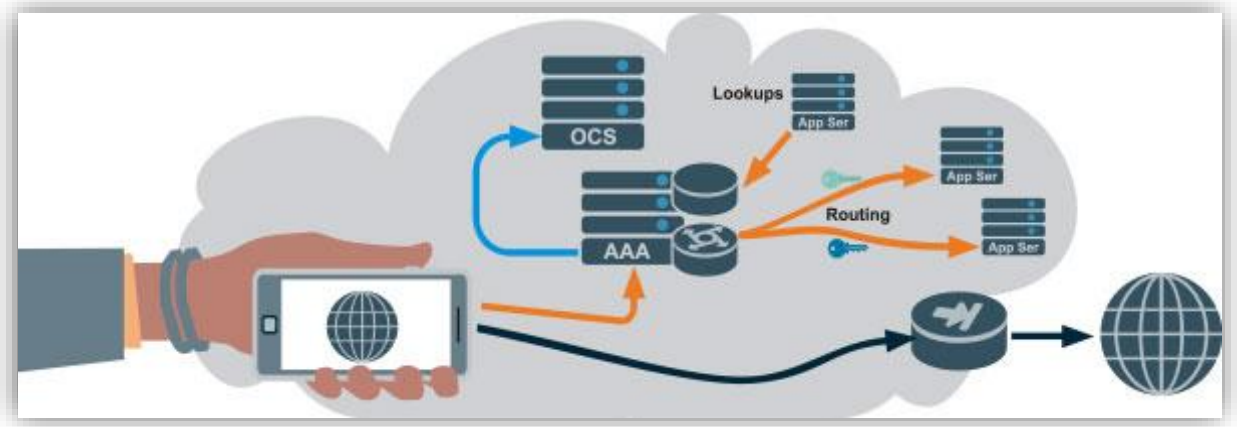
2. คุณได้รับอนุญาตให้ทำอะไรบ้าง What you are allowed to do (Authorization)

3. คุณทำอะไรไปบ้าง What you actually do (Accounting)

Authentication คือ การตรวจสอบผู้ใช้บริการอินเทอร์เน็ตโดยตรวจสอบจาก Username และ Password ว่าถูกต้องหรือไม่

Authorization คือ การตรวจสอบ "สิทธิ" ของผู้ใช้บริการอินเทอร์เน็ต ในเรื่องของเวลาการใช้ งาน หรือความเร็วในการใช้งาน

Accounting คือ ขบวนการที่ใช้ในการบันทึกข้อมูลการใช้อินเทอร์เน็ต



บรรณานุกรม

สำนักงานคณะกรรมการการอาชีวศึกษา กระทรวงศึกษาธิการ. (2565). อุปกรณ์รักษาความปลอดภัย (Security device). ใน คุณพนม บุญญ์ไพร และ คุณมาลี แผงดี, *เครือข่ายคอมพิวเตอร์เบื้องต้น (Introduction to Computer Networks) รหัสวิชา 20204 - 2005.*