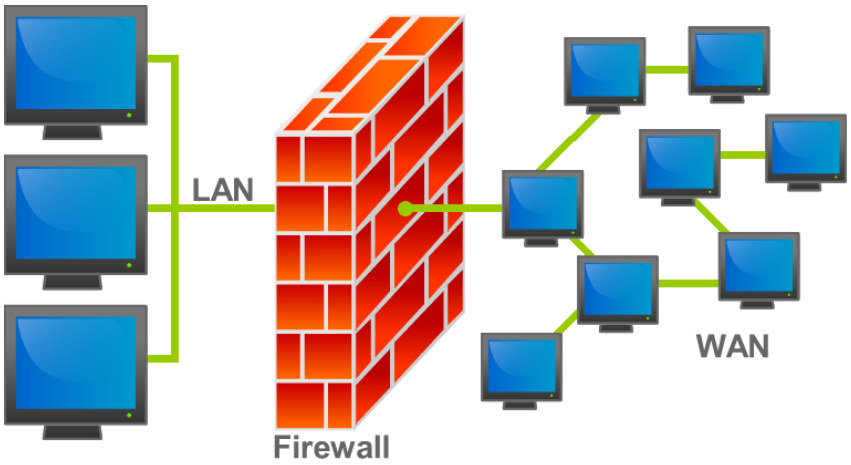
# Firewall




Firewall  คืออะไร

Firewall เป็นซอฟต์แวร์หรือฮาร์ดแวร์ชนิดหนึ่ง ที่มีหน้าที่ตรวจสอบแพ็คเกจที่ผ่านเข้า-ออกระบบเครือข่าย คัดกรองข้อมูลที่เข้ามาว่าเป็นข้อมูลอะไร มาจากที่ไหนและจะส่งไปที่ใด เพื่อเป็นการป้องกันว่าข้อมูลที่จะส่งผ่านเข้ามานั้นมีความปลอดภัยหรือไม่ ด้วยการตั้งกฎ (Rule) หรือนโยบาย (Policy) ของผู้ดูแลระบบ หากแพ็คเกจไม่ตรงตามกฎที่ตั้งไว้แม้เพียงข้อเดียว Firewall ก็จะไม่ให้ผ่าน Firewall เข้าไปได้

ทำไมต้องติดตั้ง Firewall

เดิมการใช้งานคอมพิวเตอร์ส่วนใหญ่ จะเป็นการใช้งานส่วนบุคคล ดังนั้น ปัญหาต่าง ๆ ที่เกิดขึ้นในระหว่างการใช้งานจึงมีไม่มากนัก ต่อมาเมื่อมีการใช้งานระบบเครือข่ายอินเตอร์เน็ตมากขึ้น ทุกองค์กร ทุกธุรกิจมีการนำอินเตอร์เน็ตมาใช้ในการติดต่อสื่อสาร และ ดำเนินธุรกิจ ดังนั้น ผลพวงที่ตามมาคือ อาจมีผู้ไม่ประสงค์ดี หรือแฮกเกอร์ หาวิธีเข้ามาขโมยข้อมูล หรือ ทดสอบความสามารถของตนเอง ตลอดจนยังมีไวรัสคอมพิวเตอร์ ก็ได้อาศัยช่องทางของเครือข่ายอินเตอร์เน็ต เป็นช่องทางในการแพร่กระจายไวรัสด้วยเช่นกัน การติดตั้ง Firewall ก็จะช่วยคัดกรองภัยคุกคามดังกล่าว ไม่ให้เข้ามาในเครือข่ายได้นั่นเอง

Firewall มีกี่ชนิด แต่ละประเภทมีข้อดี-ข้อเสียอย่างไร

ในปัจจุบัน Firewall มีทั้งหมด 2 ชนิด แบ่งเป็น Hardware Firewall กับ Software Firewall ดังนี้

**1.Hardware Firewall**

เป็นอุปกรณ์ที่ถูกออกแบบมาเป็น Hardware ในลักษณะเฉพาะ จึงทำให้มีความเสถียร ปลอดภัยและ มีความเร็วในการทำงานสูง และยังยากต่อการเจาะเข้าระบบ ยกเว้นแต่แฮกเกอร์จะพัฒนาวิธีการในการเจาะระบบที่เฉพาะอุปกรณ์ Hardware นั้น ๆ โดยที่ Hardware Firewall จะวางกั้นระหว่าง เครือข่ายภายใน ก่อนออกสู่ภายนอก โดยมีข้อดีหลักของ Hardware Firewall ดังนี้

- ปกป้องเครือข่ายแบบรวมศูนย์
- เนื่องจากไม่แชร์ Hardware กับใครจึงมีช่องโหว่ให้โจมตีน้อยกว่า
- เร็วกว่า ทำให้ลดเวลาในการประมวลผลแพ็คเกจลง
- รองรับ Bandwidth ได้จำนวนมาก
- กรองแพ็คเกจด้วยการตั้ง Rule ที่ตั้งมาจากผู้ผลิต
- เพราะเป็น Hardware แยกต่างหาก ทำให้ไม่ต้องใช้ทรัพยากรร่วมกับ Server ต่าง ๆ
- สามารถทำ VPN ในกรณีที่ต้องการการเชื่อมต่อที่ปลอดภัยมากขึ้น

Hardware Firewall มีทั้งหมด 5 ประเภท ดังนี้

**Packet Filtering Firewall :** เป็น Firewall ที่จะทำการตรวจสอบแพ็คเกจ (กลุ่มข้อมูล) ว่าตรงกับเงื่อนไขหรือเกณฑ์ที่ผู้ดูแลระบบกำหนดไว้หรือไม่
ถ้าผ่านเกณฑ์ทั้งหมด = ข้อมูลมีความน่าเชื่อถือข้อมูลก็จะถูกส่งออกไปหรือรับเข้ามาในเครือข่าย
ถ้าไม่ผ่านเกณฑ์ = ข้อมูลไม่น่าเชื่อถือ ข้อมูลก็จะถูกปฏิเสธการนำเข้าหรือส่งออก

ข้อดี : ประสิทธิภาพในการประมวลผลแพ็คเกจ
ข้อเสีย : มีความเสี่ยงต่อการถูกโจมตี

**Circuit-level Gateway :** เป็น Firewall ที่ใช้ตรวจสอบเส้นทางการเชื่อมต่อของเครือข่าย โดยสร้างแบบจำลองโครงข่ายการเชื่อมต่อขึ้น เพื่อพิจารณาความน่าเชื่อถือของเครือข่ายที่เชื่อมต่อเข้ามา โดย Firewall ประเภทนี้จะไม่สามารถตรวจสอบ Packet ด้วยตนเองได้ แต่การตรวจสอบ Packet จะทำงานบน Transport Layer ใน OSI Model

ข้อดี : การรับส่งและประมวลผลข้อมูลดีกว่า Application-level Gateway
ข้อเสีย : ไม่สามารถกรองเนื้อหา Packet ที่เข้ามาได้

**Stateful Inspection Firewall :** เป็น Firewall ที่ใช้ตรวจสอบ Packet ซึ่งสามารถตรวจสอบได้ว่า Packet นี้เคยเข้ามาในระบบเครือข่ายหรือไม่ โดยนำข้อมูลของแพ็คเกจเดิมและ Packet ปัจจุบันมาตรวจสอบกัน ซึ่งมีความปลอดภัยกว่าการกรองแพ็คเกจ หรือการตรวจสอบเส้นทางการเชื่อมต่อเพียงอย่างเดียว

ข้อดี : ปิดกั้นและป้องกันการโจมตีช่องโหว่ของ Protocol ได้
ข้อเสีย : ผู้ดูแลระบบต้องมีความรู้เป็นพิเศษเพื่อการกำหนดค่าที่ปลอดภัย

**Application-level Gateway :** เป็น Firewall ประเภทที่ตรวจสอบเส้นทางการส่งข้อมูลและเนื้อหาของ Packet ในระดับ Application นอกจากนั้นยังกรองและปิดกันการโจมตีที่มองไม่เห็นบนเครือข่าย OSI Model ได้ และยังสามารถทำหน้าที่แทน Proxy Firewall ได้ในบางครั้ง
ข้อดี : สามารถตรวจสอบและปิดกั้นการโจมตีที่มองไม่เห็นจากเครือข่ายจำลองบน OSI Model ได้
ข้อเสีย : มีค่าใช้จ่ายสูงและต้องมีการติดตั้ง Proxy สำหรับแอปพลิเคชั่นเครือข่ายทุกตัวที่ใช้งาน

**Next-generation Firewall :** เป็น Firewall ที่มีประสิทธิภาพสูง และสามารถรับมือภัยคุกคามที่ซับซ้อน รวมการตรวจสอบเส้นทางเครือข่ายเข้ากับการตรวจสอบ Packet และยังรวมถึง Deep Packet Inspection (DPI) เป็นการรวมรูปแบบของ Packet ที่หลากหลาย รวมทั้งระบบรักษาความปลอดภัยเครือข่ายอื่นๆ เช่น การตรวจจับ / ป้องกันการบุกรุกการกรองมัลแวร์ และโปรแกรมป้องกันไวรัส โดยฟังก์ชันที่เพิ่มมีความแตกต่างจาก Firewall ทั่วไป คือ การเข้าถึงระดับ Application Layer สามารถแยกการใช้งานของ Application Layer ว่าเป็นการใช้โปรแกรม LINE, Facebook, Youtube หรือเป็นโปรแกรมประเภทอะไร ทำให้สามารถตั้ง Policy เพื่อทำการควบคุมการใช้งาน Application ต่าง ๆ เหล่านั้นได้

ข้อดี : รวมความสามารถของ Firewall ประเภทอื่นและระบบความปลอดภัยอื่นๆ เข้าไว้ด้วยกัน สามารถใช้งานได้รอบด้าน
ข้อเสีย : มีค่าใช้จ่ายสูงและต้องมีการกำหนดค่าโดยผู้เชี่ยวชาญเพื่อให้ Firewall สามารถทำงานบนระบบที่ซับซ้อนได้อย่างมีประสิทธิภาพ

**2. Software Firewall**

Software Firewall เป็นโปรแกรมที่ใช้ติดตั้งบน Client หรือ Server โดยสามารถดาวน์โหลดมาติดตั้งได้ และ ยังมีแบบที่เป็นโปรแกรมที่ติดตั้งมากับระบบปฏิบัติการคอมพิวเตอร์ด้วย เช่น Windows Defender (ระบบปฏิบัติการ Windows) และ UFW (ระบบปฏิบัติการ Ubuntu) ซึ่ง Software Firewall จะมีข้อดีหลัก ๆ ดังนี้

- มีทั้งแบบฟรี และเสียค่าใช้จ่าย ในราคาที่ไม่แพง
- ติดตั้งโดยไม่ต้องติดตั้งพื้นที่ใน Data Center เพิ่มเติม
- ติดตั้งได้ง่าย เพียงดาวน์โหลดมาติดตั้งเองได้ และมีค่า Default ที่สามารถป้องกันพื้นฐานได้ทันที
- ไม่ติดกับ Hardware สามารถลงได้บน Hardware ที่หลากหลาย

| Hardware Firewall | Software Firewall |
|---|---|
| • ปกป้องเครือข่ายแบบรวมศูนย์<br>• ไม่แชร์ Hardware ร่วมกับคนอื่น จึงทำให้มีช่องโหว่ให้โจมตีน้อยกว่า เร็วกว่า ทำให้ลดเวลาในการประมวลผลแพคเกจลง<br>• รองรับจำนวน Bandwidth ได้สูง<br>• กรองแพคเกจด้วยการตั้ง Rule ที่ตั้งจากผู้ผลิต<br>• เนื่องจากเป็น Hardware ที่แยกจาก Server จึงทำให้ไม่กินทรัพยากรของ Server<br>• สามารถทำ VPN ในกรณีที่ต้องการ การเชื่อมต่อ<br>• ที่ปลอดภัยมากขึ้น | • มีทั้งแบบฟรี และเสียค่าใช้จ่าย<br>• ติดตั้งโดยไม่ต้องติดตั้งพื้นที่ Data Center เพิ่มเติม<br>• ติดตั้งได้ง่าย เพียงดาวน์โหลดมาพร้อมติดตั้งด้วยค่า Default พื้นฐานของโปรแกรม<br>• ไม่ติดกับ Hardware สามารถติดตั้งได้กับ Hardware ที่หลากหลาย |