ความรู้พื้นฐานเกี่ยวกับ Firewall

Firewall คืออะไร

Firewall นั้นหากจะแปลตรงตัวจะแปลว่ากำแพงไฟ แต่ที่จริงแล้ว firewall นั้นเป็นกำแพงที่มีไว้เพื่อป้องกันไฟโดยที่ตัวมันเองนั้นไม่ใช่ไฟตามดังคำแปล firewall ในสิ่งปลูกสร้างต่างๆนั้นจะทำด้วยอิฐเพื่อแยกส่วนต่างๆของสิ่งปลูกสร้างออกจากกันเพื่อที่ว่าในเวลาไฟไหม้ไฟจะได้ไม่ลามไปทั่วสิ่งปลูกสร้างนั้นๆ หรือ Firewall ในรถยนต์ก็จะเป็นแผ่นโลหะใช้แยกส่วนของเครื่องยนต์และส่วนของที่นั่งของผู้โดยสารออกจากกัน

ในเครือข่าย Internet นั้น firewall อาจถูกใช้สำหรับป้องกันไม่ให้ "ไฟ" จากเครือข่าย Internet ภายนอกลามเข้ามาภายในเครือข่าย LAN ส่วนตัวของท่านได้ หรืออาจถูกใช้เพื่อป้องกันไม่ให้ผู้ใช้ใน LAN ของท่านออกไปโดน "ไฟ" ในเครือข่าย Internet ภายนอกได้

ตามคำจำกัดความแล้ว firewall หมายความถึง ระบบหนึ่งหรือกลุ่มของระบบที่บังคับใช้นโยบายการควบคุมการเข้าถึงของระหว่างเครือข่ายสองเครือข่าย โดยที่วิธีการกระทำนั้นก็จะแตกต่างกันไปแล้วแต่ระบบ แต่โดยหลักการแล้วเราสามารถมอง firewall ได้ว่าประกอบด้วยกลไกสองส่วนโดยส่วนแรกมีหน้าที่ในการกั้น traffic และส่วนที่สองมีหน้าที่ในการปล่อย traffic ให้ผ่านไปได้

ประเภทของ Firewall

Firewall โดยทั่วไปจะถูกแบ่งออกเป็น ๒ ประเภทคือ firewall ระดับ network (network level firewall) และ firewall ระดับ application (application level firewall)

ก่อนที่ firewall ระดับ network จะตัดสินใจยอมให้ traffic ใดผ่านนั้นจะดูที่ address ผู้ส่งและผู้รับ และ port ในแต่ละ IP packet เมื่อพิจารณาแล้วเห็นว่า traffic สามารถผ่านไปได้ก็จะ route traffic ผ่านตัวมันไปโดยตรง router โดยทั่วไปแล้วก็จะถือว่าเป็น firewall ระดับ network ชนิดหนึ่ง firewall ประเภทนี้จะมีความเร็วสูงและจะ transparent ต่อผู้ใช้ (คือผู้ใช้มองไม่เห็นความแตกต่างระหว่างระบบที่ไม่มี firewall กับระบบที่มี firewall ระดับ network อยู่) การที่จะใช้ firewall ประเภทนี้โดยมากผู้ใช้จะต้องมี IP block (ของจริง) ของตนเอง

Firewall ระดับ application นั้นโดยทั่วไปก็คือ host ที่ run proxy server อยู่ firewall ประเภทนี้สามารถให้รายงานการ audit ได้อย่างละเอียดและสามารถบังคับใช้นโยบายความปลอดภัยได้มากกว่า firewall ระดับ network แต่ firewall ประเภทนี้ก็จะมีความ transparent น้อยกว่า firewall ระดับ network โดยที่ผู้ใช้จะต้องตั้งเครื่องของตนให้ใช้กับ firewall ประเภทนี้ได้ นอกจากนี้ firewall ประเภทนี้จะมีความเร็วน้อยกว่า firewall ระดับ network

บางแหล่งจะกล่าวถึง firewall ประเภทที่สามคือประเภท stateful inspection filtering ซึ่งใช้การพิจารณาเนื้อหาของ packets ก่อนๆในการที่จะตัดสินใจให้ packet ที่กำลังพิจารณาอยู่เข้ามา

ขีดความสามารถของ Firewall

ขีดความสามารถของ firewall ทั่วๆไปนั้นมีดังต่อไปนี้

- ป้องกันการ login ที่ไม่ได้รับอนุญาตที่มาจากภายนอกเครือข่าย
- ปิดกั้นไม่ให้ traffic จากนอกเครือข่ายเข้ามาภายในเครือข่ายแต่ก็ยอมให้ผู้ที่อยู่ภายในเครือข่ายสามารถติดต่อกับโลกภายนอกได้

- เป็นจุดรวมสำหรับการรักษาความปลอดภัยและการทำ audit (เปรียบเสมือนจุดรับแรงกระแทก หรือ “choke” ของเครือข่าย)

<u>ข้อจำกัดของ firewall</u>

ข้อจำกัดของ firewall มีดังต่อไปนี้

- firewall ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่าน firewall (เช่น การโจมตีจากภายในเครือข่ายเอง)
- ไม่สามารถป้องกันการโจมตีที่เข้ามากับ application protocols ต่างๆ (เรียกว่าการ tunneling) หรือกับโปรแกรม client ที่มีความล่อแหลมและถูกดัดแปลงให้กระทำการโจมตีได้ (โปรแกรมที่ถูกทำให้เป็น Trojan horse)
- ไม่สามารถป้องกัน virus ได้อย่างมีประสิทธิภาพเนื่องจากจำนวน virus มีอยู่มากมาย จึงจะเป็นการยากมากที่ firewall จะสามารถตรวจจับ pattern ของ virus ทั้งหมดได้

ถึงแม้ว่า firewall จะเป็นเครื่องมือที่สามารถนำมาใช้ป้องกันการโจมตีจากภายนอกเครือข่ายได้อย่างมีประสิทธิภาพ การที่จะใช้ firewall ให้ได้ประโยชน์สูงสุดนั้นจะขึ้นอยู่กับนโยบายความปลอดภัยโดยรวมขององค์กรด้วย นอกจากนี้ แม้แต่ firewall ที่ดีที่สุดก็ไม่สามารถนำมาใช้แทนการมีจิตสำนึกในการที่จะรักษาความปลอดภัยภายในเครือข่ายของผู้ที่อยู่ในเครือข่ายนั้นเอง