โดย: บรรจง หะรังษี
พุธ นาฑีสุวรรณ

# แนะนำไฟร์วอลล์เบื้องต้น

การบุกรุกเข้าสู่เครือข่ายภายในองค์กรจากอินเทอร์เน็ตนับวันเริ่มทวีความรุนแรงมากขึ้นเรื่อยๆ บางครั้งการบุกรุกอาจจะนำมาซึ่งความเสียหายและสูญเสียเพียงเล็กน้อย แต่ทว่าในบางครั้งก็สามารถนำมาซึ่งความเสียหายและสูญเสียอย่างมากมาสู่องค์กรได้ อาทิ การขโมยเลขบัตรเครดิตที่เก็บอยู่ในอิเล็กทรอนิกส์ไฟล์ การเปิดเผยข้อมูลที่เป็นความลับขององค์กร ส่วนตัว หรือทางทรัพย์สินทางปัญญาเป็นต้น

ไฟร์วอลล์เป็นหนทางหนึ่งที่สามารถลดหรือกำจัดปัญหาการบุกรุกทางอินเทอร์เน็ตได้ และเป็นทางเลือกที่ประหยัดค่าใช้จ่ายในการลงทุน อีกทั้งยังมีประสิทธิภาพและผลสูง ในปัจจุบันไฟร์วอลล์ได้รับความนิยมมากขึ้นเรื่อยๆ ที่จะนำมาใช้งานกับองค์กร บทความนี้มีจุดมุ่งหมายที่จะแนะนำให้ผู้อ่านได้รู้จักกับไฟร์วอลล์เบื้องต้น องค์ประกอบของไฟร์วอลล์ สถาปัตยกรรมประเภทต่างๆ ของไฟร์วอลล์ อีกทั้งทางเลือกขององค์กรที่จะซื้อหรือสร้างไฟร์วอลล์ขึ้นมาใช้งานเอง

บทความนี้มีจุดมุ่งหมายที่จะแนะนำให้ท่านผู้อ่านได้รู้จักกับไฟร์วอลล์เบื้องต้นโดยผู้เขียนจะเริ่มต้นจากการให้คำนิยามของไฟร์วอลล์ แสดงให้เห็นถึงความจำเป็นของการใช้ไฟร์วอลล์ ตลอดจนองค์ประกอบและสถาปัตยกรรมแบบต่างๆ ของไฟร์วอลล์

ประเด็นต่างๆ ดังกล่าวข้างต้นเป็นข้อมูลโดยพื้นฐาน ของไฟร์วอลล์ซึ่งองค์กรต่างๆ ทั้งภาครัฐและเอกชนควรจะได้เริ่มทำความรู้จักคุ้นเคยอันจะนำไปสู่การตระหนักถึงความสำคัญของไฟร์วอลล์ที่มีต่อองค์กร โดยเฉพาะอย่างยิ่งองค์กรที่มีการเชื่อมต่อกับอินเทอร์เน็ต หรือพูดง่ายๆ ก็คือไฟร์วอลล์ทำหน้าที่เป็นนายด่านประตูเข้าออกสู่อินเทอร์เน็ตนั่นเอง

บทความนี้จะนำเสนอโดยเรียงลำดับหัวข้อตามประเด็นต่างๆ ดังต่อไปนี้

- ไฟร์วอลล์คืออะไร
- ทำไมจึงจำเป็นต้องใช้ไฟร์วอลล์
- สิ่งที่ไฟร์วอลล์ป้องกันได้
- สิ่งที่ไฟร์วอลล์ป้องกันไม่ได้
- องค์ประกอบสำคัญของไฟร์วอลล์
- สถาปัตยกรรมประเภทต่างๆ ของไฟร์วอลล์ที่พบเห็นกันบ่อยๆ และ
- จะซื้อไฟร์วอลล์ใหม่หรือจะสร้างขึ้นมาเอง

ในบทความนี้คำดังต่อไปนี้จะปรากฏอยู่ทั่วไปซึ่งมีความหมายดังนี้

**บริการบนอินเทอร์เน็ต (Internet Services)** หมายถึง การใช้บริการบนอินเทอร์เน็ต อาทิ บริการ

– SMTP (Simple Mail Transfer Protocol) เพื่อใช้ในการส่งและรับอีเมล์

– TELNET เพื่อใช้ในการติดต่อสื่อสารกับเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งซึ่งตั้งอยู่ห่างไกลออกไป

– FTP (File Transfer Protocol) เพื่อใช้ในการโอนย้ายไฟล์ระหว่างเครื่องคอมพิวเตอร์สองเครื่อง

– DNS (Domain Name Service) เพื่อใช้ในการแปลงชื่อเครื่อง เช่น notes.nectec.or.th ให้เป็น IP แอดเดรส (ที่อยู่ของเครื่องๆ นั้นบนอินเทอร์เน็ต)

– TELNET, FTP และบริการอื่นๆ จะเรียกใช้บริการ DNS เพื่อทำการสอบถาม IP แอดเดรสของเครื่องคอมพิวเตอร์ที่จะทำการติดต่อสื่อสารกัน

– Gopher เพื่อใช้ในการสืบค้นข้อมูลโดยตัวเซิร์ฟเวอร์ของ Gopher จะทำการจัดเก็บข้อมูลเอาไว้และตัวบราวเซอร์ของ Gopher จะสามารถบราวผ่านอินเทอร์เน็ตเข้ามาสืบค้นข้อมูลที่อยู่บนเซิร์ฟเวอร์นั้นได้

– WWW (World Wide Web) หรือ HTTP (Hypertext Transfer Protocol) บริการนี้จะครอบคลุมทั้ง FTP และ Gopher (ที่กล่าวถึงข้างบน) อยู่ในตัวมันทั้งหมด เป็นต้น

**การสื่อสาร (Traffic)** ในบทความฉบับนี้ส่วนใหญ่จะหมายถึง การสื่อสารอิเล็กทรอนิกส์ที่เข้าหรือออกจากองค์กรโดยผ่านทางเครือข่ายภายในองค์กรและอินเทอร์เน็ต และเมื่อกล่าวถึงคำ “ประเภทของการสื่อสาร” ผู้เขียนจะหมายถึงประเภทของบริการบนอินเทอร์เน็ตต่างๆ ดังที่ได้กล่าวไว้ข้างบน

แพ็กเก็ต (Packet) (6) หมายถึง เมื่อมีการรับหรือส่งข้อมูลกันในระบบเครือข่ายอินเทอร์เน็ตตัวข้อมูล เช่น ข้อความอีเมล์ ไฟล์ต่างๆ อาทิ ไฟล์ HTML จะถูกทำให้มีขนาดเล็กลงโดยแบ่งออกเป็นส่วนย่อยๆ ซึ่งเรียกกันว่า Data Packet หรือเรียกสั้นๆ ว่า แพ็กเก็ตนั่นเอง

## ไฟร์วอลล์คืออะไร

ระบบหรือกลุ่มของระบบที่ทำหน้าที่ควบคุมการสื่อสารที่เกิดขึ้นระหว่างเครือข่ายอย่างน้อย 2 เครือข่าย เพื่อให้การสื่อสารหนึ่งๆ ที่เกิดขึ้นนั้นเป็นไปตามนโยบายเครือข่ายขององค์กร (Network Access Policy) (1,3) ระบบหรือกลุ่มของระบบดังกล่าวอาจจะอนุญาตหรือไม่อนุญาตให้การสื่อสารหนึ่งๆ เกิดขึ้น ทั้งนี้จะขึ้นอยู่กับนโยบายเครือข่ายขององค์กรที่ได้กำหนดเอาไว้ (อาจจะเป็นลายลักษณ์อักษรหรือไม่ก็ตาม) ระบบหรือกลุ่มของระบบดังกล่าวจะมีคอมพิวเตอร์และซอฟต์แวร์เป็นองค์ประกอบโดยพื้นฐาน

อีกนัยหนึ่ง ผู้อ่านสามารถมองว่าอินเทอร์เน็ตคือเครือข่ายที่มีขนาดใหญ่มหึมาอันหนึ่ง และเครือข่าย

ภายในองค์กรของเราก็เป็นอีกเครือข่ายหนึ่ง โดยเครือข่ายทั้งสองนี้จะเชื่อมโยงถึงกันและทำให้เกิดการสื่อสารเข้าออกจากองค์กรได้ ระบบหรือกลุ่มของระบบซึ่งได้ทำการติดตั้งไว้ภายในองค์กรและทำหน้าที่เป็นไฟร์วอลล์จะทำหน้าที่ควบคุมหรือจำกัดการสื่อสารที่ผ่านเข้าออกระหว่างสองเครือข่ายนี้

## ทำไมต้องใช้ไฟร์วอลล์

บนอินเทอร์เน็ตมีกลุ่มคนประเภทแอตแทกเกอร์หรือแฮกเกอร์ที่ชอบเข้ามาแอบด้อมๆ มองๆ ดูซิว่าไซต์ (องค์กร) ของเรามีอะไรดีๆ น่าสนใจบ้าง บางครั้งยังสะท้อนถึงการเข้ามาขโมยทรัพย์สินต่างๆ เช่น หมายเลขบัตรเครดิตที่เก็บอยู่ในอิเล็กทรอนิกส์ไฟล์ต่างๆ ขององค์กรหรือทรัพย์สินทางปัญญาอื่นๆ ซึ่งในกรณีเช่นนี้ถือเป็นการกระทำที่ผิดทางกฎหมาย นอกจากนั้นแล้วกลุ่มคนดังกล่าวยังอาจจะชอบ "ลองของ" กับไซต์ดังๆ เช่น AT&T, ทำเนียบขาว, World Bank หรืออื่นๆ ซึ่งอาจจะดูแล้วเป็นสิ่งที่น่าท้าทายสำหรับกลุ่มคนดังกล่าว และเพื่อจะดูซิว่าไซต์ต่างๆ เหล่านี้มีความแกร่งต่อการถูกแฮ็กโดยพวกเขาหรือไม่

ปัจจุบันเป็นยุคของสารสนเทศ องค์กรต่างๆ แข่งขันกันด้วยการใช้สารสนเทศในรูปแบบต่างๆ สารสนเทศที่องค์กรจัดเก็บไว้บนอิเล็กทรอนิกส์ไฟล์ต่างๆ และอยู่ในเครือข่ายภายในขององค์กรจึงจำเป็นต้องได้รับการคุ้มครองป้องกัน เพื่อมิให้เกิดการเสียหาย ถูกเปลี่ยนแปลงแก้ไข (อันจะนำไปสู่การผิดจากวัตถุประสงค์เดิม) (7) ถูกขโมยไป (เช่นสารสนเทศที่เกี่ยวกับทรัพย์สินทางปัญญา) เป็นต้น

จากสาเหตุที่ได้กล่าวไว้ใน 2 ย่อหน้าที่แล้ว ได้ชี้ให้เห็นเป็นนัยว่า "ผู้ร้าย" สามารถเข้าสู่เครือข่ายภายในขององค์กรได้โดยผ่านทางอินเทอร์เน็ต จึงเป็นเหตุให้ผู้ดูแลเครือข่ายขององค์กรจะต้องหาทางควบคุมหรือจำกัดการเข้าออกจากเครือข่ายขององค์กร ในที่นี้ก็คือการควบคุมการสื่อสารทั้งหมดที่เข้าและออกจากองค์กรนั่นเอง และไฟร์วอลล์เป็นทางเลือกหนึ่งที่มีการใช้งานกันอย่างแพร่หลายในปัจจุบันและมีประสิทธิภาพมาก ซึ่งสามารถนำมาใช้งานเพื่อการควบคุมการสื่อสารทางเครือข่ายขององค์กร

## ไฟร์วอลล์ป้องกันอะไรได้

ไฟร์วอลล์จะยอมให้เฉพาะการสื่อสารบางประเภท เช่น อีเมล์, FTP เป็นต้น เกิดขึ้นได้ระหว่างภายในกับภายนอกองค์กรโดยนโยบายเครือข่ายขององค์กรจะเป็นตัวบอกว่าอนุญาตหรือไม่อนุญาต และดังนั้นไฟร์วอลล์จึงทำหน้าที่สกัดกั้นการสื่อสารประเภทอื่นๆ ที่เหลือทั้งหมดที่ไม่ได้มีกำหนดเอาไว้ในนโยบายเครือข่ายว่าอนุญาตให้กระทำได้

โดยปกติแล้วไฟร์วอลล์จะทำการตรวจสอบการสื่อสารที่เกิดขึ้นระหว่างภายในกับภายนอกองค์กร แต่มักจะอนุญาตให้ผู้ใช้ภายในองค์กรสามารถทำการสื่อสารกันภายในองค์กรได้อย่างเต็มที่ ดังนั้นไฟร์วอลล์จึงเปรียบเสมือนเป็นเกตเวย์ (ประตูเข้าออก) ขององค์กร และโดยปกติควรจะเป็นประตูเข้าออกแต่เพียงทางเดียวเท่านั้น (ไม่ควรมีทางเข้าออกอื่นๆ) เพื่อว่าไฟร์วอลล์จะได้สามารถควบคุมการสื่อสารทั้งหมดได้อย่างแท้จริงซึ่งเกิดขึ้นระหว่างภายในและภายนอกองค์กร

ผู้ดูแลเครือข่ายขององค์กรสามารถทำการคอนฟิกไฟร์วอลล์เพื่อให้ทำการบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ข้อมูลต่างๆ ที่เรียกกันว่า log ที่ได้จากการบันทึกสามารถนำมาใช้ในการวิเคราะห์โดยเจ้าหน้าที่ดูแลเครือข่ายเพื่อตรวจสอบประเภทของการสื่อสารต่างๆ ที่เกิดขึ้น ปริมาณการสื่อสารที่เกิดขึ้น นอกจากนั้นแล้วข้อมูล log นี้ยังอาจจะสะท้อนถึงว่าได้มีการใช้ความพยายามกี่ครั้งแล้วที่จะบุกรุกเข้าสู่เครือข่ายภายในองค์กรของเรา

## ไฟร์วอลล์ป้องกันอะไรไม่ได้

ไฟร์วอลล์จะไม่สามารถป้องกันการบุกรุกใดๆ ก็ตามที่ไม่ได้กระทำผ่านทางเกตเวย์ (ประตูเข้าออก) ขององค์กร เช่น การลักลอบนำข้อมูลสำคัญขององค์กรออกไปทางดิสก์หรือเทป การคุยกันทางโทรศัพท์บอกความลับขององค์กร การส่งแฟกซ์ซึ่งเป็นข้อมูลความลับขององค์กร เป็นต้น การกระทำดังกล่าวทั้งสิ้นถือเป็นความพยายามที่จะหลีกเลี่ยงหรือเล็ดลอดกลไกการทำงานตรวจสอบตามปกติของไฟร์วอลล์

มีคำพูดหนึ่งที่สะท้อนให้เห็นว่าไฟร์วอลล์ก็ช่วยอะไรเราไม่ได้ กล่าวคือ "จะมีประโยชน์อะไรที่คุณอุตส่าห์ทำเกตเวย์หนาตั้ง 6 ฟุต (ไฟร์วอลล์ที่แข็งแรง

มาก) แต่คุณปล่อยให้มีประตูหลังเข้าออกองค์กรในที่อื่นๆ (ที่ไม่ใช่ตำแหน่งของเกตเวย์ขององค์กร) (1) เพราะนั่นหมายถึงว่าผู้ร้ายจะสามารถเล็ดลอดผ่านเข้าออกทางประตูหลัง อาทิ การล็อกอินเข้าสู่ระบบโดยผ่านทางโมเด็ม เป็นต้น"

ดังนั้นสิ่งที่ฝ่ายบริหารขององค์กรจะต้องคำนึงถึงเป็นอย่างยิ่งคือนโยบายทางด้านความมั่นคงปลอดภัยขององค์กร ซึ่งรวมถึงนโยบายเครือข่ายขององค์กรจะต้องมีความสอดคล้องกับโครงสร้างรากฐานทางด้านความมั่นคงปลอดภัยขององค์กร ในกรณีข้างบนโครงสร้างรากฐานมีรอยรั่วซึ่งก็คือการล็อกอินโดยผ่านทางโมเด็ม ซึ่งทำให้ผู้ร้ายอาศัยเป็นช่องทางเข้าสู่เครือข่ายภายในองค์กรของเราได้

ปัญหาที่สำคัญอันหนึ่งของ TCP/IP คือ แอตแทกเกอร์สามารถสร้างแพ็กเก็ตที่ดูเสมือนว่าถูกส่งมาจากเครื่องต้นทาง (IP Source Address) เครื่องหนึ่งที่โดยนโยบายเครือข่ายขององค์กรแล้วจะได้รับการอนุญาตให้ผ่านเข้ามาได้ แต่ทว่าแพ็กเก็ตที่เข้ามาเหล่านี้นี่เองอาจจะเป็นตัวบ่อนทำลายที่เข้ามาแบบมีจุดประสงค์ร้ายแอบแฝงอยู่ เช่น การลักลอบขโมยข้อมูลสำคัญๆ ต่างๆ ขององค์กรได้ (7) เป็นต้น (วิธีการบุกรุกเครือข่ายในลักษณะดังกล่าวมีชื่อเรียกกันว่า Spoofing Attack (4,5)) ไฟร์วอลล์โดยเนื้อแท้แล้วจะเพียงหยิบแพ็กเก็ตขึ้นมาดูแต่จะไม่สามารถบอกได้อย่าง "เต็มปาก" ว่าแพ็กเก็ตที่หยิบขึ้นมาดูนั้นมาจากเครื่องต้นทางที่ถูกแท้แน่จริงหรือไม่ (5) และดังนั้นอาจนำมาสู่ปัญหาการบุกรุกเครือข่ายได้

โดยปกติข้อมูลที่ผ่านออกจากไฟร์วอลล์ขององค์กรของเราไปสู่อินเทอร์เน็ตและมุ่งหน้าไปสู่อีกองค์กรหนึ่ง (ที่องค์กรของเราอนุญาตให้ทำการติดต่อสื่อสารด้วยได้) จะไม่มีการเข้ารหัส สาเหตุที่เป็นเช่นนั้นเป็นเพราะว่าหากมีการเข้ารหัสองค์กรปลายทางจะต้องรู้วิธีการถอดรหัสข้อมูลซึ่งโดยปกติแล้วองค์กรปลายทางอาจจะไม่มีความสัมพันธ์ใดๆ ทั้งสิ้นกับองค์กรของเรา และดังนั้นจึงไม่จำเป็นจะต้องรู้วิธีการถอดรหัสน์ข้อมูลที่ผ่านเข้ามาสู่ตน พูดง่ายๆ ก็คือองค์กรของเราไม่มีสิทธิไปบังคับให้องค์กรอื่นที่ไม่มีความเกี่ยวข้องกับเราต้องรู้วิธีการเข้าหรือถอดรหัสข้อมูลนั้น ดังนั้นไฟร์วอลล์โดยทั่วไปจะไม่สามารถทำให้ข้อมูลที่ผ่านเข้าออกจากตัวของมันเป็นความลับได้

## องค์ประกอบของไฟร์วอลล์

ไฟร์วอลล์ที่พบเห็นกันโดยทั่วไปมีองค์ประกอบหลักอยู่ 4 ส่วนดังนี้

- นโยบายเครือข่าย (Network Access Policy)
- การตรวจสอบการเข้าสู่ระบบโดยใช้เทคนิคแอดวานซ์ (Advanced Authentication Mechanisms)
- ระบบกรองแพ็กเก็ต (Packet Filtering) และ
- Proxy Services

### 1. นโยบายเครือข่าย

นโยบายการใช้งานเครือข่ายซึ่งมีอิทธิพลต่อการออกแบบ ติดตั้ง และใช้งานไฟร์วอลล์ประกอบไปด้วย 2 ส่วน (3) คือ

**1.1 นโยบายในระดับบริหาร** (Service Access Policy) ส่วนนี้จะกล่าวถึงว่าองค์กรจะอนุญาตหรือไม่อนุญาตให้มีการใช้งานเครือข่ายในลักษณะอย่างไร เช่น องค์กรมีนโยบายในระดับบริหารดังนี้

- ไม่อนุญาตให้มีการใช้งาน TELNET จากอินเทอร์เน็ตเข้าสู่เครื่องในองค์กร
- อนุญาตให้ทำการสื่อสารได้เฉพาะกับอีเมล์และเว็บเซิร์ฟเวอร์ที่องค์กรจัดไว้ให้เท่านั้น
- อนุญาตให้ผู้ใช้จากอินเทอร์เน็ตโอนย้ายข้อมูลโดยโปรแกรม FTP แต่ต้องกระทำที่พอร์ตสูงๆ เช่นมากกว่า 1024 เป็นต้น

**1.2 นโยบายในระดับปฏิบัติการ** (Firewall Design Policy) ส่วนนี้จะกล่าวถึงการเซ็ตไฟร์วอลล์ให้ทำงานตามนโยบายในระดับบริหารที่ได้กำหนดเอาไว้ ดังนั้นก่อนที่จะมีการจัดหาตัวไฟร์วอลล์ โดยหลักการแล้วองค์กรจะต้องร่างนโยบายระดับบริหารออกมาก่อน เพราะนโยบายตัวนี้จะเป็นตัวบอกว่าเราจะจัดหาไฟร์วอลล์ที่มีคุณสมบัติอย่างไรเพื่อให้สามารถทำงานตามที่ได้กำหนดเอาไว้

โดยพื้นฐานแล้วเราจะใช้ขีดความสามารถของ Screening Router และ Proxy Server (ดูรายละเอียดเพิ่มเติมในหัวข้อ 6.3 และ 6.4 ตามลำดับ) ที่องค์กรจัดหามาได้ในการกำหนดให้เป็นไปตามนโยบายระดับบริหาร กล่าวคือเจ้าหน้าที่ดูแลเครือข่ายจะต้องทำการเซ็ตทั้ง Screening Router และ Proxy Server เพื่อให้เป็นไปตามนโยบายระดับบริหารที่ได้กำหนดเอาไว้

## 2. การตรวจสอบการเข้าสู่ระบบโดยใช้เทคนิคแอดวานซ์

โดยหลักการแล้วไฟร์วอลล์จะทำหน้าที่ตรวจสอบการสื่อสารโดยเฉพาะที่มาจากอินเทอร์เน็ตก่อนที่จะอนุญาตให้กระทำได้หรือไม่ ดังนั้น ณ จุดตรวจสอบนี้องค์กรควรจะได้ทำการติดตั้งระบบเพื่อใช้ในการตรวจสอบว่าผู้ใช้ท่านนั้นมีสิทธิที่จะผ่านเข้ามาสู่ระบบภายในหรือไม่

ระบบการตรวจสอบดังกล่าวอาจจะใช้สมาร์ตการ์ด การตรวจสอบทางชีวภาพ (Biometrics) หรือซอฟต์แวร์ (3) เพื่อทำการตรวจสอบ ในกรณีของซอฟต์แวร์เทคนิคที่ใช้ในการตรวจสอบจะต้องมีความแอดว้านซ์เพื่อไม่ให้แอตแทกเกอร์สามารถแกะรอยได้ อาทิ การใช้รหัสผ่านเข้าสู่ระบบแบบใช้ได้ครั้งเดียว (One-time Passwords) (กล่าวคือ ครั้งถัดไปจะต้องใช้รหัสผ่านตัวใหม่เพื่อการเข้าสู่ระบบ) และควรจะหลีกเลี่ยงการใช้รหัสผ่านแบบคงที่ (Static Passwords)

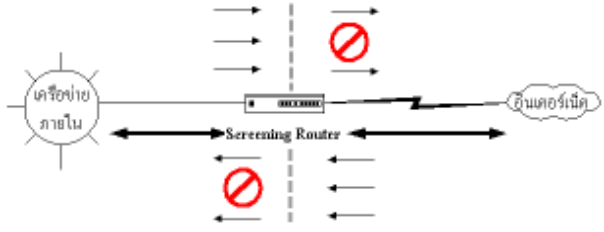
การใช้สมาร์ตการ์ดและการตรวจสอบทางชีวภาพเป็นวิธีการตรวจสอบที่ใช้เทคนิคแอดวานซ์ ดังนั้นโอกาสที่จะแกะรอยโดยแอตแทกเกอร์จึงแทบจะเป็นไปไม่ได้เลย

การสื่อสารที่มาจากอินเทอร์เน็ตและเข้าสู่ไฟร์วอลล์ขององค์กร เช่น TELNET และ FTP เป็นต้น เป็นการสื่อสารที่องค์กรควรจะให้ความสนใจเป็นพิเศษโดยการใช้วิธีการตรวจสอบการเข้าสู่ระบบแบบแอ็ดว้านซ์ณจุดไฟร์วอลล์ก่อนที่จะอนุญาตให้ทำการสื่อสารได้ การตรวจสอบโดยใช้รหัสผ่านแบบคงที่อาจก่อให้เกิดความเสียหายต่อองค์กรได้หากแอตแทกเกอร์สามารถทำการแกะรหัสผ่านนั้นได้สำเร็จ หรือคอยดักจับรหัสผ่านคงที่ที่วิ่งมาจากอินเทอร์เน็ตเพื่อเข้าสู่ไฟร์วอลล์ขององค์กรของเรา

## 3. ระบบกรองแพ็กเก็ต

ระบบกรองแพ็กเก็ตจะทำหน้าที่ตรวจสอบแพ็กเก็ต ทั้งที่เข้าและออกจากเครือข่ายขององค์กร ระบบกรองจะอนุญาตให้เฉพาะแพ็กเก็ตที่ได้กำหนดเอาไว้ในนโยบายเครือข่ายขององค์กรว่าแพ็กเก็ตดังกล่าวสามารถผ่านเข้าออกจากองค์กรได้ เป็นต้นว่านโยบายอาจจะระบุว่าอนุญาตให้ผู้ใช้จากภายนอกองค์กรทำการส่งมอบอีเมล์ได้ ดังนั้นแพ็กเก็ตของข้อความอีเมล์หนึ่งๆ ที่ส่งมาจากภายนอกจะสามารถผ่านเข้ามาสู่เครือข่ายภายในองค์กรของเราได้

ไฟร์วอลล์โดยทั่วไปจะมีระบบการกรองแพ็กเก็ตเป็นองค์ประกอบหนึ่งซึ่งเรียกกันว่า Screening Router รูปที่ 1 แสดง Screening Router ซึ่งทำหน้าที่อนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่านเข้าออกจากเครือข่ายขององค์กร เครื่องหมายห้าม ในรูปที่ 1 จะสะท้อนถึงว่ามีบางการสื่อสารที่ Screening Router จะไม่ยอมให้เข้าหรือออกจากองค์กร




***รูปที่ 1 แสดง Screening Router ที่ทำหน้าที่ตรวจสอบแพ็กเก็ต***

ในทุกๆ แพ็กเก็ตส่วนหัวของมันประกอบไปด้วยข้อมูลสำคัญซึ่งเป็นข้อมูลที่ Screening Router สามารถจะนำเอาไปใช้ประโยชน์ในการตัดสินใจว่าจะอนุญาตให้แพ็กเก็ตเหล่านั้นผ่านเข้าออกได้หรือไม่ ข้อมูลสำคัญดังกล่าว (2,3) ประกอบด้วย

1. IP Source Address หมายถึงแอดเดรสต้นทางไหนที่จะอนุญาตหรือไม่อนุญาตให้ทำการสื่อสารด้วย

2. IP Destination Address หมายถึงแอดเดรสปลายทางไหนที่จะอนุญาตหรือไม่อนุญาตให้ทำการสื่อสารด้วย

3. TCP/UDP Source Port หมายถึง พอร์ต[1] ต้นทางไหนที่จะอนุญาตหรือไม่อนุญาตให้ทำการสื่อสารด้วย

4. TCP/UDP Destination Port หมายถึงพอร์ตปลายทางไหนที่จะอนุญาตหรือไม่อนุญาตให้ทำการสื่อสารด้วย

เจ้าหน้าที่ดูแลเครือข่ายสามารถทำการเซ็ตเราเตอร์โดยกำหนดเป็นกฎเกณฑ์ต่างๆ ที่จะอนุญาตให้การสื่อสารระหว่างภายในและภายนอกองค์กรสามารถ

---

*[1]พอร์ต หมายถึง ช่องทางการสื่อสารซึ่งผู้พัฒนาซอฟต์แวร์ เช่น TELNET, FTP สามารถกำหนดได้ว่าจะให้ซอฟต์แวร์นั้นทำการติดต่อสื่อสารผ่านทางช่องทางการสื่อสารไหน เช่น ที่พอร์ต 23 เป็นต้น การกำหนดพอร์ตจะเป็นการระบุลงไปในตัวซอฟต์แวร์ที่ทำการพัฒนาขึ้นมานั้น*

กระทำได้หรือไม่ การเซ็ตเราเตอร์ สามารถอ้างถึงแอดเดรส (ในข้อ 1 และ 2 ข้างบน) และพอร์ตต่างๆ (ในข้อ 3 และ 4 ข้างบน) ตารางที่ 1 และ 2 ข้างล่างแสดงการเซ็ตเราเตอร์ เพื่อให้เห็นไอเดียการเซ็ตโดยสังเขป

| Action | Protocol | IP Source Address | IP Destination Address | Port No. |
|---|---|---|---|---|
| Deny | Tcp | * | 202.44.248.67 | 23 |

***ตารางที่ 1***

หมายถึง จำกัดสิทธิไม่ให้เครื่องใดๆ ก็ตามจากอินเทอร์เน็ตเข้าใช้บริการ TELNET ที่เครื่องที่มี IP แอดเดรส 202.44.248.67 บริการ TELNET โดยปกติจะใช้โพรโตคอล Tcp และใช้พอร์ตหมายเลข 23 ซึ่งเป็นมาตรฐานที่ยอมรับกันโดยทั่วไป

| Action | Protocol | IP Source Address | IP Destination Address | Port No. |
|---|---|---|---|---|
| Allow | Tcp | 201.45.248.10 | 202.44.248.67 | 23 |

***ตารางที่ 2***

หมายถึง อนุญาตให้เฉพาะเครื่องที่ใช้ IP แอดเดรส 201.45.248.10 จากอินเทอร์เน็ตสามารถเข้าใช้บริการ TELNET ได้ที่เครื่อง 202.44.248.67

## 4. Proxy Services

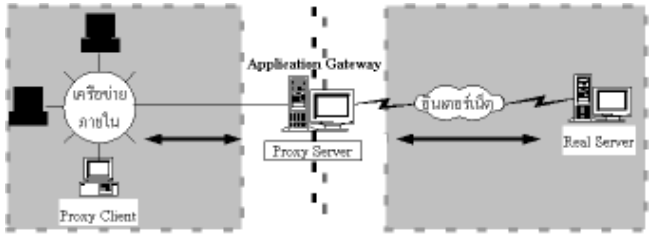
Proxy Service คือตัวซอฟต์แวร์ที่ทำงานอยู่บนไฟร์วอลล์ขององค์กรที่ทำหน้าที่รองรับความต้องการของผู้ใช้ในการขอใช้บริการบนอินเทอร์เน็ตต่างๆ เช่น บริการ FTP, บริการ TELNET เป็นต้น และทำการส่งต่อคำขอนั้นไปยังผู้ให้บริการนั้นๆ บนอินเทอร์เน็ต แต่ก่อนการส่งต่อ ตัวซอฟต์แวร์ที่เรียกกันสั้นๆ ว่า Proxy จะต้องทำการตรวจสอบก่อนว่าบริการดังกล่าวเป็นสิ่งที่ต้องห้ามหรือไม่ กล่าวคือ องค์กรมีนโยบายการใช้เครือข่ายให้กระทำได้หรือไม่ ดังนั้น Proxy อีกนัยหนึ่งก็คือซอฟต์แวร์ที่ทำหน้าที่เป็น “นายด่าน” ขององค์กรที่ควบคุมการสื่อสารบางประเภทที่เข้า-ออกจากองค์กร โดยปกติแล้วตัว Proxy ต่างๆ (ซึ่งเราอาจจะมีอยู่หลายตัว) จะทำงานอยู่บนเครื่องที่เราเรียกกันว่า Application Gateway ดังแสดงในรูปที่ 2

โดยทั่วไปแล้ว Proxy Service หนึ่งๆ จะทำงานโดยที่ผู้ใช้จะไม่รู้สึกว่าการสื่อสารที่เกิดขึ้นระหว่างภายใน (ผู้ใช้ขององค์กร) และภายนอกองค์กร (บริการบนอินเทอร์เน็ตต่างๆ)มีการติดต่อกันโดยผ่านทางนายด่าน (เพื่อทำการตรวจสอบการสื่อสารนั้น) ลักษณะของการทำงานดังกล่าวคือการเกิดสภาพ Transparency ซึ่งเป็นข้อดีของ Proxy ทั่วๆ ไป ดังนั้นจึงเกิดเป็นภาพเสมือนว่าผู้ใช้กำลังติดต่อกับอินเทอร์เน็ตเซิร์ฟเวอร์โดยตรง ในรูปที่ 2 ข้างล่างผู้ใช้ซึ่งอยู่ที่เครื่องที่มี Proxy Client กำลังติดต่อสื่อสารกับอินเทอร์เน็ตเซิร์ฟเวอร์ (หรือ Real Server ในรูป) ซึ่งอยู่ภายนอกองค์กร

Proxy Service หนึ่งๆ จำเป็นต้องมี 2 สิ่งนี้

1. Proxy Server และ
2. Proxy Client

เป็นองค์ประกอบพื้นฐานในการทำงานสถานภาพ ตัว Proxy Server จะทำงานอยู่บนเครื่อง Application Gateway ส่วน Proxy Client ก็คือ โปรแกรมที่ผู้ใช้ใช้งานและโดยปกติมักเป็นโปรแกรมที่ติดต่อกับอินเทอร์เน็ต เช่น โปรแกรม TELNET และโปรแกรม FTP เป็นต้น แต่เป็นโปรแกรมเวอร์ชันพิเศษที่จะทำการสื่อสารกับตัว Proxy Server แทนที่จะเป็นการสื่อสารโดยตรงกับ Server แท้ๆ (ในรูปคือ Real Server) ที่ให้บริการนั้นๆ อยู่บนอินเทอร์เน็ตภายนอกองค์กร (ให้ดูรูปที่ 2 ประกอบด้วย)




***รูปที่ 2 แสดงการทำงานของ Proxy โดยทั่วไปบนเครื่อง Application Gateway***

ตัว Proxy Server จะทำการตรวจสอบว่าคำขอจากผู้ใช้เพื่อขอใช้บริการบนอินเทอร์เน็ตหนึ่งๆ นั้นจะยอมให้กระทำได้หรือไม่ถ้าสามารถทำได้โดยสอดคล้องกับนโยบายเครือข่ายขององค์กร Proxy Server นั้นก็จะทำการติดต่อกับตัว Server แท้ที่ให้บริการนั้นใน

นามของผู้ใช้ และทำการส่งต่อการขอใช้บริการนั้นผ่านไปยังตัว Server แท้ อีกทั้งยังทำการผ่านกลับ Response ต่างๆ ที่มาจากตัว Server แท้กลับไปยังตัว Proxy Client

มีซอฟต์แวร์หลายตัวที่ออกมาและทำหน้าที่เป็น Proxy เช่น SOCKS ซึ่งเป็นทูลคิทที่ใช้ในการแปลงซอฟต์แวร์ประเภท Client/Server ไปสู่เวอร์ชันที่เป็น Proxy ของมันได้อย่างง่ายๆ ทูลคิทอีกตัวหนึ่งชื่อ Trusted Information Systems Internet Firewall Toolkit (TISFWTK) ทูลคิตตัวนี้จะรวมเอา Proxy Servers ที่สำคัญๆ หลายตัวอยู่ในตัวมันได้แก่ TELNET, FTP, HTTP, rlogin, X11 เป็นต้น

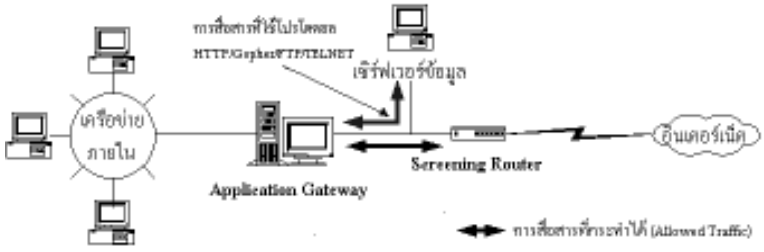
นอกจากนั้นแล้วในปัจจุบันซอฟต์แวร์ประเภทไคลเอนต์/เซิร์ฟเวอร์ ทั้งที่วางขายและให้ฟรีได้ออกมาพร้อมๆ กับเวอร์ชันที่เป็น Proxy ของมันหรือสามารถใช้ SOCKS เพื่อทำการแปลงให้เป็นเวอร์ชันที่เป็น Proxy ของมันได้

## สถาปัตยกรรมของไฟร์วอลล์

มีวิธีการในการออกแบบไฟร์วอลล์อยู่หลายวิธี สถาปัตยกรรมดังต่อไปนี้เป็นการออกแบบไฟร์วอลล์ที่สามารถพบเห็นกันได้บ่อยครั้งกับไฟร์วอลล์ของสำนักงานหรือองค์กรต่างๆ มีอยู่ 3 แบบ คือ สถาปัตยกรรมแบบ Dual-Homed Gateway สถาปัตยกรรมแบบ Screened Host และสถาปัตยกรรมแบบ Screened Subnet

### สถาปัตยกรรมแบบ Dual-Homed Gateway

สถาปัตยกรรมแบบนี้ หลักการสำคัญของมันก็คือบริการบนอินเทอร์เน็ตที่องค์กรจัดให้กับผู้ใช้ทั้งภายในและภายนอก เช่น TELNET, FTP เป็นต้น จะต้องมี Proxy ของบริการเหล่านั้นทำงานอยู่บนเครื่อง Application Gateway ดังนั้นการขอใช้บริการใดๆ ก็ตามจากอินเทอร์เน็ตโดยที่องค์กรไม่มี Proxy รองรับบริการตัวนั้น เครื่องเกตเวย์จะปฏิเสธที่จะให้บริการนั้นๆ และดังนั้นจะไม่มีการสื่อสารเกิดขึ้นดังรูปที่ 3




*รูปที่ 3 แสดงสถาปัตยกรรมแบบ Dual-Homed Gateway*

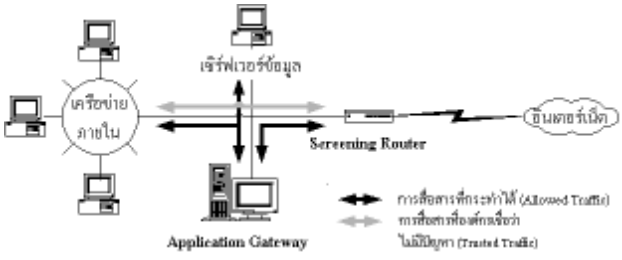
จากรูปที่ 3 การสื่อสารที่มาจากอินเทอร์เน็ตที่องค์กรอนุญาตให้กระทำได้และเป็นการสื่อสารที่ต้องการเข้าถึงข้อมูลที่องค์กรเปิดเผยจะถูกส่งต่อโดย Proxy ตัวหนึ่งที่ทำงานอยู่บนเครื่องเกตเวย์ไปยังเครื่อง "เซิร์ฟเวอร์ข้อมูล" (Information Server) ซึ่งอาจประกอบไปด้วยเซิร์ฟเวอร์สำหรับ TELNET, สำหรับ FTP, สำหรับ Gopher, สำหรับ HTTP เป็นต้น

วิธีการเซ็ตอัพไฟร์วอลล์แบบนี้ที่พบเห็นกันบ่อยๆ ก็คือจะมี Proxy สำหรับ TELNET และ FTP ทำงานอยู่บนเครื่องเกตเวย์และทำหน้าที่ส่งต่อการขอใช้บริการทั้งสองประเภทนี้ไปยังเครื่องเซิร์ฟเวอร์ข้อมูล รวมถึงการมีเซิร์ฟเวอร์อีเมล์ทำงานอยู่บนเครื่องเกตเวย์เพื่อทำหน้าที่รับและส่งอีเมล์ขององค์กร

ข้อด้อยของสถาปัตยกรรมแบบนี้คือบริการบนอินเทอร์เน็ตเฉพาะที่องค์กรมี Proxy ของมันเท่านั้น ผู้ใช้ภายในจึงจะสามารถใช้บริการนั้นๆ ได้ นั่นคือบริการบนอินเทอร์เน็ตอื่นๆ ผู้ใช้จะไม่สามารถขอรับบริการได้แม้ว่าจะมีความต้องการก็ตาม

### สถาปัตยกรรมแบบ Screened Host

สถาปัตยกรรมแบบ Screened Host ซึ่งมีความยืดหยุ่นมากกว่าสถาปัตยกรรมแบบ Dual-Homed Gateway แต่ความยืดหยุ่นที่ได้มานี้ก็ต้องแลกกับความปลอดภัยของเครือข่ายที่จะต้องลดลงไป สถาปัตยกรรมแบบนี้จึงเหมาะสมกับองค์กรที่ต้องการความยืดหยุ่นทางด้านการสื่อสารที่สูงขึ้น เช่น เปิดโอกาสให้การสื่อสารบางประเภทที่แม้ไม่มี Proxy ของมัน เราก็ยินยอมให้เกิดขึ้นได้ (ซึ่งตรงกันข้ามกับสถาปัตยกรรมแบบ Dual-Homed Gateway ที่การสื่อสารทุกประเภท (ทุกโพรโตคอล) จะต้องมี Proxy ของมันมาควบคู่อยู่ด้วยเสมอ) ดังรูปที่ 4




*รูปที่ 4 แสดงสถาปัตยกรรมแบบ Screened Host*

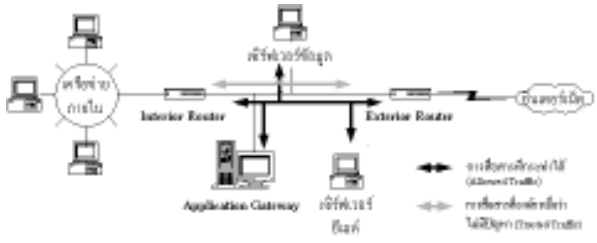
จากรูปที่ 4 จะเห็นได้ชัดว่าการสื่อสารเส้นสีเทาจะเป็นการสื่อสารแบบ (3)

- ที่ไม่มี Proxy เป็นตัวควบคุม หรือไม่ก็
- ที่อาจก่อให้เกิดอันตรายต่อเครือข่ายภายในแต่อันตรายที่อาจจะเกิดขึ้นนั้นอยู่ในระดับที่ไม่สูงนักและเป็นที่ยอมรับได้ เช่น ถ้าเครื่องใดเครื่องหนึ่งภายในองค์กรของเราต้องการข้อมูล DNS จากเครื่องที่ตั้งอยู่บนอินเทอร์เน็ต ก็สามารถที่จะทำการสื่อสารออกไปสู่เครื่องเหล่านั้นเพื่อขอข้อมูล DNS ได้

การวางเลย์เอาต์ของสถาปัตยกรรมแบบ Dual-Homed Gateway จะก่อให้เกิดเป็นเครือข่ายย่อย (Subnet) ซึ่งวางตัวอยู่ระหว่างเครื่องเกตเวย์และ Router (ให้ดูรูปที่ 3 ประกอบด้วย) และตัวเกตเวย์จะทำหน้าที่สกัดกั้นการสื่อสารที่ไม่มี Proxy (ซึ่งสามารถเทียบได้กับการสื่อสารเส้นสีเทาของScreened Host)ในขณะที่สถาปัตยกรรมแบบ Screened Host จะไม่มีตัวเกตเวย์มาคั่นกลาง (และดังนั้นจึงไม่มีเครือข่ายย่อยเกิดขึ้น) จึงทำให้สถาปัตยกรรมแบบหลังนี้มีความยืดหยุ่นมากกว่าในแง่ที่ว่าการสื่อสารบางประเภท (เส้นสีเทา) จะสามารถผ่านเข้ามาสู่เครื่องภายในองค์กรได้ ไม่ถูกสกัดกั้นโดยหลังเครื่องเกตเวย์ (ในกรณีของสถาปัตยกรรมแบบ Dual-Homed Gateway จะไม่มีการสื่อสารประเภทเส้นสีเทาปรากฏเลย)

## สถาปัตยกรรมแบบ Screened Subnet

สถาปัตยกรรมแบบ Screened Subnet ที่แสดงไว้ในรูปที่ 5 เป็นการผสานเอาจุดดีของสถาปัตยกรรมแบบ Dual-Homed Gateway และ Screened Host เข้ามาอยู่ในตัวมัน จุดดีของ Dual-Homed Gateway คือการมีเครือข่ายย่อยตั้งอยู่ระหว่างเราเตอร์ตัวนอก (Exterior) และตัวใน (Interior) ซึ่งสามารถป้องกันการบุกรุกเข้าสู่เครือข่ายภายในองค์กรได้ (จะได้อธิบายถึงเหตุผลข้างล่าง) จุดดีของ Screened Host คือ ความยืดหยุ่นในการให้บริการได้มากขึ้น เช่น บริการบางประเภทแม้ไม่มี Proxy เป็นตัวควบคุมองค์กรก็ยอมรับให้กระทำได้ถึงแม้จะมีความเสี่ยงอยู่บ้างก็ตาม




*รูปที่ 5 แสดงสถาปัตยกรรมแบบ Screened Subnet*

จากรูปที่ 5 สถาปัตยกรรมแบบนี้จะมีการกระจายงานให้แต่ละเครื่องที่อยู่ในบริเวณเครือข่ายย่อยซึ่งในรูปก็คือ เครื่องเซิร์ฟเวอร์ข้อมูล เครื่องเซิร์ฟเวอร์อีเมล์ และเครื่องเกตเวย์ ทำหน้าที่ของตัวมันเอง แทนที่จะไปยัดหน้าที่ต่างๆ เหล่านั้นไว้บนเครื่องเกตเวย์เพียงตัวเดียว (อย่างในกรณีของ Dual-Homed Gateway เครื่องเซิร์ฟเวอร์อีเมล์อาจทำงานอยู่บนเครื่องเกตเวย์นั้นที่อาจมี Proxy ตัวอื่นๆ อีกหลายตัวทำงานอยู่บนเครื่องเดียวกันนี้) การกระจายงานแยกไปตามเครื่องใครเครื่องมันทำให้เจ้าหน้าที่ดูแลระบบสามารถทำการคอนฟิกแต่ละเครื่องได้ง่ายยิ่งขึ้น และเมื่อพบปัญหาการบุกรุกทำให้สามารถวิเคราะห์หาสาเหตุได้ง่ายขึ้น

สาเหตุของความแกร่งยิ่งขึ้นของสถาปัตยกรรมแบบนี้เมื่อเทียบกับสถาปัตยกรรมแบบScreenedHost ก็คือในกรณีของ Screened Host หากตัว Router ถูกบุกรุกเข้ามา ทุกอย่างภายในเครือข่ายภายในองค์กร อันได้แก่ เครื่องและข้อมูลทั้งหมดที่มีอยู่มีสิทธิที่จะถูกเข้าถึงได้ทั้งหมด และในสายตาของแอตแทก-เกอร์แล้ว เมื่อเห็นว่าถ้าสามารถบุกผ่านเราเตอร์เข้ามาได้เพื่อเข้าไปหา “ทอง” ที่นั่น เขาก็จะใช้ความพยายามอย่างยิ่งที่จะพังเราเตอร์เข้ามาให้ได้ โดยการมีเครือข่ายย่อยแม้ว่าแอตแทกเกอร์สามารถฝ่าทะลุเราเตอร์เข้ามาได้ เขาก็ยังเข้าไปติดอยู่ในเครือข่ายย่อยและยังไม่สามารถผ่านทะลุเข้าไปสู่เครือข่ายภายในองค์กรได้ทันที

บางองค์กรยิ่งไปไกลกว่านั้น โดยการมีหลายๆ ชั้นของเครือข่ายย่อย กล่าวคือ ถ้าผ่านเข้าไปได้ชั้นหนึ่งแอตแทกเกอร์ก็ยังไปติดอยู่ที่เครื่องข่ายย่อยที่อยู่ชั้น

ในกว่านั้น จุดประสงค์หนึ่งของการสร้างเครือข่ายย่อยแบบหลายชั้นก็คือการมีบริการต่างๆ ที่องค์การต้องการให้วางไว้ตามชั้นต่างๆของเครือข่ายย่อย โดยชั้นนอกสุดของเครือข่ายย่อยจะมีบริการประเภทที่มีโอกาสที่จะถูกแฮ็กได้ง่ายหรือเปราะบางแต่องค์กรมักไม่แคร์ว่าจะถูกแฮ็กหรือไม่ ส่วนชั้นในๆ จะมีบริการประเภทที่เราต้องการให้มีความมั่นคงปลอดภัยสูงและมีโอกาสน้อยมากๆ ที่แอตแทกเกอร์จะบุกรุกเข้ามาถึงชั้นนี้ได้

คำอธิบายโดยพื้นฐานที่ว่าทำไมแอตแทกเกอร์จึงยังไม่สามารถบุกเข้าสู่เครือข่ายภายในองค์กรได้อย่างทันทีทันใด คือจากความจริงที่ว่าในขณะที่แอตแทกเกอร์กำลังอยู่ที่เครือข่ายย่อยระหว่างเราเตอร์ทั้งสอง เขาจะมองเห็นได้เฉพาะการสื่อสารการที่กำลังเกิดขึ้นในเครือข่ายย่อยนั้นเท่านั้น แต่จะมองไม่เห็นการสื่อสารทั้งหลายที่กำลังเกิดขึ้นภายในเครือข่ายภายในขององค์กร ความจริงที่ว่านี้เกิดจากในปัจจุบันเทคโนโลยีเครือข่ายที่เราใช้กันอยู่มีรากฐานอยู่บน Ethernet เทคโนโลยีตัวนี้ทำให้เรามองเห็นเฉพาะการสื่อสารที่กำลังเกิดขึ้นในวงเครือข่ายของเราเอง แต่จะมองไม่เห็นในวงเครือข่ายอื่นๆ (เทคโนโลยีแบบ Token Ring และ FDDI ก็มีลักษณะเช่นเดียวกันกับ Ethernet)

เมื่อแอตแทกเกอร์สามารถบุกเข้ามาถึงเครือข่ายย่อยได้ การแอบดักจับข้อมูลที่สำคัญๆ โดยแอตแทกเกอร์ก็จะสามารถกระทำได้ แต่โดยปกติแล้วข้อมูลที่มีการไหลเข้า-ออก ณ ที่บริเวณเครือข่ายย่อยนี้มักจะเป็นข้อมูลที่มีความสำคัญน้อยหรือไม่มีเลย ดังนั้นการแอบดักจับข้อมูลสำคัญของแอตแทกเกอร์จึงไม่เป็นผล แต่อย่างไรก็ตามการออกแบบไฟร์วอลล์ควรจะได้มีการคำนึงถึงประเภทของข้อมูลที่ไหลไปมาในเครือข่ายแต่ละชั้นขององค์กรด้วย

## จะซื้อไฟร์วอลล์ใหม่หรือสร้างเอง

(5) ได้กล่าวว่าปัจจุบันในท้องตลาดได้มีจำนวนผู้ขายไฟร์วอลล์มากกว่า 50 รายแล้ว ถึงแม้ว่าจะมีจำนวนผู้ขายอยู่มากมายบนท้องตลาดแต่การที่จะเลือกซื้อผลิตภัณฑ์ไฟร์วอลล์ตัวใดตัวหนึ่งมาเป็นกำแพงคุ้มครองป้องกันเครือข่ายขององค์กรยังเป็นเรื่องที่กระทำได้ไม่ง่ายนัก ทั้งนี้เพราะผลิตภัณฑ์แต่ละตัวที่ออกมาขายจะมีจุดดีจุดด้อยที่แตกต่างกันไป และดังนั้นการที่จะเลือกตัวใดตัวหนึ่งเพื่อให้สอดคล้องกับความต้องการทางด้านความมั่นคงปลอดภัยขององค์กร (Security Requirements) ซึ่งในแต่ละองค์กรจะมีความหลากหลายไม่เหมือนกัน จึงเป็นเรื่องที่ทำได้ไม่ง่ายนักและต้องพิจารณากันให้รอบคอบก่อนตัดสินใจ ในกรณีที่เมื่อพิจารณาแล้วและเห็นว่าไม่มีตัวใดตัวหนึ่งที่สอดคล้องกับความต้องการ องค์กรอาจพิจารณาทำการสร้างขึ้นมาใช้เอง

ประเด็นต่างๆ ข้างล่างนี้ (5) ไม่ว่าจะซื้อใหม่หรือสร้างเอง ควรจะได้รับการพิจารณาอย่างรอบคอบก่อนการตัดสินใจ

- ความยืดหยุ่น ผลิตภัณฑ์ไฟร์วอลล์หลายตัวไม่ยืดหยุ่นอย่างพอเพียงและดังนั้นไม่สามารถปรับให้สอดคล้องกับความต้องการเฉพาะขององค์กรได้ ในขณะที่ถ้าเราทำการสร้างขึ้นมาเองเราสามารถจัดหาซอฟต์แวร์ทูลต่างๆ (ซึ่งมีทั้งแจกฟรีและที่ต้องซื้อ) และฮาร์ดแวร์เพื่อมาประกอบรวมตัวกัน และสามารถทำงานอย่างสอดคล้องกับความต้องการทางด้านความมั่นคงปลอดภัยขององค์กรได้
- การจัดการและดูแลไฟร์วอลล์ ผลิตภัณฑ์ไฟร์วอลล์ในปัจจุบันได้รับการพัฒนาไปอย่างมากมาย ซึ่งรวมถึงการพัฒนา User Interface ให้มีความง่ายต่อการใช้งาน และดังนั้นทำให้สามารถจัดการและดูแลไฟร์วอลล์ได้อย่างง่ายดาย บางผลิตภัณฑ์ที่ออกมาช่วยให้ผู้ดูแลระบบสามารถจัดการและดูแลไฟร์-วอลล์โดยการล็อกอินผ่านทางเครือข่ายเข้ามา โดยปกติแล้วซอฟต์แวร์ทูลที่ใช้ในการสร้างไฟร์วอลล์ขึ้นมาใช้เองจะขาดในเรื่อง User Interface หรือความง่ายในการใช้งานเพื่อการจัดการและดูแลรักษาไฟร์วอลล์
- ค่าใช้จ่ายในการสร้างไฟร์วอลล์ขึ้นมาใช้เอง ซอฟต์แวร์ทูลหลายตัวที่แจกฟรีและมีปรากฏอยู่ใน Public Domain สามารถนำเอามาประกอบกันเป็นองค์ประกอบหนึ่งของไฟร์วอลล์ แต่อีกองค์ประกอบหนึ่งที่สำคัญและขาดไม่ได้ของไฟร์วอลล์คือฮาร์ดแวร์ การพิจารณาทางด้านค่าใช้จ่ายควรจะดูที่ค่าใช้จ่ายทั้งหมดทั้งซอฟต์แวร์และฮาร์ดแวร์รวมกันว่ามีมูลค่ามากน้อยเพียงไรเมื่อเปรียบเทียบกับการซื้อผลิตภัณฑ์ไฟร์วอลล์ใหม่มาหนึ่งตัว

นอกจากนั้นแล้วองค์กรยังต้องพิจารณาในเรื่องซอฟต์แวร์ทูลที่ให้ฟรีเหล่านั้นว่ายังมีบุคคลหรือหน่วยงานที่ให้การสนับสนุนในการแก้ไข bugs ในตัวซอฟต์แวร์เมื่อพบหรือไม่ รวมถึงแนวโน้มในอนาคต

ว่ายังมีการให้การสนับสนุนในการทำเวอร์ชันถัดๆ ไปของซอฟต์แวร์อยู่หรือไม่

- การให้การสนับสนุนผู้ขายไฟร์วอลล์หลายรายมักจะเสนอขายสินค้าในราคาเพิ่มขึ้นอีกประมาณ 20 เปอร์เซ็นต์ ซึ่งเป็นราคาของการให้ความช่วยเหลือทางด้านต่างๆ เช่น การอัปเกรดไฟร์วอลล์ สามารถขอความช่วยเหลือทางด้านเทคนิคต่างๆ สามารถโทรถามเมื่อพบปัญหาหรือเมื่อต้องการปรึกษาปัญหาต่างๆ เกี่ยวกับไฟร์วอลล์ เป็นต้น

ส่วนในกรณีของการสร้างขึ้นมาเองเจ้าหน้าที่ดูแลเครือข่ายจะต้องเป็นผู้มีหูตา กว้างไกล เช่น จะต้องรู้ว่าเมื่อเกิดปัญหากับไฟร์วอลล์ของตนจะสามารถหาที่ปรึกษาหรือผู้เชี่ยวชาญเรื่องไฟร์วอลล์ได้จากที่ไหน รวมทั้งจะสามารถติดต่อกับเจ้าของซอฟต์แวร์ไฟร์-วอลล์ฟรีตัวนั้นๆ ได้อย่างไร

## บทสรุป

จากรายละเอียดต่างๆที่ได้นำเสนอไปแล้วนั้นสรุปได้ว่าไฟร์วอลล์มีความสำคัญต่อบทบาทการรักษาความมั่นคงปลอดภัยของสารสนเทศขององค์กรที่มีการเชื่อมต่อกับอินเทอร์เน็ต การละเลยที่จะจัดหาและติดตั้งไฟร์วอลล์อาจจะนำผลเสียหายมาสู่องค์กร ซึ่งความสูญเสียที่เกิดขึ้นอาจจะเริ่มต้นจากเล็กน้อยไปจนกระทั่งมีมูลค่าสูง สถาปัตยกรรมต่างๆ ที่ได้นำเสนอไปแล้วข้างต้น เป็นแนวทางโดยพื้นฐานในการเลือกที่จะติดตั้งไฟร์วอลล์อย่างไรเพื่อให้มีความสอดคล้องและเหมาะสมกับความต้องการทางด้านความมั่นคงปลอดภัยขององค์กร และท้ายสุดการจะซื้อหรือจะสร้างไฟร์วอลล์ขึ้นมาใช้เองก็สุดแล้วแต่ผลการพิจารณาประเด็นต่างๆ ว่าน้ำหนักของการซื้อจะมากหรือน้อยกว่าน้ำหนักของการสร้างขึ้นมาเอง

### เอกสารอ้างอิง


*[1] Internet Firewalls Frequently Asked Questions, Marcus J. Ranum and Matt Curtin, http://www.clark.net/pub/mjr/pubs/index.shtml, May 1998*

*[2] Building Internet Firewalls, D. Brent Chapman and Elizabeth Zwicky, O'Reill , 1995*

*[3] Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, John P. Wack and Lisa J. Carnahan, NIST Special Publication 800-10, U.S DEPARTMENT OF COMMERCE, National Institute of Standards and Technology*

*[4] Internet Security Policy: A Technical Guide, Barbara Guttman and Robert Bagwill, September 1998*

*[5] Internet Security for Business, Terry Bernstein, Anish B. Bhimani, Eugene Schultz and Carol A. Siegel, John Wiley & Sons, Inc., 1996*

*[6] เปิดโลก TCP/IP และโปรโตคอลของอินเทอร์เน็ต, สุวัฒน์ ปุณณชัยยะ, ต้น ตันท์สุทธิวงศ์ และสุพจน์ ปุณณชัยยะ, Provision, 2543*

*[7] Computer Security for E-Commerce, ณรงค์ชัย นิมิตบุญอนันต์, SUM Publishing, 1999.*