Firewall

กล่าวนำ

ในบทที่ผ่านมา เราได้กล่าวถึงรายละเอียดวิธีการโจมตีทางเครือข่ายหลายวิธีการ สำหรับในบทนี้เราจะกล่าวถึงเครื่องมือหลักที่ถือได้ว่าเป็นทัพหน้าของเครื่องมือที่ใช้ในการป้องกันการโจมตีนั่นก็คือ ไฟร์วอลล์เพราะไฟร์วอลล์นับเป็นเครื่องมือแรกที่เกิดขึ้นมาในโลกของ Security เป็นเครื่องมือที่พัฒนาไปมากที่สุด เป็นที่รู้จักกันมากที่สุดและเป็นเครื่องมือตัวแรกที่มักจะใส่เข้าไปในระบบเพื่อป้องกัน เพราะหากไม่มีไฟร์วอลล์ทำหน้าที่ป้องกันไว้ชั้นหนึ่งแล้ว เครื่องมืออย่าง IDS (Intrusion Detection System) อาจต้องรับภาระหนักขึ้น หรือต้องกลายเป็นเป้าในการโจมตีซะเอง

Firewall เป็นอุปกรณ์หรือซอฟต์แวร์ที่ทำหน้าที่ในการคัดกรองข้อมูลภายในเครือข่าย โดยตรวจสอบเพ็กเก็ตที่วิ่งผ่านไปมาในเครือข่าย ซึ่งเป็นองค์ประกอบในระบบสารสนเทศที่ทำหน้าที่ในการสร้าง Access Control สำหรับแพ็กเก็ตต่างๆ ในระบบเครือข่าย ไฟร์วอลล์นั้นหากจะกล่าวในมุมกว้างก็อาจกล่าวได้ว่าเป็น Smart Router เพราะไฟร์วอลล์จะต้องทำหน้าที่เป็นเราเตอร์ โดยทำหน้าที่เป็นเกตเวย์ของเครือข่ายที่มันป้องกันอยู่ ปัจจุบันไฟร์วอลล์ได้รับการพัฒนาไปมากจนมีความสามารถพิเศษต่าง ๆ เพิ่มขึ้นมากมาย

ประเภทของไฟร์วอลล์ ซึ่งแบ่งออกเป็น 3 ประเภท ได้แก่

1) Packet Filtering
2) Stateful Inspection
3) Application Proxy

1. Packet Filtering Firewall

ไฟร์วอลล์ชนิดนี้ เป็นไฟร์วอลล์ที่มีรูปแบบการทำงานง่ายที่สุดและเป็นไฟร์วอลล์ที่เก่าแก่ที่สุด ปัจจุบันไฟร์วอลล์ประเภทนี้แทบไม่มีการนำไปใช้งานจริง ๆ แล้ว ที่ยังมีใช้งานอยู่มักจะเป็นฟังก์ชั่นหนึ่งของเราเตอร์โดยเราเตอร์ที่มีความสามารถนี้ นอกจากจะสามารถหาเส้นทางได้แล้ว ยังสามารถกรองแพ็กเกจได้อีกด้วยกล่าวคือสามารถจะอนุญาตหรือไม่อนุญาตให้แพ็กเกจผ่านเราเตอร์ได้ โดยการกำหนดเป็นกฎขึ้นมา เช่น

```
router(config)#access-list 11 deny 161.246.20.0 0.0.0.255
router(config)#access-list 11 permit any
router(config)#interface fastethernet1
router(config-if)#ip access-group 11 in
```

คำสั่งข้างต้นเป็นคำสั่งที่ใช้ในการตั้งค่าให้กับเราเตอร์ของ Cisco ดังนั้นหากเป็นเราเตอร์ยี่ห้ออื่นรูปแบบคำสั่งอาจต่างออกไป แต่หลักการของการตั้งค่าจะยังคงเป็นหลักการเดียวกัน สำหรับคำสั่งข้างต้นนั้นบรรทัดแรก

เป็นคำสั่งที่ใช้ในการกำหนด access-list หมายเลข 11 โดยกำหนดให้ปฏิเสธไอพีแอดเดรสหมายเลข161.246.20.0 โดยให้ปฏิเสธทั้ง Class C เลย คือ จะหมายถึงไอพีหมายเลขตั้งแต่ 161.246.20.1-161.246.20.255สำหรับบรรทัดถัดมาเป็นการกำหนดว่าจะตั้งค่าให้กับพอร์ต Fast Ethernet หมายเลข 1 และในบรรทัดสุดท้าย จะเป็นการกำหนดว่าให้นำ access-list ที่ได้กำหนดไว้ก่อนหน้านี้มาใช้กับพอร์ต Fast Ethernet 1 โดยให้ Filter เฉพาะฝั่ง inbound ซึ่งหมายถึง แพ็กเกจใด ๆ ที่มี Source IP Address อยู่ในช่วงดังกล่าวจะผ่านเราเตอร์นี้มาไม่ได้แต่ยังสามารถส่งออกไปได้ รูปแบบข้างต้นเรียกว่าเป็น *Standard ACL (Access Control List)* แต่เราเตอร์ของ Cisco ยังมี ACL อีกรูปแบบหนึ่ง คือ Extend ACL ดังตัวอย่างต่อไปนี้

```
router(config)#access-list 110 deny tcp host 161.246.4.3 smtp
router(config)#access-list 110 deny tcp host 161.246.4.3 ftp
router(config)#access-list 110 permit tcp host any any
router(config)#interface fastethernet1
router(config-if)#ip access-group 110 in
```

จากคำสั่งข้างต้น บรรทัดแรกเป็นคำสั่งกำหนด Extend ACL หมายเลข 110 โดยกำหนดให้ห้ามการเชื่อมต่อชนิด TCP ที่มีหมายเลข IP เป็น 161.246.4.3 และมีหมายเลขพอร์ตเป็นพอร์ตของ SMTP (25) และ TCP(23) โดยกำหนดให้มีผลกับพอร์ต Fast Ethernet 1 สำหรับการเชื่อมต่ออื่น ๆ สามารถผ่านได้ ซึ่งจะเห็นได้ว่าการกำหนด Extend ACL เราสามารถจะกำหนดลงไปยังหมายเลขพอร์ตได้ ว่าจะอนุญาตหรือไม่อนุญาตการเชื่อมต่อไปยังพอร์ตใด ๆ ได้ ซึ่งทำให้เราสามารถกำหนดได้ว่าจะให้แอดเดรสหรือช่วงแอดเดรสใด ติดต่อกับแอปพลิเคชันแบบใดได้ ซึ่งจะเห็นได้ว่า การกำหนดในแบบ Extend ACL นี้ มีประโยชน์อย่างมาก นอกจากนั้น ยังสามารถกำหนดกฎในลักษณะเช่นนี้ได้อีกด้วย

```
router(config)#access-list 110 permit host 161.246.5.10 gt 1024 host –161.246.4.7 eq 80
router(config)#access-list 110 deny tcp host any any
router(config)#interface fastethernet1
router(config-if)#ip access-group 110 in
```

คำสั่งข้างต้นเป็นคำสั่งที่ให้เครื่องคอมพิวเตอร์ 161.246.5.10 เท่านั้นที่สามารถติดต่อกับ Web Server ที่มีหมายเลขไอพี 161.246.4.7 สำหรับเครื่องอื่น ๆ จะติดต่อไม่ได้ ซึ่งจะเห็นว่าเราสามารถตั้งค่าให้กับเราเตอร์ได้ค่อนข้างหลากหลายเงื่อนไข นอกจากนั้นแล้ว คำสั่งที่เป็น Extend ACL นี้ ยังสามารถกำหนดในบล็อก ICMP เช่น

```
router(config)#access-list 110 deny icmp any any echo-request
router(config)#access-list 110 permit tcp host any any
router(config)#interface fastethernet1
```

```
router(config-if)#ip access-group 110 in
```

ในการกำหนด Access List นั้น หากจะกำหนดให้ครบถ้วน มักจะต้องมีการป้องกันแอดเดรสต่อไปนี้ด้วย คือ แอดเดรสที่ใช้งานเป็นหมายเลข Private IP Address ซึ่งได้แก่หมายเลขแอดเดรสที่มีหมายเลข 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255 และ 192.168.0.0-192.168.255.255 เอาไว้ด้วย เพราะเนื่องจากหมายเลขเหล่านี้เป็นหมายเลขที่ใช้งานภายใน ดังนั้นหากปรากฏเป็นหมายเลขของ Source IP Address แล้ว ก็หมายความว่าแพ็กเกจนั้นมีการปลอมหมายเลข Source IP Address มา นอกจากนั้น ก็ควรจะมีการ Filter หมายเลข IP Address ที่เป็นหมายเลขขององค์กรไว้ด้วย เพราะการติดต่อเข้ามายังองค์กรนั้น ย่อมจะต้องไม่มีหมายเลข Source IP Address เป็นหมายเลขภายในองค์กรแน่ ๆ เช่น หากภาควิชาฯ จะป้องกันตามรูปแบบข้างต้น ก็จะสามารถสร้าง ACL ได้เป็น

```
router(config)#access-list 11 deny 10.0.0.0 0.255.255.255
router(config)#access-list 11 deny 127.0.0.0 0.255.255.255
router(config)#access-list 11 deny 172.16.0.0 0.0.255.255
router(config)#access-list 11 deny 192.168.0.0 0.0.255.255
router(config)#access-list 11 deny 161.246.4.0 0.0.0.255
router(config)#access-list 11 deny 161.246.5.0 0.0.0.255
router(config)#access-list 11 deny 161.246.6.0 0.0.0.255
router(config)#access-list 11 deny 161.246.70.0 0.0.0.255
router(config)#access-list 11 permit any
router(config)#interface fastethernet1
router(config-if)#ip access-group 11 in
```

2) Stateful Inspection

ในไฟร์วอลล์แบบ Packet filtering ที่ได้กล่าวมานั้น จะเห็นได้ว่าเราสามารถตั้งค่าเพื่อกรองแพ็กเกจที่ไม่ต้องการออกไป แต่ไฟร์วอลล์ดังกล่าวก็ยังไม่ปลอดภัยมากพอ เพราะแม้ว่าเราสามารถจำกัดการเชื่อมต่อให้เหลือแต่พอร์ต 80 เท่านั้นที่ติดต่อเข้ามาได้ แต่ไฟร์วอลล์ข้างต้นก็ไม่ได้ตรวจสอบว่า การเชื่อมต่อผ่านพอร์ต 80 นั้นเป็นการเชื่อมต่อตามปกติหรือไม่ คือหากเป็นพอร์ต 80 แล้วก็จะปล่อยผ่านหมด ทั้งที่อาจเป็นแพ็กเกจโจมตีก็ได้เพราะแฮกเกอร์อาจเทลเน็ตไปยังพอร์ต 80 เพื่อรันโปรแกรม Backdoor ก็ได้ นอกจากนั้นกรณีที่แพ็กเกจที่ผ่านไฟร์วอลล์มาเป็นแพ็กเกจที่มีการทำ Fragmentation มาด้วยแล้ว ไฟร์วอลล์ประเภทนี้จะไม่สามารถตรวจสอบอะไรได้เลย (เราเตอร์บางตัวสามารถกำหนดให้ไม่ส่งผ่านแพ็กเกจแบบ Fragment ได้)

และหากเป็นกรณีที่เป็นการโจมตีโดยการกำหนดแพ็กเกจที่ผิดปกติแล้ว ไฟร์วอลล์แบบนี้ก็จะไม่สามารถตรวจสอบได้เช่นกัน เพราะหากหมายเลขไอพีผ่านและพอร์ตผ่าน ไฟร์วอลล์แบบ Packet filtering ก็ยอมให้ผ่านได้ทันที และหากมีการปลอมหมายเลขไอพีด้วยแล้ว ก็ยิ่งทำให้การป้องกันของไฟร์วอลล์มีความสามารถลดลง

นอกจากนั้นสำหรับพอร์ตที่มีหมายเลขมากกว่า 1024 ไฟร์วอลล์ดังกล่าวจะต้องเปิดพอร์ตเหล่านั้นไว้ตลอดเวลา เพราะไฟร์วอลล์ไม่รู้ว่าแอปพลิเคชันใดจะใช้งานพอร์ตหมายเลขใดบ้าง ซึ่งถือเป็นความไม่ปลอดภัยอีกเช่นกัน

ซึ่งข้อบกพร่องทั้งหมดนี้ ไฟร์วอลล์แบบ Stateful Inspection สามารถป้องกันได้ (ต่อไปจะเรียกว่าสเตทฟูล) โดยไฟร์วอลล์ ก็จะมีการตั้งกฎขึ้นมาเช่นเดียวกัน แต่ไฟร์วอลล์ประเภทนี้จะมีความสามารถในการติดตาม State ตามการเชื่อมต่อ โดยเฉพาะการเชื่อมต่อแบบ TCP ที่ได้อธิบายไปในบทก่อนหน้านี้ โดยในระหว่างการเชื่อมต่อไฟร์วอลล์จะทำการสร้าง State Table ที่จะเก็บสถานะของการเชื่อมต่อในทุกๆ การเชื่อมต่อเอาไว้ เช่น การเชื่อมต่อในแบบ TCP จะต้องเริ่มด้วย 3 Way Handshake ไฟร์วอลล์สเตทฟูลก็จะตรวจสอบว่าแพ็กเกจแรกเป็น SYN หรือไม่ และแพ็กเกจตอบกลับเป็น SYN/ACK หรือไม่ และแพ็กเกจยืนยันเป็น ACK หรือไม่ และแต่ละแพ็กเกจมีลำดับของ Sequence Number ถูกต้องหรือไม่ นอกจากในระหว่างการเชื่อมต่อไฟร์วอลล์สเตทฟูลยังมีการตรวจสอบหมายเลขลำดับ หมายเลขตอบรับและแฟล็กต่างๆ ตลอดเวลา ดังนั้นจะเห็นได้ว่าการสร้างแพ็กเกจแปลกปลอมให้ผ่านไฟร์วอลล์สเตทฟูลจะยากขึ้นมาก

สำหรับกรณีของแพ็กเกจที่มีการ Fragmentation มานั้น ไฟร์วอลล์สเตทฟูลจะรอจนครบทั้ง Datagram แล้วจึงทำการ Reassemble แล้วจึงตรวจสอบว่าถูกต้องหรือไม่ ดังนั้นการโจมตีโดยวิธีการแบ่งเป็น Fragment ย่อย ๆ เพื่อหลอกไฟร์วอลล์ก็จะทำได้ยากขึ้น และไฟร์วอลล์แบบสเตทฟูลไม่จำเป็นต้องเปิดพอร์ตหมายเลข1024 ขึ้นไปทิ้งเอาไว้ด้วย เพราะเมื่อไฟร์วอลล์สามารถติดตามสเตทได้แล้ว ก็ย่อมจะรู้ว่าการเชื่อมต่อ นั้นๆ ฝั่งไคลเอนต์มีการใช้งานพอร์ตใดก็จะเปิดพอร์ตนั้น “เฉพาะ” สำหรับไคลเอนต์นั้นและเมื่อการเชื่อมต่อจบลง ก็จะปิดพอร์ตนั้นไว้เหมือนเดิมทำให้ระบบมีความปลอดภัยเพิ่มขึ้นมาก

อย่างไรก็ตามไฟร์วอลล์แบบสเตทฟูลนั้น ไม่ได้ทำงานเหมือนกันไปหมด ไฟร์วอลล์สเตทฟูลบางตัวจะขยับไปทำงานที่ชั้นแอปพลิเคชันในบางโพรโตคอล เช่น ในโพรโตคอล FTP นั้นจะมีการใช้พอร์ต 2 พอร์ต คือพอร์ต 21 ใช้งานเป็นพอร์ตควบคุม และพอร์ต 20 เป็นพอร์ตข้อมูล ดังนั้นในการทำงานแบบสเตทฟูลนั้น สมมติว่าในครั้งแรกเครื่องไคลเอนต์ 161.246.5.10 ติดต่อมายังพอร์ต 21 ของเซิร์ฟเวอร์ 161.246.4.3 โดยจะสุ่มค่าพอร์ตฝั่งไคลเอนต์มาด้วย เช่น 1234 ซึ่งไฟร์วอลล์ก็จะกำหนดใน State Table ว่า ไอพี 161.246.4.3 พอร์ต 21 กับไอพี 161.246.5.10 พอร์ต 1234 มีการเชื่อมต่อกัน ไฟร์วอลล์ก็จะเปิดพอร์ตทั้ง 2 เอาไว้ แต่เมื่อมีการส่งข้อมูลเครื่องไคลเอนต์กลับติดต่อมายังพอร์ต 20 ซึ่งไฟล์วอลล์ที่ไม่เข้าใจการทำงานของโพรโตคอล FTP ก็จะบล็อกข้อมูล ทำให้ไม่สามารถเชื่อมต่อได้

หรือในการส่งข้อมูลประเภทมัลติมีเดีย เช่น H.323 นั้น พอร์ตควบคุมกับพอร์ตที่ใช้ในการส่งข้อมูล ก็จะเป็นคนละพอร์ตเช่นเดียวกับ FTP และบางครั้งยังเป็นการใช้พอร์ต UDP อีกด้วย ดังนั้นหากไฟร์วอลล์ไม่มีการทำงานในชั้นแอปพลิเคชั้น หรือไม่เข้าใจโพรโตคอลนั้นๆ แล้ว ก็จะใช้งานแอปพลิเคชันนั้นๆ ไม่ได้ หรือหากต้องการจะทำให้ได้ ก็จะต้องเปิดพอร์ตนั้นทิ้งเอาไว้ถาวร นอกจากนั้นในไฟร์วอลล์หลายตัว จะมีการติดตามสถานะการทำงานของ HTTP เป็นพิเศษ เพราะเป็นที่ทราบกันดีว่าข้อมูลในโลกนี้ มีบทบาทของ HTTP อยู่ไม่น้อย และมีการโจมตีผ่านทางเว็บมาก ดังนั้นการติดตามสถานะของ HTTP ก็จะทำให้ระบบเครือข่ายมีความปลอดภัยมากขึ้น

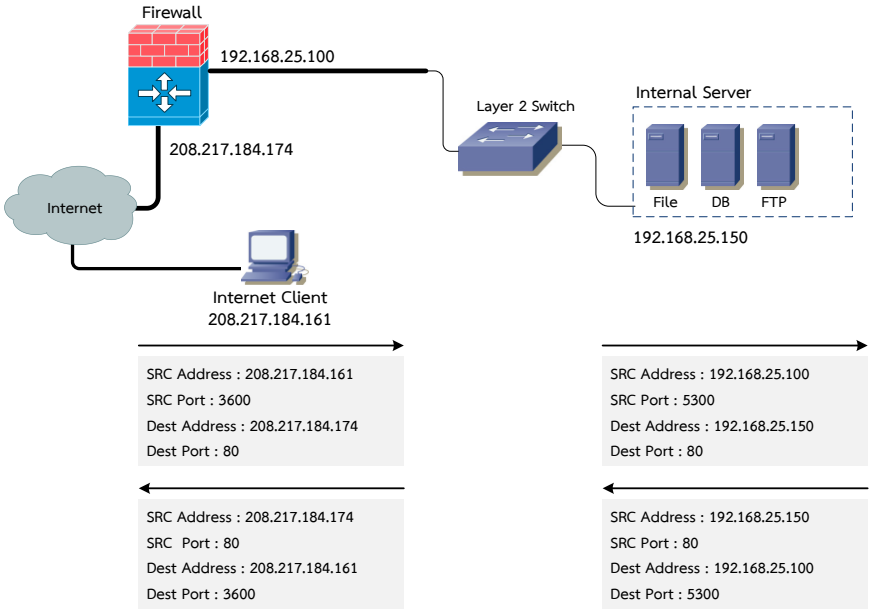
แต่แม้ว่าไฟร์วอลล์แบบสเตทฟูลจะมีความปลอดภัยเพิ่มขึ้นมากแล้วก็ตาม ไฟร์วอลล์ประเภทนี้ยังไม่สามารถป้องกันการโจมตีที่แทรกซึมมากับการเชื่อมต่อตามปกติได้ เช่น โพรโตคอล FTP นั้น แม้ว่าไฟร์วอลล์แบบสเตทฟูลจะมีการติดตามให้มีการเปิดพอร์ต 20 และ 21 อย่างถูกต้อง แต่หากมีการส่งข้อมูลอื่นๆ ที่ไม่ใช่ข้อมูล

FTP แทรกมาในระหว่างการเชื่อมต่อ ไฟร์วอลล์ประเภทนี้ก็จะไม่รู้ ดังนั้นหากต้องการให้ไฟร์วอลล์มีความสามารถในการติดตามการทำงานของชั้นแอปพลิเคชันมากขึ้น โดยทราบว่าการติดต่อเป็นการติดต่อตามรูปแบบของโพรโตคอลนั้นๆ อย่างถูกต้องหรือไม่ ไฟร์วอลล์นั้นจะต้องก้าวขึ้นไปทำงานในชั้นแอปพลิเคชันโดยจะเรียกไฟร์วอลล์ชนิดนี้ว่า Application Proxy Firewall

3) Application Proxy

ไฟร์วอลล์ประเภทนี้ จะทำงานในระดับชั้นแอปพลิเคชันเป็นสำคัญ โดยไฟร์วอลล์ประเภทนี้จะทำหน้าที่เป็นตัวแทน (Proxy) ในการส่งต่อ การเชื่อมต่อใดๆ ไปยังเซิร์ฟเวอร์ เช่น เมื่อไคลเอนต์ 161.246.5.10 ติดต่อไปยังเว็บเซิร์ฟเวอร์ 161.246.4.7 ผ่านทางไฟร์วอลล์ 161.246.5.1 ไฟร์วอลล์จะทำหน้าที่รับแพ็กเกจที่ขอเชื่อมต่อจาก 161.246.5.10 เอาไว้ จากนั้นก็ถอดแพ็กเกจเดิมออก แล้วสร้างแพ็กเกจใหม่ โดยอาศัยข้อมูลร้องขอเดิม ไปยัง 161.246.4.7 เสมือนกับว่าไฟร์วอลล์เป็นผู้ร้องขอเอง ดังนั้น ข้อดีประการแรกของไฟร์วอลล์ประเภทนี้คือ บุคคลภายนอกจะไม่รู้หมายเลขไอพีของเครือข่ายภายในที่ขอเชื่อมต่อออกมาภายนอก และเมื่อเว็บเซิร์ฟเวอร์ตอบกลับ มันก็จะส่งผลลัพธ์กลับไปยังเครื่อง 161.246.5.10

และโดยการที่มันทำหน้าที่เป็นตัวแทนในการเชื่อมต่อนี่เอง ทำให้การติดต่อผ่านไฟร์วอลล์ทุกครั้ง ไฟร์วอลล์ก็จะทำหน้าที่ในการตรวจสอบรูปแบบการติดต่อ ว่ามีรูปแบบที่ถูกต้องตามโพรโตคอลนั้นๆ หรือไม่ ทำให้มีความปลอดภัยเพิ่มขึ้น นอกจากนั้นไฟร์วอลล์แบบนี้ยังป้องกันการปลอมไอพีได้โดยเด็ดขาด เพราะมันจะทำหน้าที่ในการส่งต่อเสียเอง แต่การติดต่อแบบนี้ก็มีข้อเสียเช่นกัน โดยข้อเสียแรก คือ ไฟร์วอลล์แบบนี้จะทำงานได้ช้ากว่า เพราะมีการตรวจสอบมากกว่า และยังต้องสร้างแพ็กเกจใหม่ในทุกๆ ครั้งด้วย และหากกรณีที่ในการเชื่อมต่อหนึ่งมีการแบ่งเป็น Segment หลายๆ Segment ด้วยแล้ว ไฟร์วอลล์ประเภทนี้ต้องรอให้ทุก Segment ส่งมาจนครบก่อน จึงจะส่งต่อได้ทำให้เกิดความล่าช้าในการทำงานขึ้น



รูปตัวอย่าง Application Proxy Firewall

นอกจากนั้นการที่ไฟร์วอลล์ประเภทนี้ทำงานในระดับชั้นแอปริเคชัน หมายความว่า มันจะส่งต่อได้เฉพาะโพรโตคอลที่มันรู้จักเท่านั้น หากโพรโตคอลใดที่มันไม่รู้จัก ก็จะไม่สามารถส่งต่อได้เลย ในขณะที่หากเป็นไฟร์วอลล์แบบสเตลฟูลแล้ว เราสามารถตั้งค่าให้เปิดพอร์ตต่างๆทำให้สามารถเชื่อมต่อได้ แต่ไฟร์วอลล์แบบ Application Proxy จะไม่สามารถติดต่อได้เลย หากไฟร์วอลล์ไม่รู้จักกับโพรโตคอลนั้น

และจากข้อดีของไฟร์วอลล์แบบสเตทฟูล ที่มีความรวดเร็วในการทำงาน และข้อดีของไฟร์วอลล์แบบ Application Proxy ที่มีความปลอดภัยสูง จึงทำให้มีผู้สร้างไฟร์วอลล์ที่ผสมผสานความสามารถของไฟร์วอลล์ทั้งสองขึ้นและเรียกไฟร์วอลล์แบบใหม่นี้ว่า Hybrid Firewall หรือบางผู้ผลิตจะเรียกว่า Adaptive Firewall โดยไฟร์วอลล์แบบใหม่นี้ จะแตกต่างกันไปตามผู้ผลิต บางผลิตภัณฑ์ก็ทำงานในแบบ Proxy สำหรับโพรโตคอลหลักๆ และแบบสเตทฟูลสำหรับโพรโตคอลทั่วๆไป บางผลิตภัณฑ์ก็ทำงานในแบบ Proxy ในช่วงแรกของการเชื่อมต่อเพราะมีความปลอดภัยสูง และต่อมาหากเชื่อว่าการเชื่อมต่อนั้น เป็นการเชื่อมต่อตามปกติก็จะขยับลงมาทำงานในแบบสเตทฟูลเพราะมีความรวดเร็วในการทำงานมากกว่า

ไฟร์วอลล์ในปัจจุบันมีการพัฒนาไปมาก จนอาจกว่าได้ว่าไม่มีผลิตภัณฑ์ไฟร์วอลล์ใด ที่เป็นแบบใดแบบหนึ่ง นอกจากนั้นผลิตภัณฑ์ไฟร์วอลล์หลายๆตัวก็มักจะมีการทำงานร่วมกับแอปพลิเคชันด้านความปลอดภัยอื่น ๆ เช่น ทำงานร่วมกับ Antivirus ทำให้ไฟร์วอลล์ส่งข้อมูลของเมล์ไปตรวจสอบไวรัสก่อนจะส่งต่อหรือทำงานร่วมกับ IDS เพื่อตรวจสอบการบุกรุก ไฟร์วอลล์บางตัวสามารถตั้งให้ทำงานตามเวลา ตามผู้ใช้ บางตัวสามารถกำหนดทราฟฟิกให้กับแอปพลิเคชันไม่เท่ากันได้ด้วย ไฟร์วอลล์บางตัวสามารถล็อกการใช้งานของผู้ใช้ให้สามารถเชื่อมต่อกับไซต์ที่กำหนดไว้เท่านั้นได้

แนวทางการออกแบบ

เป้าหมายหลักของการออกแบบโครงสร้างความปลอดภัย ก็เพื่อที่จะปกป้องทรัพย์สินขององค์กร ให้สามารถใช้งานได้ โดยที่ไม่มีใครสามารถมาโจมตีได้ ซึ่งแนวทางในการออกแบบจะประกอบด้วย 4 ขั้นตอน คือ ออกแบบระบบ (Design) สร้างระบบ (Deploy) นำไปใช้งานใช้งาน (Manage) และประเมินผล (Assess) โดยขั้นตอนทั้ง 4 จะมีลักษณะเป็นงานที่ต่อเนื่องไปเรื่อยๆ ไม่รู้จบ ทั้งนี้เพราะการออกแบบระบบนั้นหลังจากนำไปใช้งาน อาจไม่เหมาะสมกับการใช้งาน เช่น อาจทำให้ระบบปลอดภัยจริง แต่ทำให้ผู้ใช้ไม่สะดวกต่อการใช้งาน อย่างนี้ก็ต้องปรับการออกแบบใหม่ หรืออาจสะดวกต่อการใช้งาน แต่เมื่อประเมินแล้ว มีความปลอดภัยไม่เพียงพอ ดังนั้นจึงต้องมีการปรับจนกว่าจะลงตัว นอกจากนั้นก็ยังจะต้องมีการตรวจประเมินเป็นระยะๆ ดังนั้นคงไม่ผิดนัก หากจะกล่าวว่า วงจรความปลอดภัยข้างต้นเป็นเรื่องที่ต้องทำไปเรื่อยๆ ตราบเท่าที่องค์กรนั้นยังคงอยู่

นอกจากนั้นการออกแบบนั้นควรจะต้องเป็นไปตาม Policy และแนวทางขององค์กร แต่หากองค์กรใดยังไม่มี Policy ก็จะต้องออกแบบและสร้างขึ้นก่อนที่จะสร้างโครงสร้างความปลอดภัย

- **การแบ่งเครือข่าย**

การแบ่งเครือข่าย หรือ Network Partition นี้ ถือเป็นขั้นตอนแรกของการออกแบบ โดยก่อนที่จะทำงานในขั้นตอนนี้กัน เราจะต้องมีผังของระบบคอมพิวเตอร์ และผังของระบบเครือข่ายขององค์กรก่อน สำหรับจุดประสงค์ของการแบ่งเครือข่ายนี้ ก็เพื่อจะจัดระดับความสำคัญของเครือข่ายในแต่ละส่วน ซึ่งโดยทั่วไปก็จะถือว่า

เครือข่ายที่เครื่องเซิร์ฟเวอร์อยู่ มีความสำคัญสูงที่สุด และเครือข่ายที่เครื่องไคลเอนต์อยู่ ก็มีความสำคัญรองลงมา โดยเครื่องของผู้บริหารอาจจะจัดให้มีความสำคัญมากกว่าเครื่องของพนักงานก็ว่ากันไป

คราวนี้เมื่อได้ระดับความสำคัญต่างๆ ของระบบเครือข่ายแล้ว ก็จะหาทางปกป้องเครือข่ายต่อไป โดยยึดหลักที่ว่าส่วนของเครือข่ายที่สำคัญมาก็ต้องปกป้องมาก ส่วนของเครือข่ายที่สำคัญน้อยก็ป้องน้อยหน่อย แต่โดยทั่วๆ ไปแล้ว จะแบ่งส่วนของเครือข่ายออกเป็น 3 ส่วนหลัก ๆ คือ ส่วนของเครือข่ายที่มีเซิร์ฟเวอร์ที่ไม่ได้ติดต่อกับภายนอกเป็นส่วนหนึ่ง ส่วนของเครือข่ายที่มีเซิร์ฟเวอร์ที่ต้องติดต่อกับภายนอกเป็นอีกส่วนหนึ่ง และอีกส่วนหนึ่งก็คือส่วนของผู้ใช้

สำหรับเหตุผลของการแบ่งเครือข่ายในส่วนของเซิร์ฟเวอร์ออกเป็น 2 ส่วน ก็เนื่องจากเซิร์ฟเวอร์ที่ทำหน้าที่ติดต่อกับภายนอก อย่างเช่น เว็บเซิร์ฟเวอร์ภายนอก หรือ เมล์เซิร์ฟเวอร์นั้น เป็นเซิร์ฟเวอร์ที่จะต้องติดต่อกับข้างนอก หรือเรียกว่า “เข้าถึงได้” จากภายนอก อย่างหลีกเลี่ยงไม่ได้ ซึ่งการป้องกันก็จะไม่สามารถทำได้อย่างเต็มที่ ประกอบกับการที่เซิร์ฟเวอร์เหล่านี้ เข้าถึงหรือเห็นได้จากภายนอก ทำให้มันกลายเป็นเป้าโจมตี และมีความเสี่ยงที่จะถูกเจาะเข้ามาได้ ในขณะที่เซิร์ฟเวอร์อย่างเซิร์ฟเวอร์ฐานข้อมูลนั้น ไม่จำเป็นต้องติดต่อกับภายนอก และไม่จำเป็นต้องให้ “เข้าถึงได้” จากภายนอก หรือพูดง่าย ๆ คือ ไม่ควรจะมองเห็นจากภายนอกเซิร์ฟเวอร์ในกลุ่มนี้จึงมีความเสี่ยงน้อยกว่า ดังนั้นหากนำเซิร์ฟเวอร์ 2 กลุ่มนี้ไปไว้ด้วยกันแล้ว เมื่อมีการเจาะเข้ามาได้จากเซิร์ฟเวอร์กลุ่มแรก ก็อาจจะสูญเสียเซิร์ฟเวอร์ทั้งหมด แต่หากมีการแบ่งเป็น 2 กลุ่ม เมื่อเซิร์ฟเวอร์กลุ่มแรกถูกเจาะเข้ามาได้ เซิร์ฟเวอร์ในกลุ่มที่ 2 ก็ยังจะมีความปลอดภัยต่อไป จนกว่าแฮกเกอร์จะเจาะเข้ามาในเซิร์ฟเวอร์กลุ่มหลังได้สำเร็จ ซึ่งจะเจาะได้ยากกว่ามาก เพราะการที่มันไม่ต้องติดต่อกับภายนอกทำให้เราสามารถป้องกันเครือข่ายส่วนนี้ได้อย่างเต็มที่มากกว่า

อย่างไรก็ตาม ในองค์กรที่มีขนาดไม่ใหญ่นัก อาจมีการแบ่งเครือข่ายออกเป็นเพียง 2 กลุ่ม คือจะรวมเอาส่วนของเครือข่ายที่เป็นเซิร์ฟเวอร์ภายในกับเครือข่ายของผู้ใช้เข้าด้วยกัน เพราะอันที่จริงเหตุผลที่เขาแยกส่วนของเครือข่ายผู้ใช้ออกจากส่วนของเครือข่ายเซิร์ฟเวอร์ภายในนั้น ก็เพราะไม่ไว้ใจผู้ใช้ภายในว่าอาจทำอันตราย

เซิร์ฟเวอร์ได้ แต่ในองค์กรขนาดเล็ก ที่สามารถไว้ใจผู้ใช้ได้ หรือสามารถควบคุมผู้ใช้โดยวิธีการอื่นได้ ก็อาจรวมเอาเครือข่าย 2 ส่วนนี้เข้าด้วยกันได้ เพื่อเป็นการประหยัดค่าใช้จ่าย

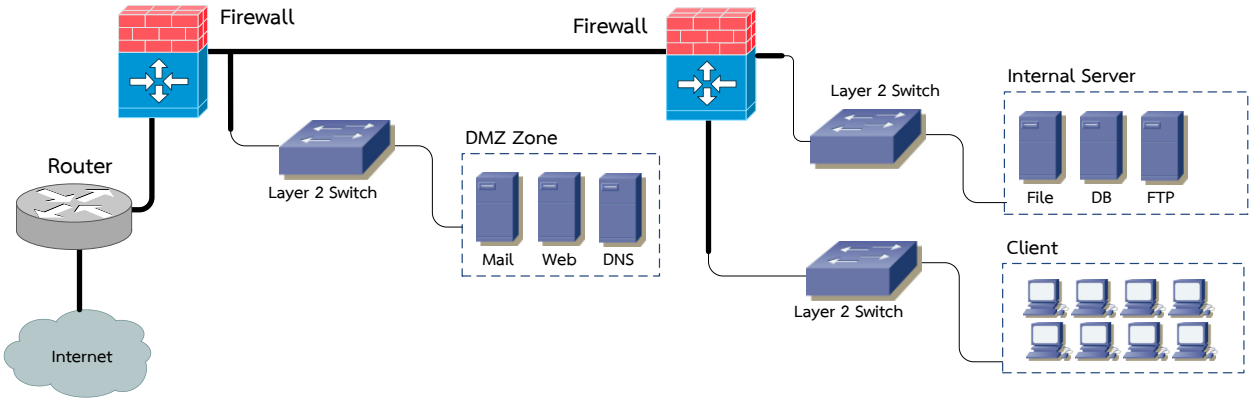
รูปแสดงการแบ่งเครื่องคอมพิวเตอร์ในเครือข่ายออกเป็น 3 ส่วน

หลังจากที่เราแบ่งเครือข่ายแล้ว จะมีศัพท์อยู่คำหนึ่งที่มักพูดถึงกันในวงการรักษาความปลอดภัย นั่นก็คือ ศัพท์คำว่า Trust ซึ่งภาษาไทย ก็น่าจะแปลว่าความเชื่อถือ คำนี้มีความหมายว่าเราจะเชื่อถือเครื่องคอมพิวเตอร์เครื่องนั้นได้มากน้อยเพียงใดว่าในระหว่างที่ติดต่อกันนั้นจะไม่เป็นอันตรายต่อเรา ซึ่งโดยทั่วไปก็มักจะให้คอมพิวเตอร์กลุ่มที่ 2 มีความน่าเชื่อถือสูงที่สุด เพราะดูแลโดยผู้ดูแลระบบเอง จากนั้นก็ตามมาด้วยคอมพิวเตอร์ในกลุ่มที่ 1 หรือกลุ่มที่ 3 ขึ้นอยู่กับว่าองค์กรนั้นเป็นลักษณะใด อย่างองค์กรของผมเป็นสถานศึกษาผมก็จะเชื่อว่าคอมพิวเตอร์กลุ่มที่ 1 น่าเชื่อถือกว่า เพราะถึงแม้จะมีความเสี่ยงอันเนื่องมาจากการต้องติดต่อกับภายนอก แต่ก็ยังเป็นเครื่องที่ดูแลเอง แต่ผมไม่สามารถเชื่อในตัวนักศึกษาได้เลยว่าจะไม่พยายามทำอันตรายต่อองค์กร ทั้งนี้เพราะนักศึกษามักจะมีนิสัยชอบทดลอง แต่หากเป็นองค์กรที่ผู้ใช้ค่อนข้างจะธรรมดาไม่ค่อยมีคนเก่งคอมพิวเตอร์ ก็อาจวางใจได้ว่า ผู้ใช้ไม่มีศักยภาพพอที่จะทำอันตรายต่อระบบในองค์กรได้ ในกรณีก็อาจเชื่อคอมพิวเตอร์ในกลุ่มที่ 3 มากกว่า สำหรับเครือข่ายที่ไม่น่าเชื่อถือเลย ก็คือเครือข่ายภายนอกองค์กร

- **การแบ่งเครือข่ายโดยใช้ไฟร์วอลล์**

เมื่อเราจัดกลุ่มเครื่องคอมพิวเตอร์เรียบร้อย พร้อมทั้งจัดอันดับความน่าเชื่อถือแล้ว เราก็จะมาหาทางแบ่งกลุ่มคอมพิวเตอร์เหล่านั้นออกจากกัน โดยเป้าหมายของการแบ่งก็คือ ให้เครือข่ายส่วนต่างๆ สามารถติดต่อใช้งานกันได้ตามปกติ แต่ไม่อนุญาตให้การใช้งานที่ผิดปกติผ่านเข้าไปได้ ซึ่งตรงนี้เราจะต้องกำหนดกฎการเข้าออก (Rule) โดยกฎที่กำหนดนี้ก็จะเป็นแนวทางที่ตั้งร่วมกันว่าจะอนุญาตหรือไม่อนุญาตการสื่อสารประเภทใดบ้าง ที่ข้ามระหว่างเครือข่ายแต่ละส่วนที่ได้แบ่งออกจากกัน

สำหรับการนำไฟร์วอลล์มาใช้ ก็จะนำมาตั้งในตำแหน่งที่แบ่งเครือข่ายแต่ละส่วนออกจากกัน อย่างเครือข่ายตัวอย่างของผม ซึ่งแบ่งออกเป็น 3 ส่วน ก็สามารถออกแบบได้ 2 วิธี โดยวิธีแรกจะใช้ไฟร์วอลล์ 2 ตัวโดยไฟร์วอลล์ตัวแรก จะทำหน้าที่กั้นระหว่างเครือข่ายภายนอกกับองค์กร และไฟร์วอลล์ตัวที่ 2 จะทำหน้าที่กั้นระหว่างเครือข่ายกลุ่มที่ 1 กลุ่มที่ 2 และกลุ่มที่ 3 โดยจะได้โครงสร้างตามรูปที่ 36 วิธีการออกแบบลักษณะนี้จะเรียกว่า Screening Subnet หรือบางทีก็เรียกว่า Three Homed Computer



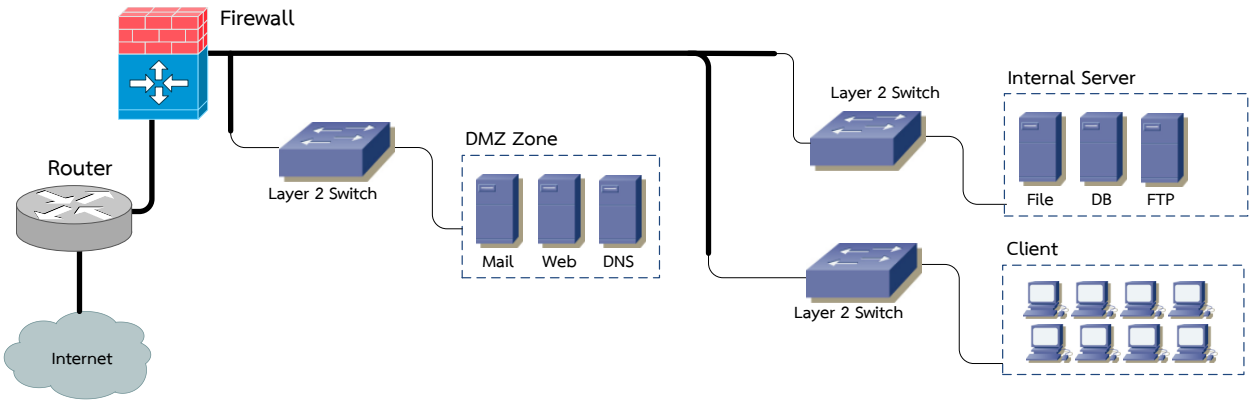
รูปแสดงการแบ่งเครือข่ายด้วยไฟร์วอลล์ 2 ตัว

สำหรับเหตุผลของการออกแบบข้างต้นนั้น ไฟร์วอลล์ตัวแรกนั้นคงไม่มีปัญหาอะไร คือ เห็นได้ชัดเจนว่าทำหน้าที่ในการกั้นระหว่างเครือข่ายที่เชื่อถือไม่ได้เลย คือเครือข่ายอินเตอร์เน็ตกับเครือข่ายภายในองค์กรสำหรับไฟล์วอลล์ตัวที่ 2 นั้นจะมี 3 ขา โดยจะทำหน้าที่กั้นระหว่างเครือข่ายภายในทั้ง 3 โดยเครือข่ายกลุ่มที่ 1 ที่ต้องเชื่อมต่อกับอินเตอร์เน็ตนั้น จะอยู่นอกสุด คือ มีไฟร์วอลล์กั้นเพียงตัวเดียว เครือข่ายส่วนนี้จะมีชื่อเรียกอีกอย่างว่า DMZ หรือ De-Militarize Zone ซึ่งหากจะแปลก็น่าจะแปลได้ว่า เขตปลอดทหาร ทั้งนี้ก็เนื่องจากว่าส่วนนี้จะเสมือนกับเป็นเขตชายแดน หรือเขตกันชนระหว่างเครือข่ายอินเตอร์เน็ตกับเครือข่ายภายใน ซึ่งจะมีการควบคุมเข้มงวดน้อยกว่าส่วนของเครือข่ายภายใน

เขต DMZ นี้เป็นเขตที่เราถือว่าเป็นเขตที่มีความปลอดภัยน้อย เพราะการตั้งกฎที่ไฟร์วอลล์ตัวนอก จะไม่สามารถตั้งอย่างเข้มงวดได้ เนื่องจากต้องติดต่อกับเครือข่ายอินเตอร์เน็ต ประกอบกับเป็นเครือข่ายที่คนข้างนอกสามารถมองเห็น และสามารถเป็นเป้าของการโจมตีได้ ซึ่งหากผู้ดูแลระบบดูแลระบบไม่ดีพอ หากเจอกับแฮกเกอร์ที่เก่ง ๆ ก็อาจทำให้สูญเสียเซิร์ฟเวอร์ตัวใดตัวหนึ่งไปได้

สำหรับเขตที่อยู่ภายในเครือข่ายถัดมา จะเป็นเครือข่ายที่ปลอดภัยมากกว่า เพราะมีไฟร์วอลล์กั้นอยู่อีกชั้นหนึ่ง และเครือข่ายส่วนนี้จะใช้กฎที่เข้มงวดมากกว่า จนกระทั่งไม่สามารถมองเห็นได้จากภายนอก เพราะหากคนในองค์กรจะส่งเมล์ ก็จะติดต่อกับเมล์เซิร์ฟเวอร์ใน DMZ หรือหากคนในองค์กรต้องการเล่นเว็บก็ต้องผ่านทาง Web Proxy ที่อยู่ใน DMZ เช่นเดียวกัน หรือแม้กระทั่งใน DMZ เองก็ยังไม่สามารถมองเห็นเครือข่ายภายในได้ตลอดเวลา โดยจะเห็นเฉพาะที่มีการเชื่อมต่อเท่านั้น ซึ่งตรงนี้จะอธิบายอีกครั้งในเรื่องชนิดของไฟร์วอลล์ ดังนั้นเครือข่ายภายในจะมีความปลอดภัยสูงมาก

นอกจากนั้นไฟร์วอลล์ตัวในก็ยังทำหน้าที่ในการกั้นระหว่างเครือข่ายของผู้ใช้กับเครือข่ายของเซิร์ฟเวอร์ภายใน ซึ่งจะทำให้เครือข่ายของเซิร์ฟเวอร์มีความปลอดภัยจากการกระทำของผู้ใช้มากขึ้น เพราะได้มีการสำรวจพบในอเมริกาว่ามากกว่าครึ่งของความไม่ปลอดภัย มักเกิดจากคนในมากกว่าคนนอก แต่นั่นก็เป็นสภาพแวดล้อมในอเมริกา สภาพแวดล้อมในประเทศไทยก็อาจต่างออกไปได้ บางองค์กรที่ผู้ใช้ค่อนข้างจะรู้คอมพิวเตอร์มาก ก็อาจจะออกแบบอย่างในรูปข้างต้น แต่ในบางองค์กรที่ผู้ใช้สามารถเชื่อใจได้ หรือองค์กรที่ผู้ใช้ไม่มีความรู้ด้านคอมพิวเตอร์มากนัก ก็อาจจะรวมเอาเครือข่ายผู้ใช้กับเครือข่ายของเซิร์ฟเวอร์ภายในเข้าด้วยกันได้ ซึ่งจะเป็นผลให้สามารถลดไฟร์วอลล์ลงได้ 1 ตัว โดยจะได้เครือข่ายที่มีรูปแบบตามรูปที่ดังนี้



รูปแสดงการแบ่งเครือข่ายด้วยไฟล์วอลล์เพียงตัวเดียว

อย่างไรก็ตามในการกั้นระหว่างเครือข่ายของเซิร์ฟเวอร์ภายในกับผู้ใช้นั้น ตามในรูปที่ 2 นั้น ในการนำไปใช้งานจริง จะค่อนข้างมีความยุ่งยากอยู่บ้าง ทั้งนี้เพราะการสื่อสารระหว่างผู้ใช้กับเซิร์ฟเวอร์ภายในบางครั้งก็มีความซับซ้อน โดยเฉพาะกับองค์กรที่ใช้ไมโครซอฟต์วินโดว์ และใช้งานในระบบของโดเมน ทั้งนี้เพราะในการสื่อสารระหว่างเครื่องที่เป็นสมาชิกของโดเมน และเครื่องโดเมนคอนโทรลเลอร์นั้น จะมีการติดต่อที่ซับซ้อน ผ่านทางพอร์ตหลายพอร์ต ดังนั้นในการใช้งานอาจมีปัญหาในเรื่องของการติดต่อกันไม่ได้เกิดขึ้นได้อย่างไรก็ตามหากมีการปรับแต่งกฎของไฟร์วอลล์ให้เหมาะสมแล้ว ก็ยังสามารถใช้งานในรูปแบบนี้ได้

จะเห็นว่าเครือข่ายจะแบ่งออกเป็นเพียง 3 ส่วน คือ เครือข่ายภายนอกองค์กร เครือข่าย DMZ และเครือข่ายภายในองค์กร ซึ่งรวมเอาเซิร์ฟเวอร์ภายในและเครื่องไคลเอนต์เข้าไว้ด้วยกัน รูปแบบนี้จัดว่าเป็นรูปแบบที่ประหยัด เพราะใช้ไฟร์วอลล์เพียงตัวเดียว แม้จะมีความเสี่ยงมากกว่าแบบที่ใช้ไฟร์วอลล์ 2 ตัวก็ตามแต่หากเลือกใช้ไฟร์วอลล์ที่ดีหน่อย และมีการดูแลรักษาอย่างเคร่งครัด และถือได้ว่ามีความปลอดภัยที่เทียบเท่าได้กับไฟร์วอลล์ 2 ตัวเลยทีเดียว วิธีการออกแบบนี้จะเรียกว่า Screening Router หรือ Dual Homed Computer

และในทำนองเดียวกัน หากต้องการความปลอดภัยมากขึ้นไปอีก ก็สามารถทำได้ โดยการเพิ่มไฟร์วอลล์ขึ้นอีกตัวหนึ่ง เพื่อกั้นระหว่างเครือข่ายภายในและเครือข่ายของเซิร์ฟเวอร์ภายในองค์กร ซึ่งก็จะกลายเป็นไฟร์วอลล์ 3 ชั้น ซึ่งบางคนอาจจะบอกว่า โอเวอร์ไปหรือเปล่า ก็ต้องขอตอบว่าในเรื่องของความปลอดภัยแล้ว ไม่มีคำว่า โอเวอร์ เพราะยิ่งเราป้องกันมากขึ้น ความปลอดภัยก็ยิ่งเพิ่มมากขึ้น แต่ก็ต้องแลกกับค่าใช้จ่ายที่ต้องเสียเพิ่มขึ้นด้วย บางองค์กรมีการใช้ไฟร์วอลล์ตั้ง 7-8 ชั้นก็ยังมีเลย เพราะเขาต้องการความมั่นใจจนถึงที่สุดว่าเครือข่ายของเขาจะปลอดภัยมากที่สุดเท่าที่จะทำได้ ไม่ว่าจะเสียค่าใช้จ่ายมากแค่ไหนก็ตาม อย่างเช่น ธุรกิจธนาคารที่มีมูลค่าธุรกิจนับแสนล้านบาทเป็นเดิมพันนี่คงเรียกว่าโอเวอร์ไม่ได้เหมือนกัน

สำหรับความแตกต่างของการมีไฟร์วอลล์มากชั้น กับไฟร์วอลล์น้อยชั้นนั้น จะไม่แตกต่างกันในแง่ของความปลอดภัย หากไฟร์วอลล์ไม่ถูกเจาะซะเอง แต่หากเมื่อไรก็ตามที่ไฟร์วอลล์ถูกเจาะสำเร็จแล้ว ไฟร์วอลล์ที่มีจำนวนชั้นมากกว่า ก็จะมีความปลอดภัยมากกว่าอย่างแน่นอน เพราะอย่างน้อยแฮกเกอร์ก็จะต้องเสียเวลาเจาะไฟร์วอลล์ตัวถัดไปเพิ่มขึ้น ทั้งนี้แม้ว่าไฟร์วอลล์จะเป็นซอฟต์แวร์เพื่อความปลอดภัย ที่ตัวมันเองจะต้องมีความปลอดภัยสูง ซึ่งที่ผ่านมาไฟร์วอลล์แต่ละยี่ห้อก็รักษาชื่อเสียงด้านนี้ได้เป็นอย่างดี

แต่อย่างไรเสียไฟร์วอลล์ก็เป็นซอฟต์แวร์ตัวหนึ่ง ที่อาจจะมีข้อบกพร่องหรือจุดโหว่ได้เช่นเดียวกันแม้ว่าจะมีน้อยกว่า เพราะมีการตรวจสอบกันอย่างเข้มงวดมาก จนถึงปัจจุบันก็อาจกล่าวได้ว่าไฟร์วอลล์ชื่อดังส่วนใหญ่ ล้วนแต่เคยมีการรายงานข้อผิดพลาดมาแล้วทั้งสิ้น แม้แต่ไฟร์วอลล์ที่ถือว่าเป็นอันดับหนึ่งอย่าง Firewall-1 ก็ยังเคยมีการรายงานข้อผิดพลาด เพราะนานๆ ทีจึงจะมีเหตุการณ์แบบนี้เกิดขึ้น และเมื่อเกิดขึ้นทางผู้ผลิตก็แก้ไขกันอย่างรวดเร็วอยู่แล้ว ดังนั้นหากเราดูแลระบบดี ๆแล้วเราก็ยังสามารถเชื่อถือในไฟร์วอลล์ได้เต็มร้อย

ดังนั้นเมื่อมีจำนวนชั้นของไฟร์วอลล์มากกว่าก็จะปลอดภัยมากกว่า และในบางองค์กรมีการออกแบบให้ใช้ไฟร์วอลล์ต่างยี่ห้อกันในแต่ละชั้นของไฟร์วอลล์ด้วยแล้ว ก็ยิ่งเป็นการยากเข้าไปอีกที่จะสามารถเจาะทะลุไฟร์วอลล์หลายๆ ยี่ห้อเข้าไปได้

ที่กล่าวมาทั้งหมดนั้น เป็นการกล่าวในแง่ของความปลอดภัยจากการโจมตี แต่ไม่ได้กล่าวในแง่ของระบบที่ไม่ล้มเหลวที่ภาษาอังกฤษเรียกว่า High Availability เพราะเครื่องคอมพิวเตอร์ที่รันโปรแกรมไฟร์วอลล์ก็เป็นคอมพิวเตอร์เครื่องหนึ่ง ที่แม้จะเป็นยี่ห้อที่น่าเชื่อถือสักเท่าใด มีราคาสูงสักเท่าใด คอมพิวเตอร์เครื่องนั้นก็สามารถ

ล้มเหลวได้ แม้จะเป็นเปอร์เซ็นต์ที่น้อยก็ตาม ดังนั้นหากต้องการความมั่นคงของไฟร์วอลล์ ให้มากขึ้นก็ต้องเพิ่มไฟร์วอลล์เข้าไปอีกให้ทำงานขนานกัน ซึ่งจะมีชื่อเรียกไฟร์วอลล์แบบนี้ว่า Load-Balanced Firewall ซึ่งแน่นอนว่าจะทำให้ราคาของระบบสูงขึ้นไปอีก

- **การเลือกใช้ไฟร์วอลล์**

หลังจากที่เราได้ออกแบบโครงสร้างที่แบ่งเครือข่ายออกเป็นส่วนๆ เรียบร้อยแล้ว คราวนี้เราจะมาพิจารณาแนวทางการเลือกใช้ไฟร์วอลล์กัน เพื่อจะได้จัดหาไฟร์วอลล์ที่เหมาะสมมาใช้กับองค์กร ไฟร์วอลล์นั้นสามารถแบ่งเป็นประเภทได้หลายอย่าง โดยอาจแบ่งตามรูปแบบเป็น 2 แบบ คือ แบบที่เป็นฮาร์ดแวร์ และแบบที่เป็นซอฟต์แวร์

ไฟร์วอลล์แบบที่เป็นฮาร์ดแวร์นั้น อันที่จริงแล้วก็เป็นแบบซอฟต์แวร์นั่นแหละ เพียงแต่ตอนที่เขาขายนั้นเขาขายมาพร้อมกับฮาร์ดแวร์ โดยซอฟต์แวร์ของไฟร์วอลล์แบบนี้จะสร้างขึ้นมาเพื่อให้ทำงานกับฮาร์ดแวร์นั้นๆ โดยเฉพาะ ดังนั้นการทำงานระหว่างซอฟต์แวร์และฮาร์ดแวร์ก็จะเข้ากันได้เป็นอย่างดี และมีความปลอดภัยมากกว่า เพราะซอฟต์แวร์ของไฟร์วอลล์แบบนี้ จะไม่ได้ทำงานอยู่บนระบบปฏิบัติการทั่วไป แต่จะรันอยู่บนระบบปฏิบัติการที่เขียนขึ้นมาเฉพาะ โดยบางบริษัทจะพัฒนาขึ้นมาใหม่ทั้งหมด แต่บางบริษัทก็นำระบบปฏิบัติการประเภทยูนิกซ์มาดัดแปลง ซึ่งทำให้การหาข้อมูลเกี่ยวกับฮาร์ดแวร์และระบบปฏิบัติการเหล่านั้นทำได้ยากขึ้น ทำให้การเจาะเข้าไปในไฟร์วอลล์ประเภทนี้ยากขึ้นไปด้วย

ไฟร์วอลล์อีกประเภทหนึ่ง คือ ไฟร์วอลล์ที่มีลักษณะเป็นซอฟต์แวร์อย่างเดียว โดยไฟร์วอลล์แบบนี้จะทำงานอยู่บนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ และระบบปฏิบัติการทั่วไป โดยอาจมีการเข้าไปแก้ไขส่วนประกอบของระบบปฏิบัติการบางส่วน โดยเฉพาะส่วนที่ทำหน้าที่ติดต่อกับเครือข่าย ทั้งนี้เพื่อให้ไฟร์วอลล์สามารถควบคุมการสื่อสารได้โดยตรง และช่วยให้คอมพิวเตอร์ที่รันโปรแกรมไฟร์วอลล์มีความแข็งแกร่งมากขึ้น ดังนั้นเครื่องคอมพิวเตอร์ที่จะใช้ทำเป็นไฟร์วอลล์จึงควรจะใช้เป็นไฟร์วอลล์เพียงอย่างเดียว ไม่ควรให้ทำหน้าที่อื่นร่วมด้วย เพราะมักจะมีปัญหาเกิดขึ้นเสมอ หากให้เครื่องคอมพิวเตอร์ที่ใช้เป็นไฟร์วอลล์ ทำหน้าที่ให้บริการอย่างอื่นด้วย

สำหรับแนวทางการเลือกระหว่างไฟร์วอลล์ประเภทซอฟต์แวร์กับฮาร์ดแวร์นั้น ไฟร์วอลล์ประเภทซอฟต์แวร์จะมีข้อดีที่มีความยืดหยุ่นในการใช้งานมากกว่า กล่าวคือ เนื่องจากทำงานบนเครื่องคอมพิวเตอร์ จึงมีการติดต่อผู้ใช้เป็นแบบกราฟิก และเนื่องจากเป็นซอฟต์แวร์ ดังนั้นจึงสามารถเลือกเครื่องคอมพิวเตอร์ที่จะติดตั้งให้เหมาะสมกับประสิทธิภาพที่ต้องการได้ เช่น หากเครือข่ายมีความเร็วไม่มากนัก ก็อาจจะใช้เครื่องสเปกทั่วไปได้ แต่หากเครือข่ายมีความเร็วสูง ก็อาจจะหาเครื่องประสิทธิภาพสูงๆ มาใช้แทนได้ เครื่องเดิมก็สามารถนำไปใช้งานอย่างอื่นต่อไป แต่ไฟร์วอลล์แบบฮาร์ดแวร์จะทำไม่ได้ แต่สิ่งที่คุณจะได้จากไฟร์วอลล์แบบฮาร์ดแวร์คือ ความปลอดภัยที่สูงกว่า จากเหตุผลที่ได้กล่าวไปแล้ว และอีกประการหนึ่ง คือ ค่าใช้จ่าย เพราะไฟร์วอลล์ประเภทฮาร์ดแวร์มีแนวโน้มที่จะมีราคาสูงกว่า

ในระบบที่ออกแบบ จะเลือกไฟร์วอลล์ประเภท Stateful Inspection แล้วจะออกแบบเงื่อนไขการทำงานไว้แบบนี้ครับ คือ สำหรับไฟร์วอลล์ตัวนอก จะเปิดเฉพาะพอร์ตที่มีการใช้งาน ซึ่งในที่นี้ก็จะมีเพียงเมล์และเว็บเท่านั้น ดังนั้นนอกเหนือจากช่องทางทั้งสองแล้วแฮกเกอร์ก็จะโจมตีระบบไม่ได้เลย หากไม่โจมตีไฟร์วอลล์เสียก่อน เพราะไฟร์วอลล์จะช่วยป้องกันเอาไว้ สำหรับไฟร์วอลล์ตัวใน ผมก็จะยิ่งตั้งเงื่อนไขให้เข้มงวดอีกว่าการติดต่อระหว่างไคลเอนต์ภายในเพื่อใช้งานเว็บ หรือ ใช้งานเมล์ จะต้องเริ่มการติดต่อจากข้างในมาข้างนอกเท่านั้น ซึ่งด้วย

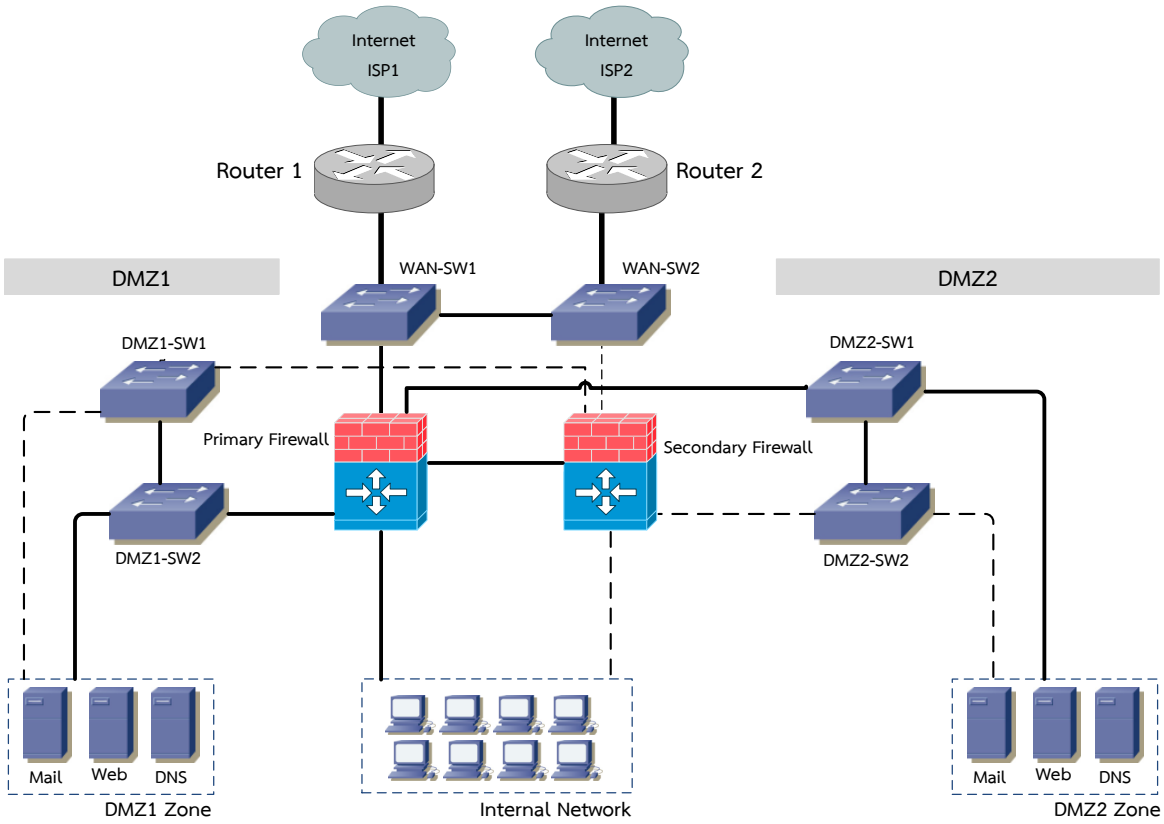
ความที่เป็นไฟร์วอลล์ประเภท Stateful Inspection มันจะเสมือนกับเป็นการปิดพอร์ตทั้งหมดจากภายนอก และจะเปิดใช้งานบางพอร์ตเฉพาะระหว่างการติดต่อเท่านั้น ดังนั้นการโจมตีเข้ามาข้างในก็จะสามารถทำได้เฉพาะเวลาที่ติดต่อกับข้างนอกเท่านั้น และจะโจมตีได้เฉพาะเครื่องที่กำลังติดต่อเท่านั้นด้วย ดังนั้นจะเห็นได้ว่าจะปลอดภัยมาก

สำหรับไฟร์วอลลที่มีจำหน่ายในปัจจุบันนั้น ได้พัฒนาก้าวหน้าไปมาก มีฟังก์ชันต่างๆ เพิ่มขึ้นมากมายและส่วนใหญ่จะไม่ได้เป็นประเภทใดประเภทหนึ่งซะทีเดียว แต่จะเป็นแบบผสมผสาน โดยไฟล์วอลล์ที่จัดว่าเป็นแบบ Stateful ได้แก่ Firewall-1 ของ Checkpoint, Symactec Enterprise Firewall (Raptor) ของ Symantec, Bulletproof ของ CA, PIX Firewall ของ Cisco และ ISA Server ของไมโครซอฟต์ ไฟล์วอลล์ที่จัดว่าเป็น Application Proxy จริงๆ ก็น่าจะเป็น Gaunlet ของบริษัท Network Associate

นอกเหนือจากที่ได้กล่าวมา ก็ควรจะพิจารณาความสามารถอื่นๆ ของไฟร์วอลล์ประกอบด้วย เช่น บางยี่ห้อมีการทำงานในระดับ User ด้วย คือ ผู้ใช้แต่ละคนจะผ่านไฟร์วอลล์ได้ไม่เท่ากัน บางยี่ห้อสามารถกระจาย Policy ไปยังไฟร์วอลล์ตัวอื่นๆ ได้ บางยี่ห้อสามารถทำงานกับแอปพลิเคชันอื่นได้ เช่น ทำงานร่วมกับโปรแกรมแอนตี้ไวรัสในการตรวจสอบไวรัสบนเมล์หรือเว็บ หรือทำงานร่วมกับโปรแกรมตรวจจับการบุกรุกได้ บางยี่ห้อสามารถตั้งปฏิทินการทำงานให้ใช้กฎ ที่ต่างกันในแต่ละช่วงเวลาได้ บางยี่ห้อมีการเพิ่มส่วนตรวจสอบเว็บ (Content Filter) เพื่อกรองข้อมูลที่ผ่านเว็บเป็นพิเศษ และอื่น ๆ อีกมากมาย

<u>ตัวอย่างการออกแบบ</u>

รูปแสดงตัวอย่างเครือข่ายเป็นการออกแบบ High Available Firewall โดยการใช้ไฟร์วอลล์ 2 ตัวทำหน้าที่กั้นระหว่างเครือข่าย โดยไฟร์วอลล์ 2 ตัวนี้จะทำงานแบบ Load Balancing คือ ใช้ Virtual IP เดียวกัน แบ่งภาระการทำงานโดยหากเป็นไมโครซอฟต์จะเรียกการเชื่อมต่อระหว่างเซิร์ฟเวอร์ 2 ตัวนี้ว่า Heartbeat โดยจะคอยตรวจสอบการทำงานของไฟร์วอลล์ทั้ง 2 หากมีตัวใดตัวหนึ่งผิดปกติ จะทำการ Failover ทันที ระบบนี้จะเหมาะสำหรับองค์กรที่ต้องการความต่อเนื่องของการให้บริการสูง



รูปแสดง ตัวอย่างเครือข่าย

ไฟร์วอลล์สำหรับ Host

ไฟร์วอลล์สำหรับนี้ เรามักได้ยินคำว่า Personal Firewall มากกว่า โดยไฟร์วอลล์ประเภทนี้จะทำหน้าที่ป้องกันเฉพาะคอมพิวเตอร์เครื่องใดเครื่องหนึ่งมากกว่าจะป้องกันเครือข่าย ผลิตภัณฑ์เหล่านี้ส่วนใหญ่มักออกแบบมาเพื่อใช้กับระบบปฏิบัติการในตระกูลวินโดว์ เพราะเป็นระบบปฏิบัติการที่มีการใช้งานเป็นไคลเอนต์มากที่สุด ผลิตภัณฑ์เหล่านี้มักมีราคาถูก และบางตัวก็ให้ดาวน์โหลดได้ฟรี นอกจากนั้นบางตัวยังมีความสามารถด้าน IDS แบบง่าย ๆ อีกด้วย โปรแกรมเหล่านี้แม้ว่าจะทำให้การใช้งานคอมพิวเตอร์มีความยุ่งยากมากขึ้น แต่ก็มีประโยชน์เพราะสามารถตรวจสอบได้ว่ามีการสแกนเข้ามาในเครื่องของเรา หรือมีความ พยายามแฮกเข้ามาในเครื่องของเราหรือไม่ นอกจากนั้นผลิตภัณฑ์เหล่านี้ ส่วนใหญ่มีการใช้งานง่าย สามารถเพิ่มกฎเข้าไปได้เอง โดยไม่จำเป็นต้องมีความรู้มากนัก ตัวอย่างของโปรแกรมเหล่านี้ได้แก่

- Zone Alarm
- Tiny Personal Firewall
- Norton Personal Firewall
- Sygate Personal Firewall
- Conseal PC Firewall
- VPN-1 Secure Client

และนอกเหนือจากโปรแกรมที่กล่าวมาข้างต้นแล้ว ยังมีโปรแกรมที่ทำหน้าที่ป้องกันเซิร์ฟเวอร์ด้วย เช่น โปรแกรม IP Filter, SunScreen Lite Firewall, Firewall-1 Secure Server และ Packet Filtering via IPSec in Windows 2000

บทสรุป

Firewall นั้นเป็นเครื่องมือหนึ่งสำหรับช่วยในการบังคับใช้นโยบายการรักษาความปลอดภัย ดังนั้นในการออกแบบ Firewall นั้นควรจะให้มีความสอดคล้องกับนโยบายการรักษาความปลอดภัยที่มีอยู่ มิฉะนั้นผลที่จะเกิดขึ้นคือความปลอดภัยของเครือข่ายในทางปฏิบัติจะไม่เป็นไปตามจุดประสงค์ของนโยบายการรักษาความปลอดภัยที่จัดตั้งขึ้นได้