บทที่ 2

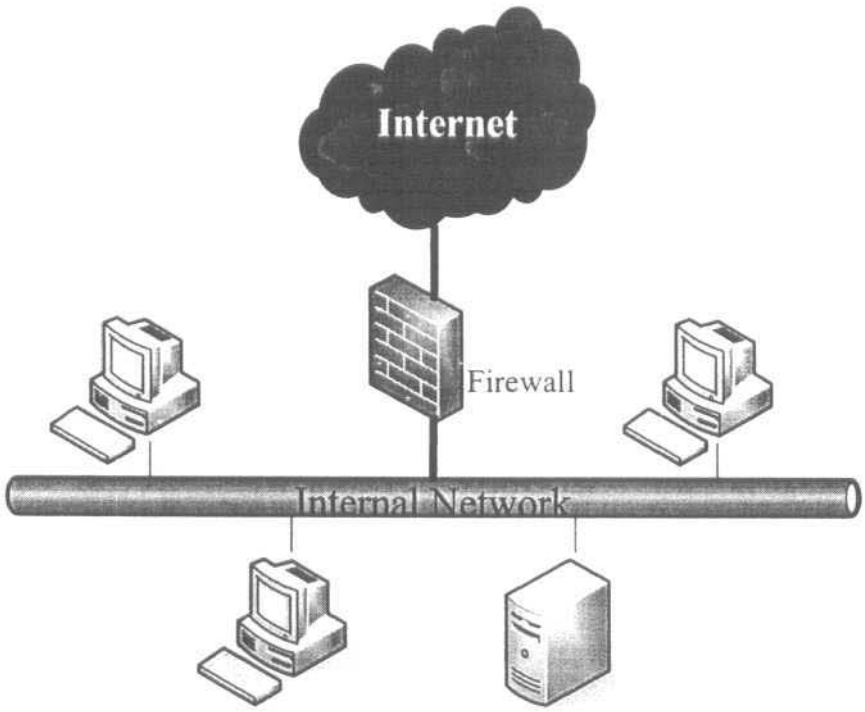
ความรู้พื้นฐานเกี่ยวกับไฟร์วอลล์

2.1 บทนำ

ทุกวันนี้แทบจะไม่มีคอมพิวเตอร์เครื่องใดที่ตั้งอยู่โดยลำพังจริงๆ ถ้าไม่มีการเชื่อมต่อกับเครือข่าย หรือไม่มีระบบเครือข่ายเฉพาะที่ (LAN) ก็ยังมักจะมีการเชื่อมต่อกับอินเทอร์เน็ต ทำให้มีโอกาสที่จะสื่อสารแลกเปลี่ยนข้อมูลกับคอมพิวเตอร์อื่นๆ อีกนับร้อยล้านเครื่องทั่วโลก แต่ในขณะเดียวกันก็เป็นการเปิดโอกาสให้อีกนับร้อยล้านเครื่องเหล่านั้น ซึ่งเราไม่เคยรู้จักมาก่อน สามารถส่งข้อมูล โปรแกรม ไวรัส คอมพิวเตอร์ รวมทั้งสิ่งอื่นๆ อีกมากมายมาหาเราได้ หรืออาจจะพยายามเจาะข้อมูลสำคัญจากเครื่องของเรา หรือพยายามขโมยข้อมูล หรือสร้างสิ่งรบกวนให้กับเราได้ซึ่งก่อให้เกิดปัญหาด้านความมั่นคงของระบบคอมพิวเตอร์มากขึ้นทุกที

จากปัญหาดังกล่าวทำให้เราต้องมีวิธีการในการรักษาความมั่นคง สิ่งที่สามารถช่วยลดความเสี่ยงนี้ได้ก็คือ ไฟร์วอลล์ โดยไฟร์วอลล์นั้นจะทำหน้าที่ป้องกันอันตรายในหลายๆ รูปแบบ จากการบุกรุกภายนอกที่จะเข้ามายังเครือข่ายของเรา การก่อกวนจากภายใน และอื่นๆ

หากจะเข้าใจได้ง่ายที่สุดไฟร์วอลล์ก็คือเครื่องมือที่ใช้ป้องกันเครือข่ายจากการสื่อสารทั่วไปที่ไม่ได้รับอนุญาต ส่วนความหมายทางด้านคอมพิวเตอร์ ไฟร์วอลล์ (Firewall) หมายถึงส่วนประกอบหรือกลุ่มของส่วนประกอบที่ทำหน้าที่ควบคุมการเข้าถึงระหว่างเครือข่ายภายนอกหรือเครือข่ายที่เราคิดว่าไม่ปลอดภัย กับ เครือข่ายภายใน หรือเครือข่ายที่เราต้องการจะป้องกัน โดยที่กลุ่มของส่วนประกอบนั้นอาจเป็น อุปกรณ์จัดเส้นทาง (Router) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) หรือเครือข่ายที่ประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือสถาปัตยกรรมไฟร์วอลล์ (Firewall Architecture) ที่ใช้ การควบคุมการเข้าถึงของไฟร์วอลล์นั้น สามารถทำได้ในหลายระดับและหลายรูปแบบขึ้นอยู่ชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น เราสามารถกำหนดได้ว่าจะให้มีการเข้ามาใช้บริการอะไรได้บ้าง จากที่ไหน เป็นต้น



ภาพที่ 2.1 ไฟร์วอลล์กั้นระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน

2.2 คุณสมบัติทั่วไปของไฟร์วอลล์

ไฟร์วอลล์เป็นเครื่องมือรักษาความมั่นคงที่ทำงานในเชิงป้องกัน (Protect) ซึ่งจะทำหน้าที่ควบคุมการเข้าถึงเครือข่าย (Access Control) โดยอาศัยกฎเป็นพื้นฐาน (Rule Base) สำหรับคุณสมบัติแต่ละอย่างของไฟร์วอลล์นั้นมีรายละเอียดดังนี้

2.2.1 Protect : ไฟร์วอลล์เป็นเครื่องมือที่ใช้ทำงานในเชิงป้องกัน โดยกลุ่มข้อมูลที่สามารถผ่านเข้า-ออกเครือข่ายได้นั้น จะต้องเป็นกลุ่มข้อมูลที่ไฟร์วอลล์เห็นว่ามีความปลอดภัย กลุ่มข้อมูลใดที่ไฟร์วอลล์เห็นว่าไม่ปลอดภัย หรืออาจจะนำมาซึ่งความไม่ปลอดภัยก็จะถูกทิ้ง (Drop) ไปไม่ส่งต่อ โดยการที่ไฟร์วอลล์จะตัดสินใจว่ากลุ่มข้อมูลใดปลอดภัย และกลุ่มข้อมูลใดไม่ปลอดภัยนั้นจะอยู่บนพื้นฐานของกฎที่ผู้ดูแลไฟร์วอลล์ (Firewall Administrator) เป็นผู้กำหนดไว้ล่วงหน้า ซึ่งเงื่อนไขของกฎเหล่านี้เองทำให้ไฟร์วอลล์สามารถป้องกันกลุ่มข้อมูลที่อาจจะส่งผลร้ายไม่ให้ผ่านเข้าไปถึงเครือข่ายได้

2.2.2 Access Control : "การเข้าถึง" (Access) หมายถึงการที่โฮสต์ (Host) ใดโฮสต์หนึ่งสามารถสื่อสารข้อมูลที่ต้องการไปยังโฮสต์ปลายทางได้สำเร็จ การเข้าถึงในแต่ละระดับจะมีวิธีการแตกต่างกันออกไป ทำให้การควบคุมการเข้าถึงสำหรับแต่ละระดับแตกต่างกันตามไปด้วย ไฟร์วอลล์จึงมีการทำงานหลายลักษณะตามวิธีที่ไฟร์วอลล์ใช้ควบคุมการเข้าถึง

2.2.3 Rule Base : ไฟร์วอลล์จะควบคุมการเข้าถึงโดยอาศัยการเปรียบเทียบคุณสมบัติของกลุ่มข้อมูลที่จะผ่านไฟร์วอลล์กับกฎของการเข้าถึงที่ได้กำหนดไว้ หากพบว่าไม่มีกฎที่ห้ามไว้ก็จะอนุญาตให้กลุ่มข้อมูลนั้นผ่านไปได้ หากมีกฎที่ห้ามไว้กลุ่มข้อมูลนั้นก็จะถูกสกัดกั้นไว้ด้วยวิธีใดวิธีหนึ่ง

ดังนั้นการที่กลุ่มข้อมูลใดๆ สามารถผ่านเข้า-ออกไฟร์วอลล์ได้หรือไม่นั้นจึงอยู่ที่กฎเป็นสำคัญ สำหรับไฟร์วอลล์โดยตัวเองแล้วนั้นจะไม่มีทางทราบได้ว่ากลุ่มข้อมูลใดเป็นกลุ่มข้อมูลที่ปลอดภัย หรือกลุ่มข้อมูลใดเป็นกลุ่มข้อมูลที่ไม่ปลอดภัย (ยกเว้นกลุ่มข้อมูลที่เป็นอันตรายโดยตัวมันเองอยู่แล้ว เช่น กลุ่มข้อมูลต่างไปจากปกติ (Anomalous Packet) ที่ใช้สำหรับการโจมตีโดยเฉพาะ) ไฟร์วอลล์จะรู้จักเฉพาะกลุ่มข้อมูลที่ได้รับอนุญาต และกลุ่มข้อมูลที่ไม่ได้รับอนุญาตตามกฎที่ระบุไว้เท่านั้น นั่นหมายความว่ากลุ่มข้อมูลที่ใช้เพื่อจุดประสงค์ร้ายหากมีลักษณะไม่เข้าข่ายหรือผิดกฎที่ตั้งไว้ก็อาจจะได้รับอนุญาตให้ผ่านเข้ามาได้โดยที่ไฟร์วอลล์ไม่สามารถทราบได้ ดังนั้นไม่จำเป็นเสมอไปว่าการบุกรุกทั้งหลายสามารถป้องกันได้ด้วยไฟร์วอลล์

2.3 ความสามารถของไฟร์วอลล์

ความสามารถของไฟร์วอลล์มีดังต่อไปนี้

2.3.1 สิ่งที่ไฟร์วอลล์สามารถทำได้

ด้วยคุณสมบัติที่มีอยู่ของไฟร์วอลล์ทำให้สามารถระบุได้อย่างชัดเจนว่าภัยประเภทใดบ้างที่ไฟร์วอลล์สามารถป้องกันได้โดยตรง แต่ทั้งนี้จะต้องอยู่บนสมมติฐานว่าไฟร์วอลล์ได้มีการกำหนดกฎต่างๆ เอาไว้อย่างถูกต้องด้วยจึงจะได้ผล สิ่งที่ไฟร์วอลล์สามารถทำได้มีดังนี้

2.3.1.1 บังคับใช้นโยบายด้านความมั่นคง โดยการกำหนดกฎให้กับไฟร์วอลล์ว่าจะอนุญาตหรือไม่ให้ใช้บริการชนิดใด

2.3.1.2 ทำให้การพิจารณาดูแลและการตัดสินใจด้านความมั่นคงของระบบเป็นไปได้ง่ายขึ้น เนื่องจากการติดต่อทุกชนิดกับเครือข่ายภายนอกจะต้องผ่านไฟร์วอลล์ การดูแลที่จุดนี้เป็นการดูแลความมั่นคงในระดับของเครือข่าย (Network-based Security)

2.3.1.3 **บันทึกข้อมูล** กิจกรรมต่างๆ ที่ผ่านเข้าออกเครือข่ายได้อย่างมีประสิทธิภาพ

2.3.1.4 **ป้องกันเครือข่ายบางส่วน**จากการเข้าถึงของเครือข่ายภายนอก เช่นถ้าหากเรามีบางส่วนที่ต้องการให้ภายนอกเข้ามาใช้บริการ (เช่นถ้ามีแม่ข่ายเว็บ) แต่ส่วนที่เหลือไม่ต้องการให้ภายนอกเข้ามากรณีเช่นนี้เราสามารถใช้ไฟร์วอลล์ช่วยได้

2.3.1.5 **ไฟร์วอลล์บางชนิดสามารถ**ป้องกันไวรัสได้ โดยจะทำการตรวจแฟ้มข้อมูลที่โอนย้ายผ่านทางโพรโทคอล HTTP FTP และ SMTP

2.3.2 สิ่งที่ไฟร์วอลล์ไม่สามารถทำได้

แม้ว่าไฟร์วอลล์จะสามารถช่วยเพิ่มความมั่นคงให้กับเครือข่ายได้มากโดยการตรวจดูข้อมูลที่ผ่านเข้าออก แต่มีสิ่งที่ไม่สามารถป้องกันได้จากการใช้ไฟร์วอลล์คือ

2.3.2.1 **อันตรายที่เกิดจากเครือข่ายภายใน** ไม่สามารถป้องกันได้เนื่องจากอยู่ภายในเครือข่ายเอง ไม่ได้ผ่านไฟร์วอลล์เข้ามา

2.3.2.2 **อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทางไฟร์วอลล์** เช่นการ Dial-up เข้ามายังเครือข่ายภายในโดยตรงโดยไม่ได้ผ่านไฟร์วอลล์

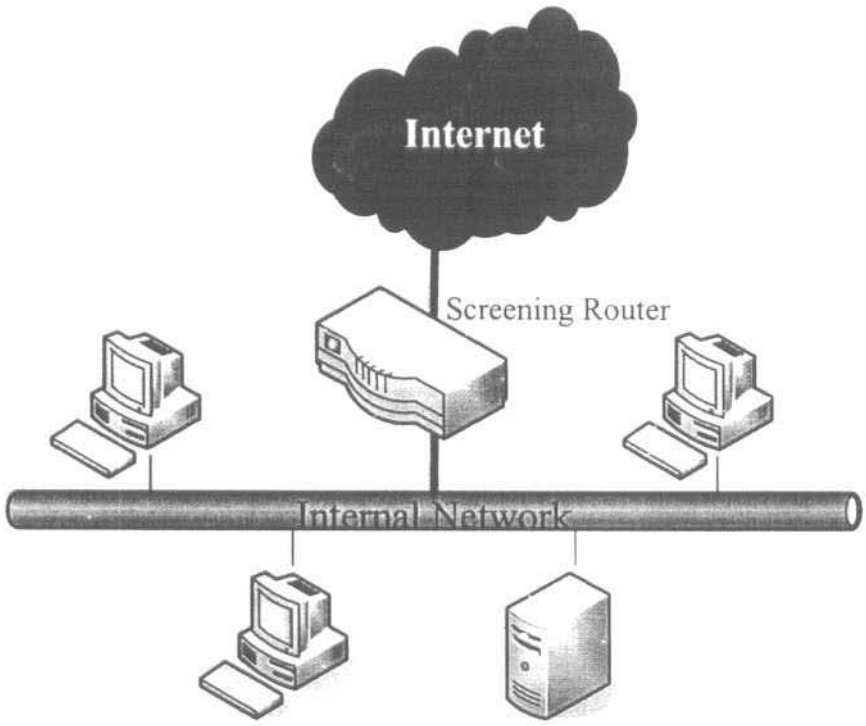
2.3.2.3 **อันตรายจากวิธีใหม่ๆ ที่เกิดขึ้น** ทุกวันนี้มีการพบช่องโหว่ใหม่ๆ เกิดขึ้นทุกวัน เราไม่สามารถไว้ใจไฟร์วอลล์โดยการติดตั้งเพียงครั้งเดียวแล้วก็หวังให้มันปลอดภัยตลอดไป เราต้องมีการดูแลรักษาอย่างต่อเนื่องสม่ำเสมอ

2.3.2.4 **ไวรัส** ถึงแม้จะมีไฟร์วอลล์บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ยังไม่มีไฟร์วอลล์ชนิดใดที่สามารถตรวจสอบไวรัสได้ในทุกๆ โพรโทคอล

2.4 ประเภทของไฟร์วอลล์

ไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม แบ่งได้เป็น

2.4.1 Packet Filtering คืออุปกรณ์จัดเส้นทางที่ทำการหาเส้นทางและส่งต่อ (Route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนหัว (Header) ของกลุ่มข้อมูลที่ผ่านเข้ามา เทียบกับกฎ (Rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (Drop) กลุ่มข้อมูลนั้นไปหรือว่าจะยอม (Accept) ให้กลุ่มข้อมูลนั้นผ่านไปได้



ภาพที่ 2.2 อุปกรณ์จัดเส้นทางแบบคัดเลือก (Screening router) ทำหน้าที่กรองกลุ่มข้อมูล

ข้อมูลที่สำคัญของกลุ่มข้อมูล ซึ่งสามารถนำมาใช้เพื่อเป็นเงื่อนไขสำหรับการควบคุมทราฟฟิคโดยไฟร์วอลล์มีดังนี้

1. Source IP Address : IP Address ของต้นทาง เพื่อใช้ในการพิจารณาต้นทางของข้อมูลว่าอยู่ในเงื่อนไขที่อนุญาตหรือไม่

2. Destination IP Address : IP Address ของปลายทาง เพื่อใช้ในการพิจารณาปลายทางของข้อมูลว่าอยู่ในเงื่อนไขที่อนุญาตหรือไม่

3. Protocol : ระบุโพรโทคอลที่อยู่ในไอพีเดทาแกรม (IP Datagram) ที่กำลังพิจารณานี้

4. Source Port : ระบุช่องทางต้นทางสำหรับโพรโทคอลที่ใช้ช่องทาง (Port) คือ TCP และ UDP ซึ่งข้อมูลช่องทางต้นทางนี้ส่วนใหญ่มักจะมีความสำคัญในลำดับรองลงไป และไม่ถูกนำมาใช้ควบคุมทราฟฟิคมากนัก

5. Destination Port : ระบุช่องทางปลายทางที่กลุ่มข้อมูลนี้ต้องการติดต่อด้วย สำหรับโพรโทคอลที่ใช้ช่องทาง (Port) คือ TCP และ UDP

6. ข้อมูลสำคัญอื่นๆ ตามลักษณะของโพรโทคอล เช่น TCP Flag ICMP Message เป็นต้น

ข้อมูลทั้ง 6 ส่วนนี้จะมีได้อย่างครบถ้วนสมบูรณ์ก็ต่อเมื่อกลุ่มข้อมูลนั้นมีข้อมูลครบถ้วนทั้งหมดของ IP Datagram หากข้อมูลกลุ่มข้อมูลนั้นเป็นส่วนที่แตกออกมา (Fragment) อาจจะทำให้ข้อมูลในส่วนที่ 3 เป็นต้นไปซึ่งอยู่ในโพรโทคอลที่อยู่ชั้นสูงกว่าไอพีไม่สมบูรณ์ อย่างไรก็ตามไฟร์วอลล์ส่วนใหญ่ทำการติดตั้งใช้งานในเครือข่ายเฉพาะที่ (LAN) ซึ่งมีขนาดของกลุ่มข้อมูลที่ใหญ่พอสำหรับรองรับ IP Datagram ได้ทั้งหมด จึงมักไม่ค่อยพบปัญหาแต่อย่างใด ยกเว้นมีการแตกกระจาย (Fragmentation) โดยความประสงค์ของไอพีเอง

การกรองกลุ่มข้อมูล (Packet Filtering) สามารถจัดเตรียมได้จาก 2 แพลตฟอร์ม คือ

1. อุปกรณ์จัดเส้นทางที่มีความสามารถในการทำ Packet Filtering ข้อดีของวิธีนี้คือ มีประสิทธิภาพสูงมีจำนวนโปรแกรมต่อประสาน (Interface) มาก แต่มีข้อเสียคือ หากมีการเปลี่ยนแปลงฟังก์ชันการทำงานจะทำได้ยาก และอาจต้องการหน่วยความจำเป็นจำนวนมากด้วย

2. คอมพิวเตอร์ที่ทำหน้าที่เป็นอุปกรณ์จัดเส้นทาง ข้อดีของวิธีนี้คือ เพิ่มเติมฟังก์ชันการทำงานได้ไม่จำกัด ซึ่งส่งผลต่อประสิทธิภาพการทำงานทำให้มีประสิทธิภาพปานกลาง จำนวนโปรแกรมต่อประสานน้อย และอาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ข้อดีของ Packet Filtering

1. ราคาถูก เพราะเป็นคุณสมบัติที่มักมีในอุปกรณ์จัดเส้นทางอยู่แล้ว อาศัยเพียงการกำหนดเข้าถึงกฎที่เหมาะสมเท่านั้น หากยังไม่มีไฟร์วอลล์อยู่เลย ก็สามารถใช้เพื่อช่วยป้องกันเครือข่ายภายในได้ดีพอสมควรในระดับหนึ่ง

2. หากเครือข่ายภายในไม่ใหญ่มาก และมีการใช้งานอินเทอร์เน็ตอย่างจำกัด ก็สามารถใช้ทดแทนไฟร์วอลล์ได้ทันที

3. การใช้อุปกรณ์จัดเส้นทางแบบคัดเลือก (Screening Router) ทำงานควบคู่กับไฟร์วอลล์จะเป็นการแบ่งเบาภาระของไฟร์วอลล์ได้มาก หากทำการกำหนดเข้าถึงกฎได้อย่างสอดคล้องกันแล้ว จะทำให้มีการป้องกันที่เข้มแข็ง

4. การป้องกันบางประเภทไม่สามารถป้องกันได้โดยไฟร์วอลล์ จะต้องทำโดยการกำหนดที่อุปกรณ์จัดเส้นทางเท่านั้น

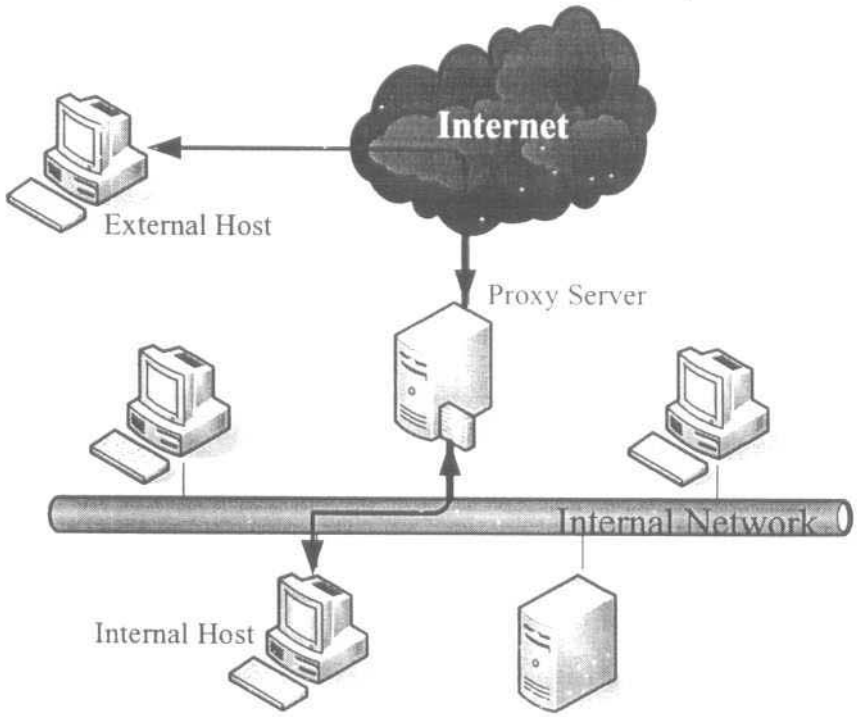
ข้อเสียของ Packet Filtering

1. คำสั่งในการทำงานจะผูกติดกับยี่ห้อของอุปกรณ์จัดเส้นทาง ไม่มีมาตรฐานของคำสั่ง หากเปลี่ยนยี่ห้อของอุปกรณ์จัดเส้นทางก็จะต้องศึกษารูปแบบของคำสั่งใหม่

2. ไม่สามารถกำหนดกฎที่ซับซ้อนได้ เนื่องจากขีดจำกัดของอุปกรณ์จัดเส้นทางที่ทำงานโดยพิจารณาครั้งละกลุ่มข้อมูลเท่านั้น

3. อุปกรณ์จัดเส้นทางมีกำลังในการประมวลผลจำกัด หากเครือข่ายมีขนาดใหญ่และมีการสื่อสารข้อมูลหนาแน่น อุปกรณ์จัดเส้นทางจะทำงานหนักอยู่แล้ว เมื่อต้องมาทำการประมวลผลเข้าถึงกฎด้วยก็อาจจะทำให้ประสิทธิภาพในการจัดเส้นทางกลุ่มข้อมูลต่ำลงไปมาก และการสื่อสารข้อมูลก็จะติดขัดที่อุปกรณ์จัดเส้นทาง เกิดปัญหาคอขวดได้

2.4.2 Proxy หรือ Application Gateway เป็นโปรแกรมประยุกต์ที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเครือข่าย 2 เครือข่าย ทำหน้าที่เพิ่มความมั่นคงของระบบเครือข่ายโดยการควบคุมการเชื่อมต่อระหว่างเครือข่ายภายในและภายนอก Proxy จะช่วยเพิ่มความมั่นคงได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของชั้นโปรแกรมประยุกต์ (Application Layer) เมื่อลูกข่าย (Client) ต้องการใช้บริการภายนอก ลูกข่ายจะทำการติดต่อไปยัง Proxy ก่อน ลูกข่ายจะเจรจา (Negotiate) กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (Connection) 2 การเชื่อมต่อ คือ ลูกข่ายกับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่ Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อกลุ่มข้อมูลให้หรือไม่



ภาพที่ 2.3 แสดงหน้าที่ของแม่ข่ายแทน (Proxy Server)

ข้อดีของ Proxy

1. สามารถควบคุมการติดต่อสื่อสารระหว่างอินเทอร์เน็ตกับเครือข่ายภายในให้อยู่ในชั้นโปรแกรมประยุกต์เท่านั้น ตัดขาดการติดต่อโดยตรงในชั้นเครือข่ายระหว่างอินเทอร์เน็ตกับเครือข่ายภายในออกจากกันอย่างเด็ดขาด ทำให้ลดความเสี่ยงต่อการถูกคุกคามจากการคัดเลือก การเจาะระบบ การก่อกวนโดยใช้เทคนิคในชั้นเครือข่ายที่จะเข้ามายังเครือข่ายภายในได้อย่างเด็ดขาด

2. สามารถเพิ่มเติมหน้าที่การทำงานอย่างอื่นเข้าไปใน Proxy ได้ เช่นสำหรับ Web Proxy นอกจากจะเป็นตัวกลางในการติดต่อแล้ว ยังสามารถควบคุมไม่ให้ Web Browser ติดต่อกับ Web Site ที่ไม่ต้องการได้อีกด้วย โดยการกำหนดรายชื่อ Web Site เหล่านั้นไว้ที่ Proxy

3. สามารถทำการแคชข้อมูลเก็บไว้ในตัว Proxy สำหรับข้อมูลใดที่มีการเรียกใช้ซ้ำบ่อยๆ ก็ไม่จำเป็นต้องไปอ่านจากแม่ข่ายใหม่ทุกครั้ง แต่ส่วนนี้จะใช้งานกับข้อมูลสถิต (Static) เท่านั้น ข้อมูลที่มีการปลี่ยนแปลงตลอดเวลาเป็นพลวัต (Dynamic) อาจจะไม่สามารถแคชไว้ได้

4. ทำให้ผู้ใช้มีการใช้แบนด์วิดท์ร่วมกันอย่างมีประสิทธิภาพ โดยเฉพาะเมื่อใช้ร่วมกับการแคชที่มีอยู่ใน Proxy ทำให้ช่วยประหยัดการใช้งานแบนด์วิดท์ไปได้มาก

5. สามารถเพิ่มเติมส่วนการพิสูจน์ตัวจริง (Authentication) เข้าไปเป็นหน้าที่หนึ่งของ Proxy ได้โดยการอนุญาตให้สามารถใช้งาน Proxy นั้นจะขึ้นอยู่กับสิทธิ์การใช้งานที่ผู้ใช้มีอยู่ ทำให้สามารถควบคุมการใช้งานได้ใกล้ชิดมากขึ้นกว่าการควบคุมโดยพิจารณาจากเลขที่อยู่ไอพี (IP Address) ของโฮสต์เพียงอย่างเดียว

6. สามารถทำการกลั่นกรองเนื้อหาของข้อมูลได้ (Content Filtering) ทำให้สามารถนำมาเป็นเงื่อนไขในการอนุญาตให้ข้อมูลเหล่านั้นผ่านเข้าออกได้ เช่น Web Proxy สามารถตรวจสอบเนื้อหาของ Web Site ที่ผู้ใช้เข้าไปดู หรือกรณีที่เป็น Email Proxy ก็จะสามารถตรวจสอบเนื้อหาในอีเมลได้ว่ามีข้อความที่ไม่เหมาะสมหรือไม่ และอาจจะครอบคลุมถึงการตรวจสอบหาไวรัสที่แนบมากับจดหมายได้อีกด้วย

ข้อเสียของ Proxy

1. ขึ้นอยู่กับโปรแกรมประยุกต์ หากโปรแกรมประยุกต์ไม่รองรับการสื่อสารโดยผ่าน Proxy ก็ไม่สามารถใช้งานได้

2. ไม่สามารถใช้งานกับโปรแกรมประยุกต์ที่ต้องการการสื่อสารโดยตรงแบบ End-to-End ซึ่งกลุ่มข้อมูลจะต้องมาจากโฮสต์ปลายทางทั้งคู่เท่านั้น ผ่านตัวกลางไม่ได้

3. เสี่ยงต่อการละเมิดความเป็นส่วนบุคคล (Privacy) เนื่องจากข้อมูลทั้งหมดที่สื่อสารจะต้องผ่าน Proxy ก่อนเสมอ และ Proxy ก็มีความสามารถที่จะเก็บข้อมูลเหล่านั้นไว้ตรวจสอบได้ หากมีผู้นำข้อมูลเหล่านั้นไปวิเคราะห์จะสามารถทราบการใช้งานหรืออาจจะทราบข้อมูลทั้งหมดของผู้ใช้ได้

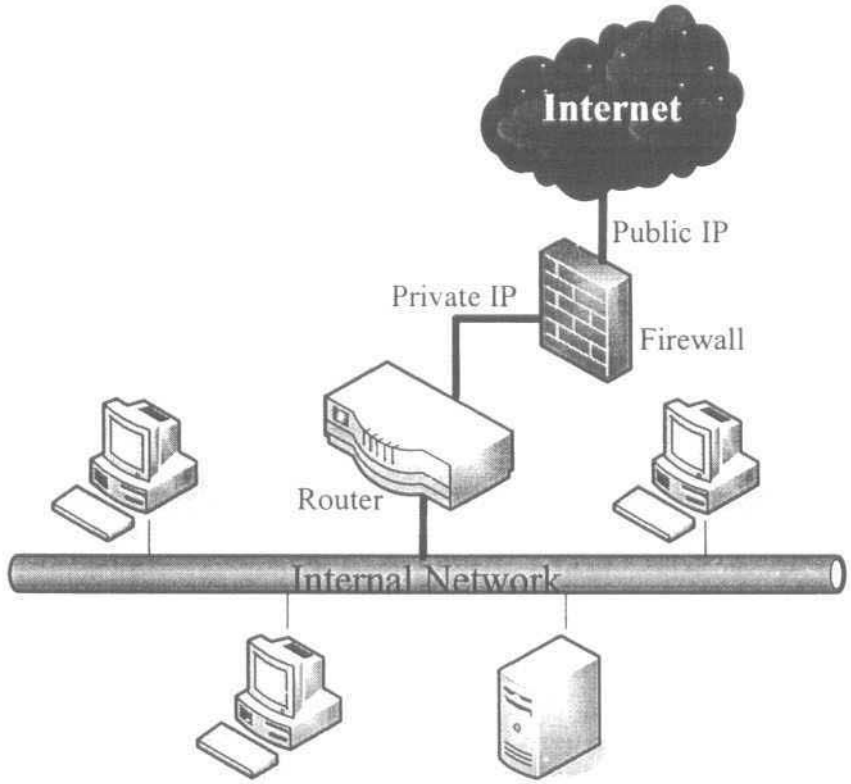
4. เนื่องจากลักษณะของแต่ละโปรแกรมประยุกต์นั้นจะแตกต่างกันออกไป ดังนั้น Proxy ของแต่ละโปรแกรมประยุกต์จึงทำหน้าที่เฉพาะโปรแกรมประยุกต์นั้นๆ ไม่สามารถใช้ร่วมกันได้ หากโฮสต์ที่อยู่หลัง Proxy มีการใช้งานหลายโปรแกรมประยุกต์ก็จะต้องมี Proxy จำนวนมากเปิดให้บริการตามจำนวนโปรแกรมประยุกต์นั้นๆ

5. ความสามารถในการประมวลผลของโฮสต์ที่ทำหน้าที่ Proxy อาจจะเป็นปัญหาคอขวดของระบบได้ เพราะการสื่อสารทั้งหมดของลูกข่ายและแม่ข่ายจะถูกรวมศูนย์ที่ Proxy ก่อนเสมอแทนที่จะกระจายไปยังลูกข่ายและแม่ข่าย ปัญหาลักษณะนี้จะสามารถพบได้ชัดเมื่อมีลูกข่ายจำนวนมาก

6. เนื่องจาก Proxy เป็นโปรแกรมประยุกต์ชนิดหนึ่งเช่นกัน การติดต่อกับในเครือข่ายจะอาศัยระบบปฏิบัติการเป็นหลัก จึงมีความสามารถในการป้องกันตัวเองต่ำกว่าไฟร์วอลล์ทั่วไป ตัว Proxy เองจึงมีความเสี่ยงต่อการถูกโจมตีได้มากและเปราะบางต่อการ DoS (Denial of Service) ด้วยเทคนิคในชั้นเครือข่าย ซึ่งอาจจะส่งผลให้ Proxy หยุดการทำงานลงได้โดยง่าย โดยเฉพาะเมื่อ Proxy นั้นเป็นโฮสต์ที่ต่อโดยตรงกับอินเทอร์เน็ต จึงเป็นเสมือนด่านหน้าของเครือข่ายที่จะต้องถูกคัดเลือก ถูกเจาะอย่างแน่นอน แต่ระดับความต้านทานของ Proxy นั้นต่ำกว่าไฟร์วอลล์ทั่วไปจึงมีแนวโน้มว่าหากใช้ Proxy โดยปราศจากไฟร์วอลล์ร่วมด้วยโอกาสที่ Proxy จะโดนเจาะได้นั้นมีอยู่สูงมาก

2.4.3 Stateful Inspection Technology โดยปกติแล้ว Packet Filtering แบบธรรมดา (ที่เป็น Stateless แบบที่มีอยู่ในอุปกรณ์จัดเส้นทางทั่วไป) จะควบคุมการเข้าออกของกลุ่มข้อมูลโดยพิจารณาข้อมูลจากส่วนหัวของแต่ละกลุ่มข้อมูล นำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในส่วนหัวเท่านั้น ดังนั้น Packet Filtering แบบธรรมดาจึงไม่สามารถทราบได้ว่า กลุ่มข้อมูลนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นกลุ่มข้อมูลที่เข้ามาติดต่อใหม่หรือเปล่า หรือว่าเป็นกลุ่มข้อมูลที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น

Stateful Inspection Technology เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยในการพิจารณาว่าจะยอมให้กลุ่มข้อมูลผ่านไปนั้น แทนที่จะดูข้อมูลจากส่วนหัวเพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของกลุ่มข้อมูล (Message content) และข้อมูลที่ได้จากกลุ่มข้อมูลก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่ากลุ่มข้อมูลใดเป็นกลุ่มข้อมูลที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว



ภาพที่ 2.4 สเตทฟูลไฟร์วอลล์

ข้อดีของ Stateful firewall

1. ใช้งานง่ายเพราะถูกออกแบบมาทำหน้าที่ของไฟร์วอลล์โดยเฉพาะ ตรวจสอบแก้ไขเข้าถึงกฎได้ง่าย ทำให้ผู้ใช้ไม่ต้องคอยกังวลถึงคำสั่ง และรูปแบบของคำสั่ง ถึงแม้ว่าจะต่างยี่ห้อกันก็สามารถเรียนรู้ใหม่ได้อย่างรวดเร็ว

2. ประสิทธิภาพในการทำงานสูง สามารถรองรับเข้าถึงกฎที่ซับซ้อนได้ โดยที่ความสามารถในการทำงานไม่ตกลง

3. มีคุณสมบัติเพิ่มเติมให้ใช้ได้มากนอกเหนือจากการควบคุมทราฟฟิค เช่น สามารถนำไปใช้ร่วมกับระบบตรวจจับการบุกรุกหรือ IDS (Intrusion Detection System) เพื่อป้องกันการโจมตีได้อัตโนมัติ สามารถบันทึกข้อมูลเอาไว้กลับมาดูในภายหลังได้ สามารถใช้งานร่วมกับระบบ Anti-Virus ได้เป็นต้น

4. การกำหนดเข้าถึงกฎทำได้ง่าย เพราะไฟร์วอลล์มีความเข้าใจในโพรโทคอลระดับสูง ดังนั้นผู้ใช้อาจจะไม่จำเป็นต้องมีความเชี่ยวชาญในเรื่องเครือข่ายมาก ก็พอจะใช้งานไฟร์วอลล์ได้โดยกำหนดกฎบนพื้นฐานของโปรแกรมประยุกต์ที่ผู้ใช้รู้จัก มากกว่าการกำหนดกฎโดยใช้ข้อมูลบนกลุ่มข้อมูลโดยตรง

5. สามารถเพิ่มเติมบริการอื่นได้ เช่น VPN (Virtual Private Network) Tunneling

6. สามารถเพิ่มเติมความมั่นคงโดยระบบการพิสูจน์ตัวจริง (Authenticatation) ได้

7. การสื่อสารระหว่างไฟร์วอลล์กับส่วนเฝ้าคุมการบริหาร (Administration Console : โฮสต์ที่ทำหน้าที่ในการบริหารไฟร์วอลล์) จะมีความมั่นคงสูง มีการตรวจสอบสิทธิ์ของผู้ที่เป็นผู้ดูแลระบบ รวมทั้งการสื่อสารระหว่างไฟร์วอลล์กับส่วนเฝ้าคุมจะมีการรักษาความมั่นคงที่เข้มงวด มีการเข้ารหัสเพื่อป้องกันการดักอ่านข้อมูล

ข้อเสียของ Stateful firewall

1. มีราคาแพง ถึงแม้ว่าปัจจุบันจะลดลงไปมากแล้วแต่ก็ยังแพงอยู่

2. ในกรณีที่เป็นไฟร์วอลล์แบบซอฟต์แวร์ที่ทำงานอยู่บนระบบปฏิบัติการทั่วไป เช่น Solaris Windows NT Windows 2000 ต่างก็มีความเสี่ยงที่จะถูกเจาะได้เนื่องจากปัญหาของแต่ละระบบปฏิบัติการเอง ซึ่งจะสามารถเจาะได้ง่ายกว่าการเจาะอุปกรณ์จัดเส้นทาง เพราะช่องโหว่ของระบบปฏิบัติการมีมากกว่าของอุปกรณ์จัดเส้นทาง

3. ในกรณีที่ไฟร์วอลล์เป็นประเภท Network Appliance คืออออกแบบทั้งซอฟต์แวร์และฮาร์ดแวร์เป็นเครื่องเดียวกันเพื่อทำหน้าที่เป็นไฟร์วอลล์โดยเฉพาะ ผู้ใช้จำเป็นต้องพึ่งพาผู้ผลิตค่อนข้างมาก หากมีปัญหาอาจจะไม่สามารถแก้ไขโดยการใช้อะไหล่ทดแทนจากที่อื่นได้

สำหรับงานวิจัยนี้ทำการค้นหาและแก้ไขกฎของไฟร์วอลล์ประเภท Packet Filtering

2.5 นโยบายความมั่นคง

นโยบายความมั่นคงเป็นสิ่งสำคัญขั้นพื้นฐานขององค์กรที่มีผลต่อการป้องกันและรักษาความมั่นคงในระบบคอมพิวเตอร์และเครือข่ายที่ชัดเจนและสามารถบังคับใช้ได้ เพราะไฟร์วอลล์นั้นเป็นเพียงเครื่องมือรักษาความมั่นคงทางเทคนิคซึ่งสามารถกำหนดให้ทำการป้องกันได้ตามที่ผู้บริหารเครือข่ายต้องการ หากมีไฟร์วอลล์แล้วแต่การควบคุมที่กำหนดให้แก่ไฟร์วอลล์นั้นมีเพียงเล็กน้อย ไฟร์วอลล์นั้นก็สามารถช่วยป้องกันได้อย่างจำกัด ในทางกลับกันหากมีการควบคุมอย่างเคร่งครัดแล้วแน่นอนว่าจะช่วยให้เกิดความมั่นคงสูงขึ้น แต่อาจจะส่งผลกระทบต่อผู้ใช้จนไม่สามารถใช้งานเครือข่ายได้อย่างสะดวกเช่นกัน หากไม่มีกฎเกณฑ์ใดเป็นแนวทางสำหรับการปฏิบัติแล้วย่อมจะทำให้การดำเนินการนั้นสำเร็จได้ยากยิ่ง

นโยบายความมั่นคงของไฟร์วอลล์ (Firewall security policy) อาจเป็นรายการของข้อความหรือเป็นรายการของกฎ หรือ Filtering rule ที่ถูกเรียงลำดับแล้ว โดยนโยบายจะกำหนดแอ็คชัน (Action) ที่ปฏิบัติต่อกลุ่มข้อมูล ซึ่งเปรียบเสมือนการจำกัดสิทธิ์ในการเข้าถึงระบบที่ให้ต่อผู้ใช้งานหรือโฮสต์ภายในเครือข่ายในทุกระดับที่ใช้งานเครือข่ายร่วมกันนั่นเอง

จุดตัดสินสำหรับความสมดุล ความเหมาะสม และความเพียงพอของการรักษาความมั่นคงนั้นจะต้องพิจารณาภาพรวมของผลกระทบที่มีต่อองค์กรเป็นหลัก ธรรมชาติและวัตถุประสงค์ของแต่ละองค์กรนั้นแตกต่างกัน ความอ่อนไหวต่อความมั่นคงก็แตกต่างกัน ตัวอย่างเช่น ระบบคอมพิวเตอร์และเครือข่ายของสถาบันการเงินย่อมต้องการความมั่นคงมากกว่าระบบฐานข้อมูลนักศึกษาของมหาวิทยาลัย เป็นต้น ดังนั้นแนวทางการปฏิบัติและกฎเกณฑ์ขององค์กรใดย่อมเป็นไปเพื่อรองรับกับองค์กรนั้น อาจจะนำมาเป็นตัวอย่างได้บ้างแต่ไม่สามารถนำมาประยุกต์ใช้ทั้งหมดได้

นโยบายความมั่นคงจึงต้องได้รับการพิจารณาจากผู้บริหารระดับสูงขององค์กรนั้น โดยพิจารณาควบคู่กับวิสัยทัศน์ ภารกิจ และกลยุทธ์ขององค์กร เมื่อมีนโยบายความมั่นคงที่ผ่านการเห็นชอบและบังคับใช้จากองค์กรแล้ว จะทำให้ผู้ปฏิบัติงานในหน่วยงานต่างๆ ขององค์กรมีแนวทางการทำงานชัดเจน ลดความขัดแย้งกันของผู้ที่มีหน้าที่แตกต่างกัน ทำให้องค์กรสามารถดำรงรักษาความมั่นคงได้ในระดับสูง และยังคงให้ความสะดวกสบายต่อผู้ใช้ได้ตามสมควร

ดังนั้นก่อนการนำไฟร์วอลล์ไปควบคุมทราฟฟิค ณ จุดใดจุดหนึ่ง จำเป็นอย่างยิ่งที่จะต้องมีนโยบายความมั่นคงเป็นหลักไว้ก่อนเสมอ แม้ว่าในความเป็นจริงยังมีหน่วยงานไม่มากที่มีนโยบายรักษาความมั่นคงสำหรับระบบงานสารสนเทศ แต่ก็มีความจำเป็นต้องร่างขึ้นมาใช้ให้ได้ในขั้นนี้

อย่างน้อยก็ควรจะจัดทำนโยบายความมั่นคงชั่วคราวให้แก่องค์กรและผ่านการอนุมัติเสียก่อน จากนั้นจึงค่อยดำเนินการในส่วนเทคนิคที่เกี่ยวข้องกับไฟร์วอลล์ตามนโยบายนั้นต่อไป

นโยบายความมั่นคงที่ดีควรจะครอบคลุมส่วนต่างๆ ดังต่อไปนี้

1. การปฏิบัติงานตามปกติของผู้ใช้ที่ทำให้ผู้ใช้ปลอดภัย เพื่อเป็นแนวทางในการปฏิบัติงานทั่วๆ ไปของผู้ใช้ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ เช่น การใช้ซอฟต์แวร์ การรับ-ส่งอีเมล เป็นต้น

2. การปฏิบัติงานของผู้ที่มีหน้าที่รับผิดชอบทางเทคนิค เช่น ผู้บริหารระบบ (System Administrator) วิศวกรเครือข่าย เป็นต้น เพื่อเป็นแนวทางในการปฏิบัติงานที่สามารถวางใจได้ว่าจะทำให้ระบบมีความมั่นคง เช่น การสำรองข้อมูล การทดสอบระบบ เป็นต้น

3. ข้อห้ามต่างๆ ที่ไม่พึงปรารถนาต่อองค์กร และไม่อนุญาตให้ผู้ใช้ดำเนินการกิจกรรมตามข้อห้ามที่กำหนดไว้ เช่น การใช้งานชื่อผู้อื่น เป็นต้น

4. ข้อจำกัดในการใช้งาน เช่น ไม่อนุญาตให้ใช้โปรแกรมบางประเภท หรือ ไม่อนุญาตให้ใช้งาน Web Site บางประเภท เป็นต้น

5. การป้องกันทางเทคนิคขั้นต่ำ เพื่อทำให้มั่นใจได้ว่าสามารถควบคุม ป้องกัน และตรวจจับเหตุการณ์ผิดปกติที่จะส่งผลกระทบต่อความมั่นคงของระบบได้

6. หน้าที่และความรับผิดชอบในด้านความมั่นคงของผู้ที่เกี่ยวข้องกับระบบสารสนเทศ ไม่ว่าจะเป็นผู้บริหาร ผู้ใช้งานระบบ และผู้มีหน้าที่ทางเทคนิคต่างๆ

2.6 กฎการเข้าถึง (Access Rules)

กฎการเข้าถึง คือกฎที่ไฟร์วอลล์ใช้ในการพิจารณาทราฟฟิคที่จะผ่านแนวป้องกันของไฟร์วอลล์ไปยังโซนต่างๆ กฎการเข้าถึงถือเป็นหัวใจสำคัญที่สุดของไฟร์วอลล์ทั้งในด้านความมั่นคงและในด้านความสามารถในการใช้งานเครือข่าย ถ้าหากขาดซึ่งเข้าถึงกฎที่ถูกต้องเหมาะสมแล้ว โครงสร้างและองค์ประกอบต่างๆ ในเครือข่ายที่ถูกจัดเตรียมไว้เป็นอย่างดีเพื่อให้ไฟร์วอลล์สามารถทำหน้าที่ควบคุมทราฟฟิคได้อย่างมีประสิทธิภาพนั้นก็ดูเหมือนจะไม่มีประโยชน์เลย เพราะเข้าถึงกฎเป็นสิ่งสำคัญในการทำให้เครือข่ายทั้งหมดปลอดภัย โดยการกำหนดกฎการเข้าถึงจะต้องพิจารณาถึงนโยบาย สภาพการใช้งาน และองค์ประกอบต่างๆ ในแต่ละเครือข่ายเป็นสำคัญ กฎการเข้าถึงที่ดีจะต้องสามารถทำให้เครือข่ายทั้งหมดปลอดภัยและสามารถใช้งานได้ดี และต้องสามารถป้องกันปัญหาความมั่นคงอื่นที่อาจเกิดขึ้นในอนาคตได้ด้วย

รูปแบบทั่วไปของกฎ คือ

<order><protocol> <src_ip> <src_port> <dst_ip> <dst_port> <action>

กฎการเข้าถึง หรือ กฎการกรอง (Filtering rule) ที่อยู่ภายในไฟร์วอลล์ โดยปกติแล้วจะประกอบด้วยเขตข้อมูลทั้งหมด 6 เขตข้อมูลที่เรียงลำดับกัน ดังนี้

1. ลำดับ (Order) คือ ลำดับใดๆ ของกฎที่อยู่ในไฟร์วอลล์ใดไฟร์วอลล์หนึ่ง

2. โพรโทคอล (Protocol) คือ รูปแบบในการสื่อสารข้อมูล โพรโทคอลที่ใช้โปรแกรมประยุกต์แต่ละตัวย่อมมีวิธีการสื่อสารข้อมูลอย่างใดอย่างหนึ่งของตนเองแน่นอน ซึ่งหากใช้ TCP/IP แล้วย่อมจะมีทางเลือกสำหรับใช้งานอยู่เพียง 3 โพรโทคอลคือ TCP UDP และ ICMP

3. เลขที่อยู่ของไอพีต้นทาง (Source IP address หรือ src_ip) คือ ต้นทางของการสื่อสารข้อมูล ที่จะแสดงให้เห็นว่าข้อมูลที่กำลังจะผ่านไฟร์วอลล์นั้นมีต้นกำเนิดมาจากที่ใด ซึ่งจะทำให้สามารถคาดการณ์ได้ว่าผู้ที่ใช้งานโฮสต์นั้นเป็นใคร มีสิทธิ์ในการใช้งานที่อนุญาตมากน้อยเพียงใด

4. ช่องทางของต้นทาง (Source port หรือ src_port) คือ ข้อมูลส่วนที่เป็นการระบุว่าต้นทางมีการใช้บริการประเภทใด หรือมีวัตถุประสงค์เพื่อให้หรือรับบริการใด เช่น ช่องทาง 80 เป็นบริการแบบ Http ช่องทาง 23 เป็นบริการแบบ Telnet หรือ ช่องทาง 21 เป็นบริการแบบ Ftp เป็นต้น

5. เลขที่อยู่ของไอพีปลายทาง (Destination IP address หรือ dst_ip) คือ ปลายทางของการสื่อสารข้อมูล ที่จะแสดงให้เห็นว่าข้อมูลที่กำลังจะผ่านไฟร์วอลล์นั้นมีเป้าหมายสุดท้ายปลายทางที่ใด ซึ่งจะทำให้สามารถคาดการณ์ได้ว่าเจ้าของข้อมูลชุดนั้นต้องการสื่อสารกับใคร

6. ช่องทางของปลายทาง (Destination port หรือ dst_port) คือ ข้อมูลส่วนที่เป็นการระบุว่าปลายทางมีการใช้บริการประเภทใด หรือมีวัตถุประสงค์เพื่อให้หรือรับบริการใด เช่น ช่องทาง 80 เป็นบริการแบบ Http ช่องทาง 23 เป็นบริการแบบ Telnet หรือ ช่องทาง 21 เป็นบริการแบบ Ftp เป็นต้น

7. แอ็คชัน (Action) ในการทำงานของไฟร์วอลล์นั้นต้นทาง (Source) ปลายทาง (Destination) และช่องทาง (Port) จะเป็นเงื่อนไขที่ไฟร์วอลล์จะนำกลุ่มข้อมูลที่ผ่านเข้ามาไม่ว่าจากทิศทางใดขึ้นมาเปรียบเทียบ หากพบว่ากลุ่มข้อมูลที่ผ่านเข้ามานั้นมีองค์ประกอบทั้ง 3 ประการตรงตามที่ระบุไว้ การตัดสินใจที่จะดำเนินการใดๆ ของไฟร์วอลล์จะต้องอาศัยคำสั่งที่ระบุอยู่ในส่วนแอ็คชัน นี้เองว่าควรจะทำอย่างไรกับกลุ่มข้อมูลที่กำลังจะผ่านไป แอ็คชันที่สามารถกำหนดให้ไฟร์วอลล์ดำเนินการได้นั้นคือ Allow หรือ Deny

Allow หมายถึง อนุญาตหรือยอมรับให้กลุ่มข้อมูลที่ตรงตามเงื่อนไขสามารถผ่านไฟร์วอลล์ไปยังปลายทางได้ตามปกติ การทำงานของไฟร์วอลล์เมื่อ Allow ก็จะเป็นเสมือนอุปกรณ์จัดเส้นทางตัวหนึ่งนั่นเอง

Deny หมายถึง บล็อกหรือปฏิเสธไม่ให้กลุ่มข้อมูลนั้นผ่านไฟร์วอลล์ไปยังปลายทางได้ โดยจะทิ้งกลุ่มข้อมูลที่เข้ามานั้นไป

2.7 ตัวอย่างกฎการเข้าถึงในไฟร์วอลล์

ตัวอย่างกฎที่มีการระบุค่าไว้ในเขตข้อมูลต่างๆ เช่น

1: 129.162.32.*, any, 184.140.*.*, 80, allow

หมายถึง กฎนี้ได้ระบุไว้ว่าจะอนุญาตให้กลุ่มข้อมูลที่มีไอพีต้นทาง 129.162.32.* และหมายเลขช่องทางต้นทางใดๆ และไอพีปลายทางไปที่ 184.140.*.* และหมายเลขช่องทางปลายทางเท่ากับ 80 ผ่านไฟร์วอลล์ไปได้

2: 184.140.18.*, any, 129.162.*.*, 21, deny

หมายถึง กฎนี้ได้ระบุไว้ว่าจะไม่อนุญาตให้กลุ่มข้อมูลที่มีไอพีต้นทาง 184.140.18.* และหมายเลขช่องทางต้นทางใดๆ และไอพีปลายทางไปที่ 129.162.*.* และหมายเลขช่องทางปลายทางเท่ากับ 21 ผ่านไฟร์วอลล์ไปได้

ตัวอย่างกลุ่มของกฎที่แสดงให้เห็นถึงความสำคัญของลำดับของกฎในไฟร์วอลล์ เช่น

1: 129.162.32.50, any, *.*.*.*. 25, deny
2: 129.162.32.*, any, *.*.*.*, 25, allow
3: *.*.*.*, any, 184.140.36.10. 25, allow
4: 129.162.32.30, any, *.*.*.*. 80, deny
5: 129.162.32.*, any, *.*.*.*. 80, allow
6: *.*.*.*, any, *.*.*.*, any, deny

ลำดับของกฎถือเป็นสิ่งที่สำคัญต่อการกำหนดนโยบายในไฟร์วอลล์ทุกๆ ตัว เนื่องจากในกระบวนการกรองกลุ่มข้อมูลจะกระทำอย่างเป็นลำดับเริ่มต้นจากกฎลำดับที่ 1 เรียงกันเป็นลำดับไป แต่ละเซตข้อมูลของกฎจะถูกพิจารณาเพื่อเปรียบเทียบกับข้อมูลในส่วนหัวของแต่ละกลุ่มข้อมูลที่ผ่านเข้ามาในไฟร์วอลล์ ผลลัพธ์จากการเปรียบเทียบหากพบว่าไม่มีกฎในลำดับใดลำดับหนึ่งที่ห้ามไว้ก็จะอนุญาต (Allow) ให้กลุ่มข้อมูลนั้นผ่านไปได้ หรือหากมีกฎในลำดับใดๆ ที่ห้ามไว้กลุ่มข้อมูลนั้นก็จะถูกบล็อกไว้ (Deny) เพื่อไม่ให้กลุ่มข้อมูลนั้นผ่านไปได้ ยิ่งไปกว่านั้นลำดับนอกจากจะถูกใช้เพื่อการกรองกลุ่มข้อมูลอย่างเป็นลำดับแล้ว ลำดับยังมีความสำคัญในเรื่องการค้นหาความผิดปกติระหว่างกฎด้วยกันเองภายในไฟร์วอลล์ เช่น กฎลำดับที่ 1 และกฎลำดับที่ 2 การเรียงลำดับเช่นนี้ไม่พบความผิดปกติระหว่างกฎทั้งสองเนื่องจากกฎลำดับที่ 2 เป็นกฎทั่วไป (General rule) ที่นอกเหนือจากข้อจำกัดของกฎลำดับที่ 1 โดยกฎลำดับที่ 1 ซึ่งหมายถึง กฎนี้ได้ระบุไว้ว่าจะไม่อนุญาตให้กลุ่มข้อมูลที่มีไอพีต้นทาง 129.162.32.50 และหมายเลขช่องทางต้นทางใดๆ และปลายทางไปที่ไอพีใดๆ และหมายเลขช่องทางปลายทางเท่ากับ 25 ผ่านไฟร์วอลล์ไปได้ และกฎลำดับที่ 2 ซึ่งหมายถึง กฎนี้ได้ระบุไว้ว่าจะอนุญาตให้กลุ่มข้อมูลที่มีไอพีต้นทาง 129.162.32.* และหมายเลขช่องทางต้นทางใดๆ และปลายทางไปที่ไอพีใดๆ และหมายเลขช่องทางปลายทางเท่ากับ 25 ผ่านไฟร์วอลล์ไปได้

อย่างไรก็ตามหากว่ากฎทั้งสองถูกเรียงลำดับสลับที่กัน นั่นคือกฎลำดับที่ 1 กลายเป็น กฎลำดับที่ 2 และกฎลำดับที่ 2 กลายเป็น กฎลำดับที่ 1 นั้นจะทำให้เกิดความผิดพลาดที่ส่งผลต่อนโยบายความมั่นคงที่ได้วางไว้ ทั้งนี้เป็นเพราะกฎลำดับที่ 1(กฎลำดับที่ 2 เดิม) อนุญาตให้กลุ่มข้อมูลที่มีไอพีต้นทาง 129.162.32.50 และหมายเลขช่องทางต้นทางใดๆ และปลายทางไปที่ไอพีใดๆ และหมายเลขช่องทางปลายทางเท่ากับ 25 ผ่านไฟร์วอลล์ไปได้ ในขณะที่กฎลำดับที่ 2 (กฎลำดับที่ 1 เดิม) ไม่อนุญาตให้กลุ่มข้อมูลเดียวกันนี้ผ่านไฟร์วอลล์ไปได้ หรือในทำนองเดียวกันกับกฎลำดับที่ 4 และกฎลำดับที่ 5

สำหรับแต่ละเซตข้อมูลของกฎที่ซึ่งสามารถนำมาเปรียบเทียบกับข้อมูลภายในส่วนหัวของกลุ่มข้อมูลจริง ได้แก่ไอพีต้นทาง (src_ip) ช่องทางของไอพีต้นทาง (src_port) ไอพีปลายทาง (dst_ip) และช่องทางของไอพีปลายทาง (dst_port) ถ้าเซตข้อมูลใดปรากฏเครื่องหมายดอกจัน (*) นั่นหมายความถึง ค่าใดๆ ตามความหมายของเซตข้อมูลนั้นๆ ยกตัวอย่างเช่น src_ip หรือ dst_ip เท่ากับ 129.162.*.* หมายความว่า ค่าของไอพีในส่วนที่ระบุเครื่องหมายดอกจันนั้นมีค่าตั้งแต่ 0-255 (8 บิต) ในขณะที่ src_port หรือ dst_port เท่ากับ * หมายความว่า ช่องทางที่ระบุเครื่องหมายดอกจันมีค่าตั้งแต่ 0-65536 (16 บิต) เป็นต้น นอกจากนี้เราสมมติให้กฎโดยปริยาย (Default filtering rule) ของแต่ละไฟร์วอลล์มีแอ็คชันเป็น Deny และอยู่ในลำดับสุดท้ายเสมอ