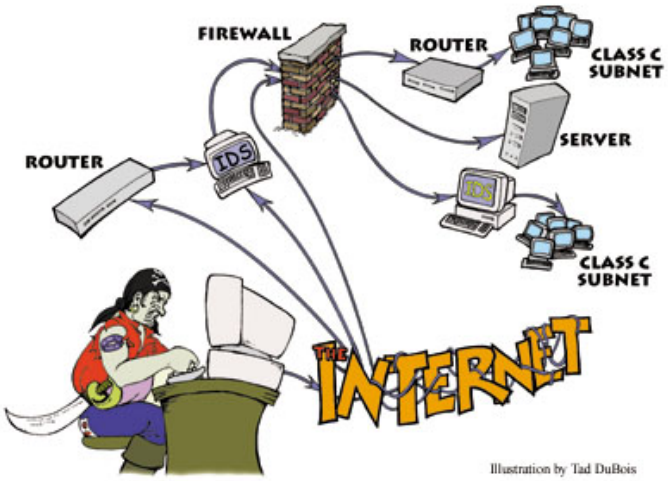
ระบบรักษาความปลอดภัยในระบบเครือข่าย

ปัจจุบันอินเตอร์เน็ตมีบทบาทสำคัญต่อการดำเนินกิจกรรมต่างๆ เป็นอย่างมาก ไม่ว่าจะเป็นด้านการติดต่อสื่อสาร ธุรกิจ การศึกษา หรือว่าเพื่อความบันเทิง องค์กรต่างๆ ระบบรักษาความปลอดภัยในระบบเครือข่าย



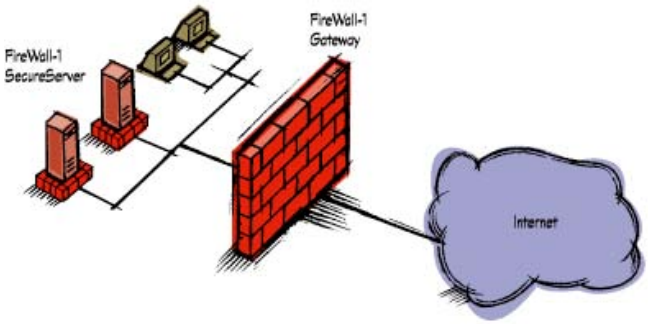
ปัญหาที่ตามมาก็คือความปลอดภัยของระบบเน็ตเวิร์ก เช่น ทำให้เกิดความเสี่ยงต่อการถูกเจาะระบบ และ ขโมยข้อมูล เป็นต้น

จากปัญหาดังกล่าวทำให้เราต้องมีวิธีการในการรักษาความปลอดภัยสิ่งที่สามารถช่วยลดความเสี่ยงนี้ได้ก็คือ ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ หมายถึงกำแพงที่เอาไว้ป้องกันไฟไม่ให้ลุกลามไปยังส่วนอื่นๆ ส่วนทางด้านคอมพิวเตอร์นั้นก็มีความหมายคล้ายๆ กันคือเป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเตอร์เน็ตหรือเน็ตเวิร์กภายนอก

ไฟร์วอลล์ เป็นคอมโพเน็นต์หรือกลุ่มของคอมโพเน็นต์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเน็ตเวิร์กภายนอกหรือเน็ตเวิร์กที่เราคิดว่าไม่ปลอดภัย กับเน็ตเวิร์กภายใน โดยที่คอมโพเน็นต์นั้นอาจจะเป็นเราเตอร์ คอมพิวเตอร์ หรือเน็ตเวิร์ก ประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือ Firewall Architecture ที่ใช้

ไฟร์วอลล์ คือ ระบบหรือกลุ่มของระบบที่บังคับใช้นโยบายการควบคุมการเข้าถึงของระหว่างสองเครือข่าย การควบคุมการเข้าถึงของไฟร์วอลล์นั้นสามารถทำได้ในหลายระดับและหลายรูปแบบขึ้นอยู่ชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น เราสามารถกำหนดได้ว่าจะให้
มีการเข้ามาใช้ Service อะไรได้บ้าง จากที่ไหน



ไฟร์วอลล์สามารถช่วยเพิ่มความปลอดภัยให้กับระบบได้โดย

1. บังคับใช้นโยบายด้านความปลอดภัย
2. ทำให้การพิจารณาดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่าย
3. บันทึกข้อมูล กิจกรรมต่างๆ ที่ผ่านเข้าออกเน็ตเวิร์กได้อย่างมีประสิทธิภาพ
4. ป้องกันเน็ตเวิร์กบางส่วนจากการเข้าถึงของเน็ตเวิร์กภายนอก
5. ไฟร์วอลล์บางชนิด สามารถป้องกันไวรัสได้

สิ่งเหล่านี้ไม่สามารถป้องกันได้จากการใช้ ไฟร์วอลล์

1. อันตรายที่เกิดจากเน็ตเวิร์กภายใน
2. อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทางไฟร์วอลล์
3. อันตรายจากวิธีใหม่ๆ
4. ไวรัสคอมพิวเตอร์

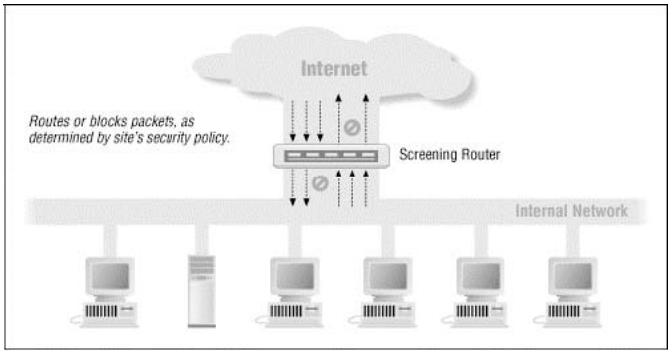
ชนิดของไฟร์วอลล์

ชนิดของไฟร์วอลล์ แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม แบ่งได้เป็น

1. Packet Filtering
2. Proxy Service
3. Stateful Inspection

1. Packet Filtering

คือเราเตอร์ที่หาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไขโดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามาเทียบกับกฎ (rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไป หรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้



ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของอินเตอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (Transport Layer) Packet Filtering ในอินเตอร์เน็ตโมเดล ซึ่งในอินเตอร์เน็ตเลเยอร์จะมีแอตทริบิวต์ที่สำคัญต่อ Packet Filtering
ดังนี้

1. ไอพีต้นทาง
2. ไอพีปลายทาง
3. ชนิดของโปรโตคอล (TCP UDP และ ICMP)

ในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ

1. พอร์ตต้นทาง
2. พอร์ตปลายทาง
3. แฟล็ก (Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต TCP)
4. ชนิดของ ICMP message (ในแพ็กเก็ต ICMP) ซึ่งพอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่

บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP, พอร์ต 21 หมายถึง FTP เป็นต้น

Packet Filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม

แพล็ตฟอร์ม	ข้อดี	ข้อเสีย
เราเตอร์	ประสิทธิภาพสูงมีจำนวนอินเตอร์เฟสมาก	เพิ่มเติมฟังก์ชันการทำงานได้ยาก, อาจต้องการหน่วยความจำมาก
คอมพิวเตอร์	เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด	ประสิทธิภาพปานกลาง,จำนวนอินเตอร์เฟสน้อย,อาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ข้อดี-ข้อเสียของ Packet Filtering

ข้อดี

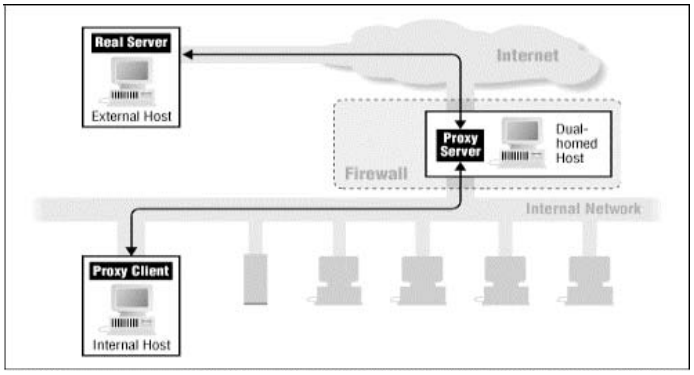
- ไม่ขึ้นกับแอพพลิเคชัน
- มีความเร็วสูง
- รองรับการขยายตัวได้ดี

ข้อเสีย

- บางโปรโตคอลไม่เหมาะสมกับการใช้ Packet Filtering เช่น FTP, ICQ

2.Proxy Service

Proxy หรือ Application Gateway เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)



ข้อดี-ข้อเสียของ Proxy

ข้อดี

- มีความปลอดภัยสูง
- รู้จักข้อมูลในระดับแอพพลิเคชัน

ข้อเสีย

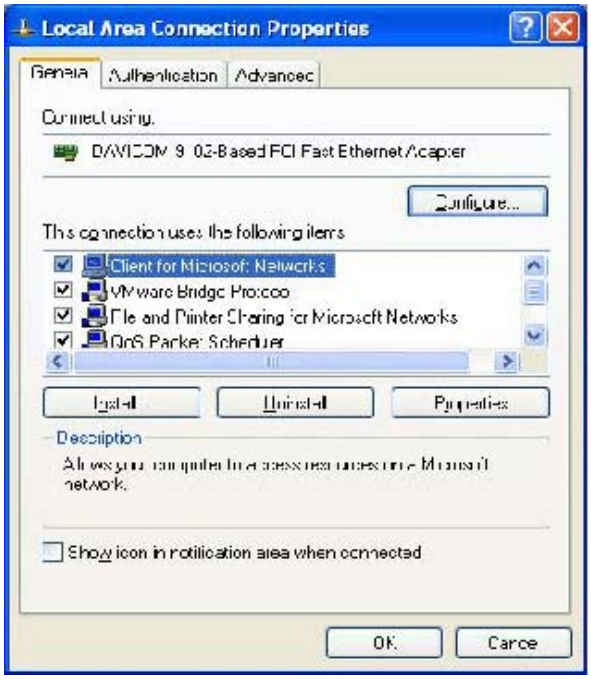
- ประสิทธิภาพต่ำ

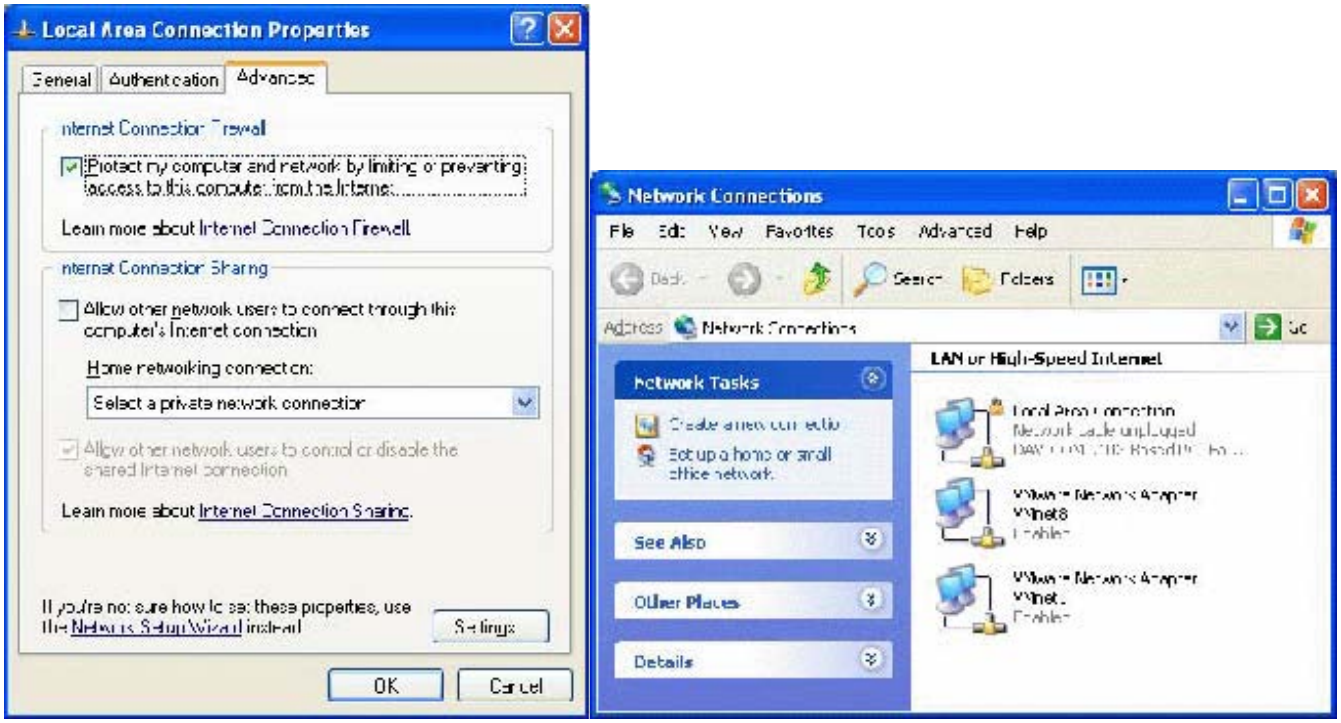
- แต่ละบริการมักจะต้องการโปรเซสของตนเอง
- สามารถขยายตัวได้ยาก

3. Stateful Inspection Technology

Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของแพ็กเกจ และข้อมูลที่ได้จากแพ็กเกจก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้มาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าเป็นแพ็กเกจที่ติดต่อเข้ามาใหม่หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อ

วิธีการเปิดใช้งานไฟร์วอลล์ XP




Local Area Connection Properties
General
Authentication
Advanced
Internet Connection Firewall
Protect my computer and network by limiting or preventing access to this computer from the Internet
Learn more about Internet Connection Firewall
Internet Connection Sharing
Allow other network users to connect through this computer's Internet connection
Home networking connection:
Select a private network connection
Allow other network users to control or disable the shared Internet connection
Learn more about Internet Connection Sharing.
If you're not sure how to set these properties, use the Network Setup Wizard instead.
Settings
OK
Cancel
Network Connections
File
Edit
View
Favorites
Tools
Advanced
Help
Back
Search
Folders
Address
Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
See Also
Other Places
Details
LAN or High-Speed Internet
Local Area Connection
Network cable unplugged
VMware Network Adapter VMnet8
Disabled
VMware Network Adapter VMnet1
Disabled