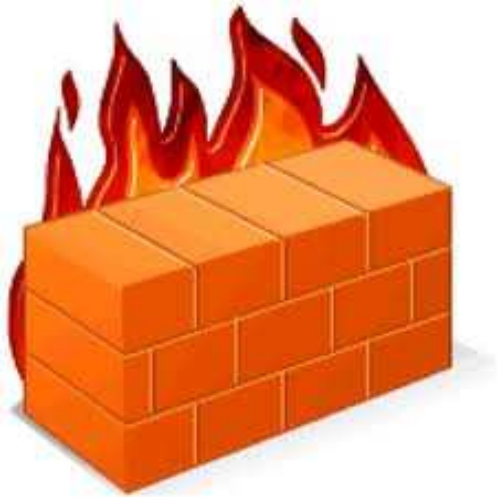
Firewall

บทที่ 5 ความรู้เกี่ยวกับ Firewall

ทำไมต้องใช้ Firewall

- องค์การต่างๆ มีระบบเครือข่ายภายใน
- เครือข่ายองค์การเชื่อมต่อกับเครือข่ายอินเตอร์เน็ต
  - ใครก็ได้ในองค์กรออกสู่อินเตอร์เน็ตได้
  - ใครก็ได้ในอินเตอร์เน็ตสามารถผ่านเข้ามาในเครือข่ายองค์กร
  - เป้าหมายของเครือข่าย ออกแบบมาให้แบ่งปันไม่ใช่ป้องกัน
- การที่ใครก็ได้สามารถผ่านเข้าออกย่อมไม่มีความปลอดภัย

Firewall คืออะไร

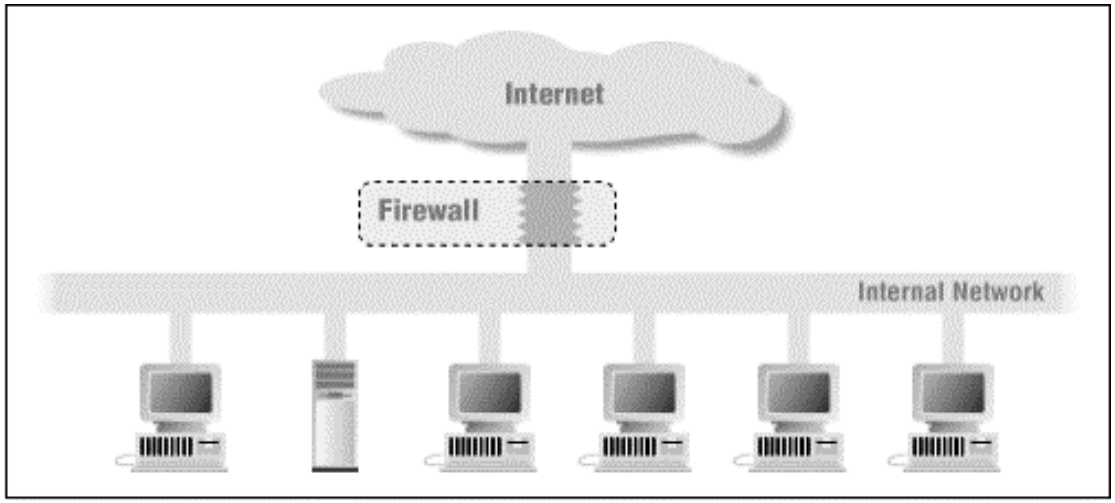


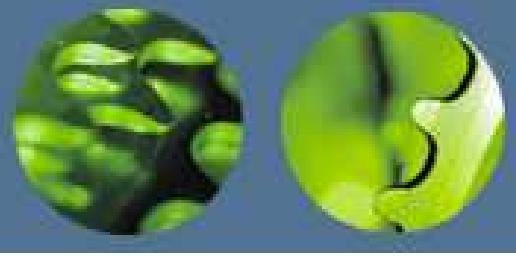
- ด้านการก่อสร้างแล้ว ไฟร์วอลล์ จะหมายถึง
  กำแพงที่เอาไว้ป้องกันไฟไม่ให้ลุกลามไปยังส่วนอื่นๆ

- ด้านคอมพิวเตอร์นั้นก็จะมีความหมายคล้ายๆ กันก็คือ
  เป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเตอร์เน็ตหรือเน็ตเวิร์คภายนอก

Firewall กับหน้าที่หลัก

- ไฟร์วอลล์ เป็นคอมโพเน็นท์หรือกลุ่มของคอมโพเน็นท์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเน็ตเวิร์คภายนอก กับ ภายใน
- คอมโพเน็นท์นั้นอาจจะเป็นเราเตอร์ คอมพิวเตอร์ หรือเน็ตเวิร์ค ประกอบกันก็ได้ ขึ้นอยู่กับวิธีการ



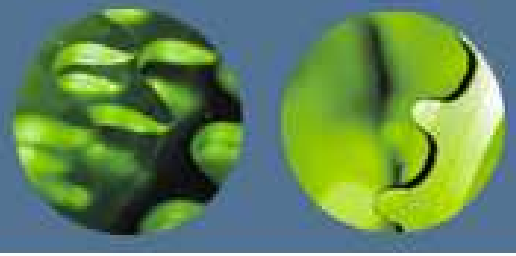


Firewall ช่วยอะไรได้

- บังคับใช้นโยบายด้านความปลอดภัย กำหนดกฎว่าจะอนุญาตหรือไม่ให้ใช้เซอร์วิสชนิดใด
- ทำให้การดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่ายขึ้น
- บันทึกข้อมูล กิจกรรมต่างๆ ที่ผ่านเข้าออกเน็ตเวิร์กได้อย่างมีประสิทธิภาพ
- ป้องกันเน็ตเวิร์คส่วนใหญ่จากการเข้าถึงของภายนอก
  เช่น ให้เรียกเข้ามาได้เฉพาะเว็บ
- ไฟร์วอลล์บางชนิด สามารถป้องกันไวรัส หรือการลักลอบผ่านเครือข่ายได้

อะไรที่ไฟร์วอลล์ช่วยไม่ได้

- อันตรายที่เกิดจากเน็ตเวิร์กภายใน ไม่สามารถป้องกันได้เพราะอยู่หลังไฟร์วอลล์ เช่น การ Dial-up เข้ามายังเน็ตเวิร์กภายใน โดยไม่ได้ผ่านไฟร์วอลล์
- อันตรายจากวิธีใหม่ๆ ที่เกิดขึ้น ทุกวันนี้มีการพบช่องโหว่ใหม่ๆ เกิดขึ้นทุกวัน ไฟร์วอลล์จึงป้องกันตลอดไปไม่ได้
- ไวรัส ถึงแม้จะมีไฟร์วอลล์บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ยังไม่มีไฟร์วอลล์ชนิดใดที่สามารถตรวจสอบไวรัสได้ในทุกๆ โปรโตคอล

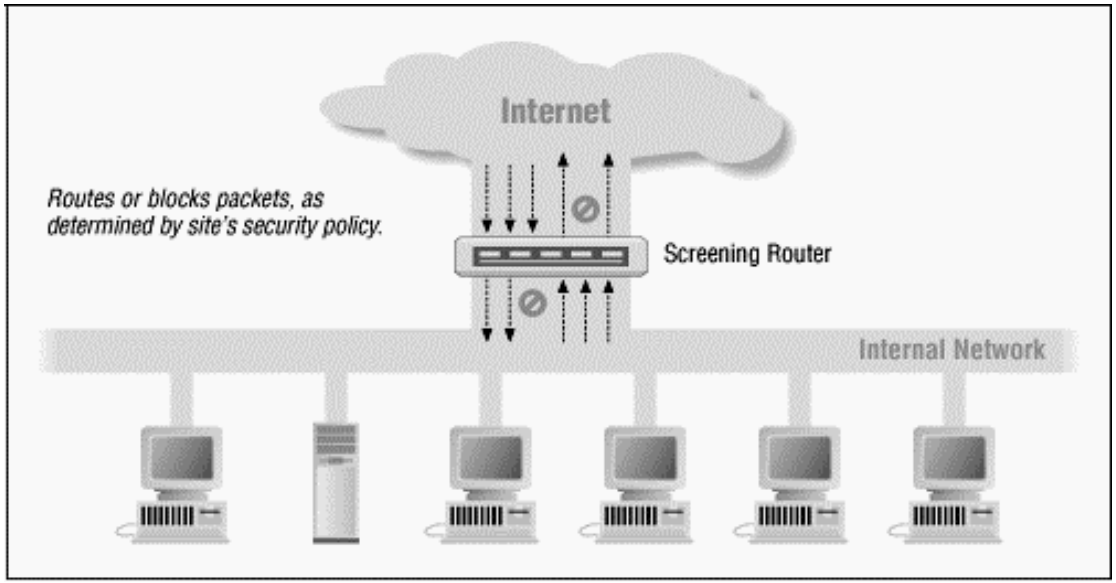


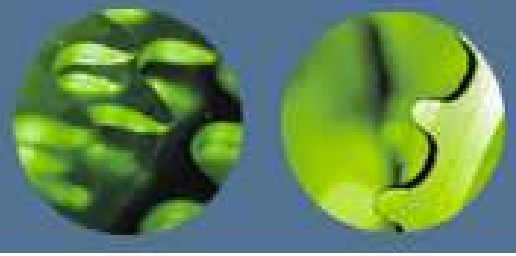
ชนิดของไฟร์วอลล์

- **Packet Filtering**
- **Proxy Service**
- **Stateful Inspection**

Packet Filtering

- **Packet Filter คือ เราเตอร์ที่ทำการหาเส้นทางและส่งต่อ (Route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (Header) ของแพ็กเก็ตที่ผ่านเข้ามาเทียบกับกฎ (Rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (Drop) แพ็กเก็ตนั้นไป หรือว่าจะยอม (Accept) ให้แพ็กเก็ตนั้นผ่านไปได้**





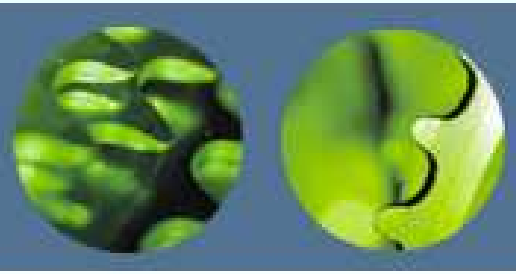
Packet Filtering(ต่อ)

- ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของอินเตอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (Transport Layer) ในอินเตอร์เน็ตโมเดล
- ในอินเตอร์เน็ตเลเยอร์จะมีแอตทริบิวต์ที่สำคัญต่อ Packet Filtering ดังนี้
  - ไอพีต้นทาง
  - ไอพีปลายทาง
  - ชนิดของโปรโตคอล (TCP UDP และ ICMP)
- ในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ
  - พอร์ตต้นทาง
  - พอร์ตปลายทาง
  - แฟล็ก (Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต TCP)
  - ชนิดของ ICMP message (ในแพ็กเก็ต ICMP)

Packet Filtering(ต่อ)

- **พอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP จะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วย เช่น พอร์ต 80 หมายถึง HTTP, พอร์ต 21 หมายถึง FTP เป็นต้น**

ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมได้ เช่น ห้ามแพ็กเก็ตทุกชนิดจาก crack.cracker.net เข้ามายังเน็ตเวิร์ก 203.154.207.0/24 , ห้ามแพ็กเก็ตที่มีไอพีต้นทางอยู่ในเน็ตเวิร์ก 203.154.207.0/24 ผ่านเราเตอร์



Packet Filtering การนำไปใช้

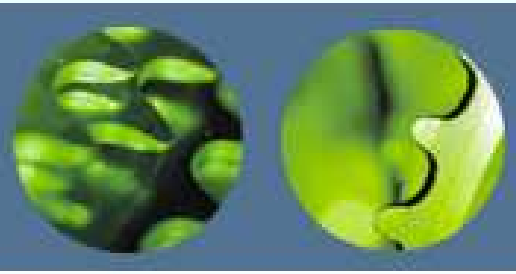
- **Packet Filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม คือ**
  - **เราเตอร์ที่มีความสามารถในการทำ Packet Filtering**
  - **คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์**

เปรียบเทียบการนำไปใช้

	ข้อดี	ข้อเสีย
เราเตอร์	ประสิทธิภาพสูงมีจำนวนอินเตอร์เฟสมาก	เพิ่มเติมฟังก์ชันการทำงานได้ยาก, อาจต้องการหน่วยความจำมาก
คอมพิวเตอร์ทำหน้าที่เป็นเราเตอร์	เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด	ประสิทธิภาพปานกลาง,จำนวนอินเตอร์เฟสน้อย,อาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ข้อดีข้อเสียของ Packet Filtering

- ข้อดี
  - ไม่ขึ้นกับแอพพลิเคชัน
  - มีความเร็วสูง
  - รองรับการขยายตัวได้ดี
- ข้อเสีย
  - บางโปรโตคอลไม่เหมาะสมกับการใช้ Packet Filtering เช่น FTP, ICQ

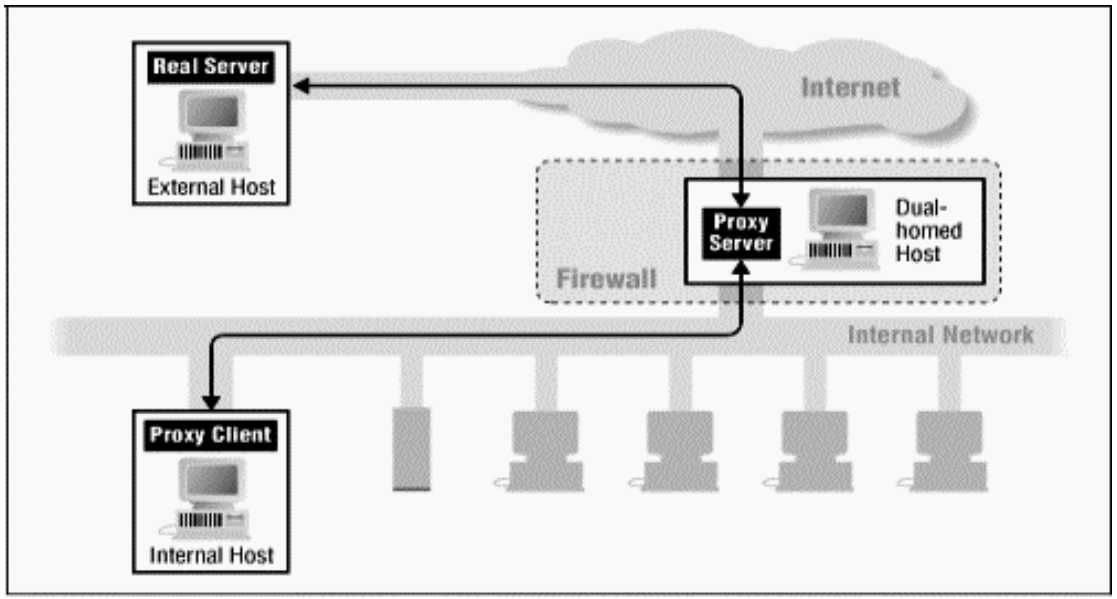


Proxy

- **Proxy หรือ Application Gateway เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก**
- **ทำหน้าควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก**
- **Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)**

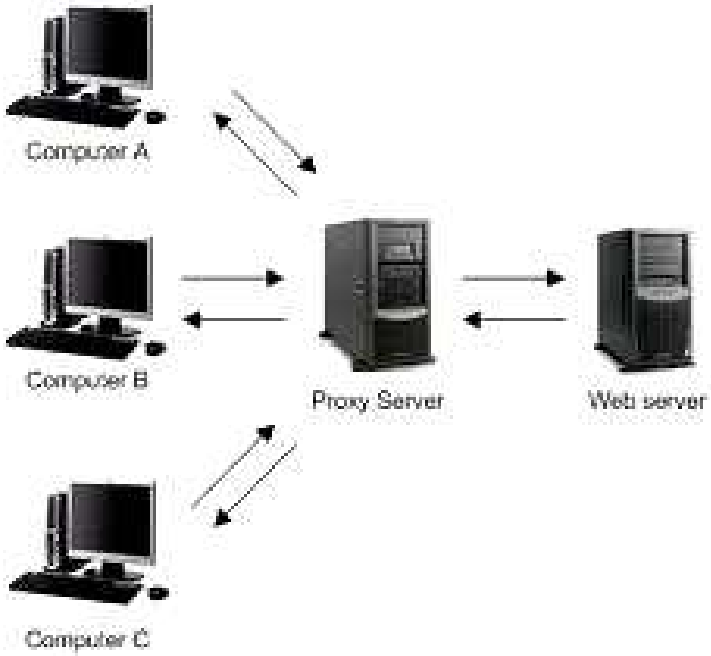
การทำงาน Proxy

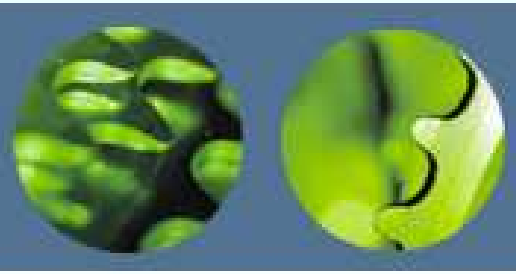
- เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก จะทำการติดต่อไปยัง Proxy ก่อน
- ไคลเอนต์จะเจรจา (negotiate) กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้
- เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง
- Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่



ข้อดีข้อเสียของ *Proxy*

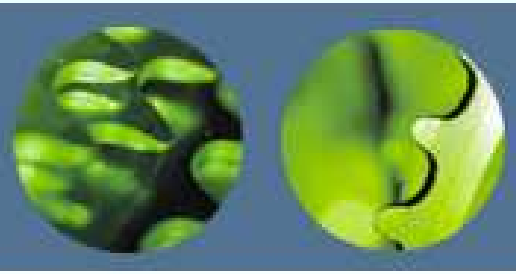
- ข้อดี
  - มีความปลอดภัยสูง
  - รู้จักข้อมูลในระดับแอพพลิเคชัน
- ข้อเสีย
  - ประสิทธิภาพต่ำ
  - แต่ละบริการมักจะต้องการโปรเซสของตนเอง
  - สามารถขยายตัวได้ยาก





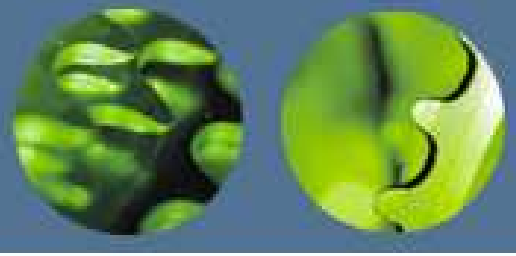
Statefull Inspection Technology

- **Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering**
- **โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของแพ็กเก็ต (message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว**



ตัวอย่างผลิตภัณฑ์

- ผลิตภัณฑ์ทางการค้าที่ใช้ Stateful Inspection Technology ได้แก่
  - Check Point Firewall-1
  - Cisco Secure Pix Firewall
  - SunScreen Secure Net
- และส่วนที่เป็น open source แจกฟรี ได้แก่
  - NetFilter ใน Linux (iptables ในลีนุกซ์เคอร์เนล 2.3 เป็นต้นไป)

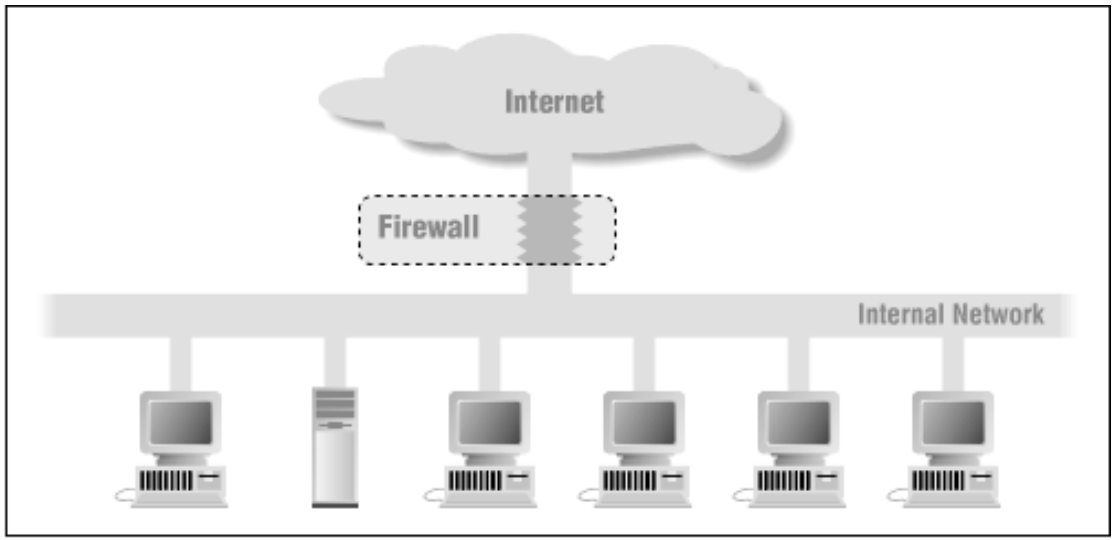


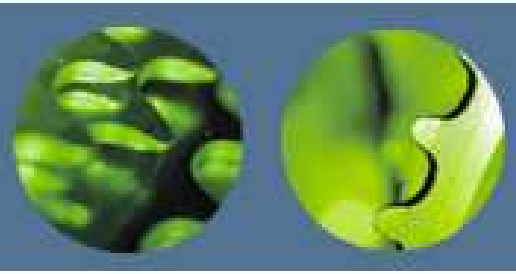
Firewall Architecture

- **Single Box Architecture**
- **Screened Host Architecture**
- **Multi Layer Architecture**
- **Screened Subnet Architecture**

Single Box Architecture

- เป็น Architecture แบบง่ายๆ ที่มีคอมโพเน็นต์ทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเน็ตเวิร์กภายในกับเน็ตเวิร์กภายนอก ข้อดีของวิธีนี้ก็คือการที่มีเพียงจุดเดียวที่หน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูล ทำให้ดูแลได้ง่าย เป็นจุดสนใจในการดูแลความปลอดภัยเน็ตเวิร์ก ในทางกลับกันข้อเสียของวิธีนี้ก็คือ การที่มีเพียงจุดเดียวนี้ ทำให้มีความเสี่ยงสูง หากมีการคอนฟิกูเรชันผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อย การผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้

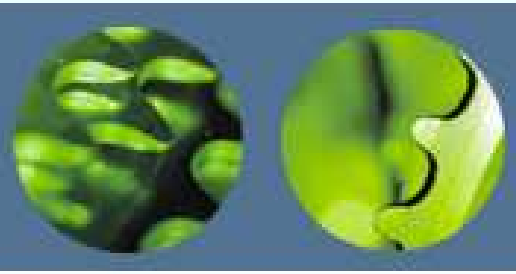




Single Box Architecture(ต่อ)

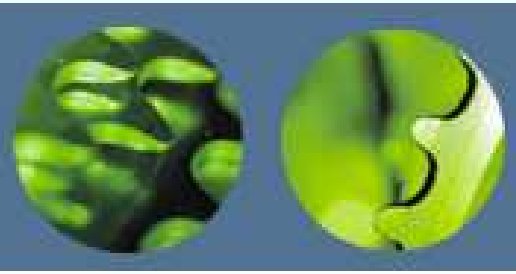
คอมโพเน็นต์ที่ใช้ใน Architecture นี้อาจเป็น

- Screening Router
- Dual-Homed Host
- Multi-purposed Firewall Box



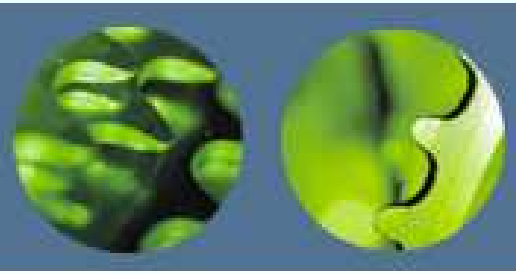
Single Box Architecture(ต่อ)

- Screening Router เราสามารถใช้เราเตอร์ทำ Packet Filtering ได้ วิธีนี้จะทำให้ประหยัดค่าใช้จ่าย Architecture แบบนี้เหมาะสำหรับ
  - เน็ตเวิร์กที่มีการป้องกันความปลอดภัยในระดับของโฮสต์ (Host security) เป็นอย่างดีแล้ว
  - มีการใช้โปรโตคอลไม่มาก และโปรโตคอลที่ใช้ก็เป็นโปรโตคอลที่ไม่ซับซ้อน
  - ต้องการไฟร์วอลล์ที่มีความเร็วสูง



Single Box Architecture(ต่อ)

- **Dual-Homed Host**
- **เราสามารถใช้ Dual-Homed Host (คอมพิวเตอร์ที่มีเน็ตเวิร์กอินเตอร์เฟสอย่างน้อย 2 อัน) ใช้การบริการเป็น Proxy ให้กับเครื่องภายในเน็ตเวิร์ก Architecture แบบนี้เหมาะสำหรับ**
  - **เน็ตเวิร์กที่มีการใช้งานอินเตอร์เน็ตค่อนค่างน้อย**
  - **เน็ตเวิร์กที่ไม่ได้มีข้อมูลสำคัญๆ**

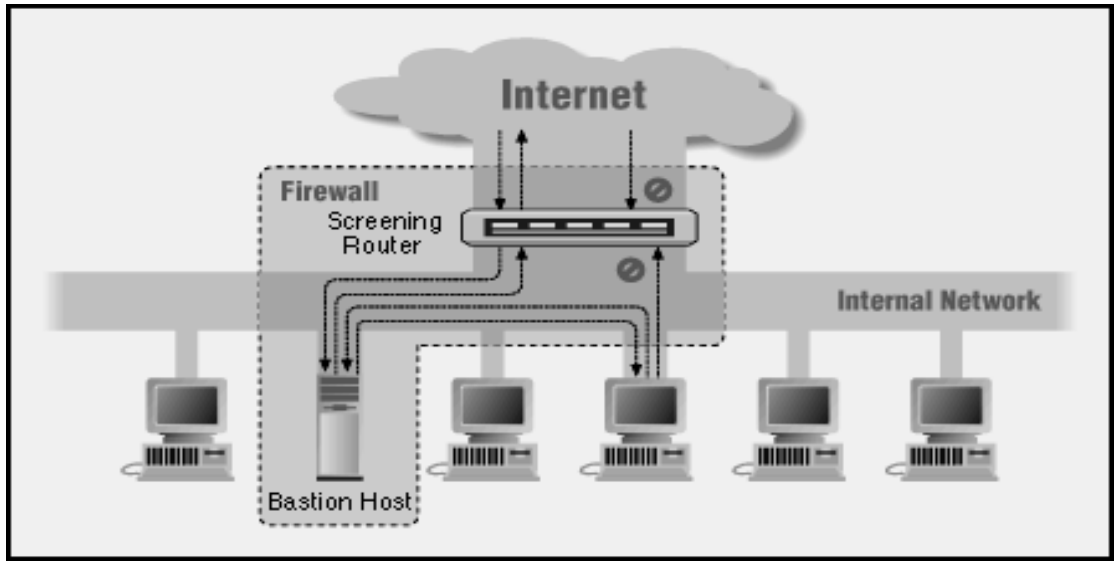


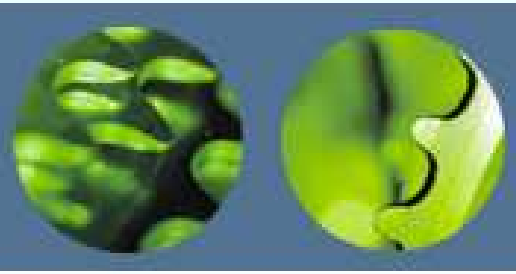
Single Box Architecture(ต่อ)

- **Multi-purposed Firewall Box**
- **มีผลิตภัณฑ์หลายชนิดที่ผลิตออกมาเป็นกล่องๆ เดียว ซึ่งทำหน้าที่ได้หลายอย่าง ทั้ง Packet Filtering, Proxy แต่ก็อย่าลืมว่านี่คือ Architecture แบบชั้นเดียว ซึ่งถ้าพลาดแล้วก็จะเสียหายทั้งเน็ตเวิร์กได้**

Screened Host Architecture

- Screened Host Architecture จะมีโฮสต์ซึ่งให้บริการ Proxy เหมือนกับใน Single Box Architecture ที่เป็น Dual-homed Host แต่จะต่างกันตรงที่ว่า โฮสต์นั้นจะอยู่ภายในเน็ตเวิร์ก ไม่ต่ออยู่กับเน็ตเวิร์กภายนอกอื่นๆ
- Filtering ช่วยบังคับให้เครื่องภายในเน็ตเวิร์กต้องติดต่อเซอร์วิสผ่าน Proxy โดยไม่ยอมให้ติดต่อใช้เซอร์วิสจากภายนอกโดยตรง
- ให้ภายนอกเข้าถึงได้เฉพาะ Bastion host



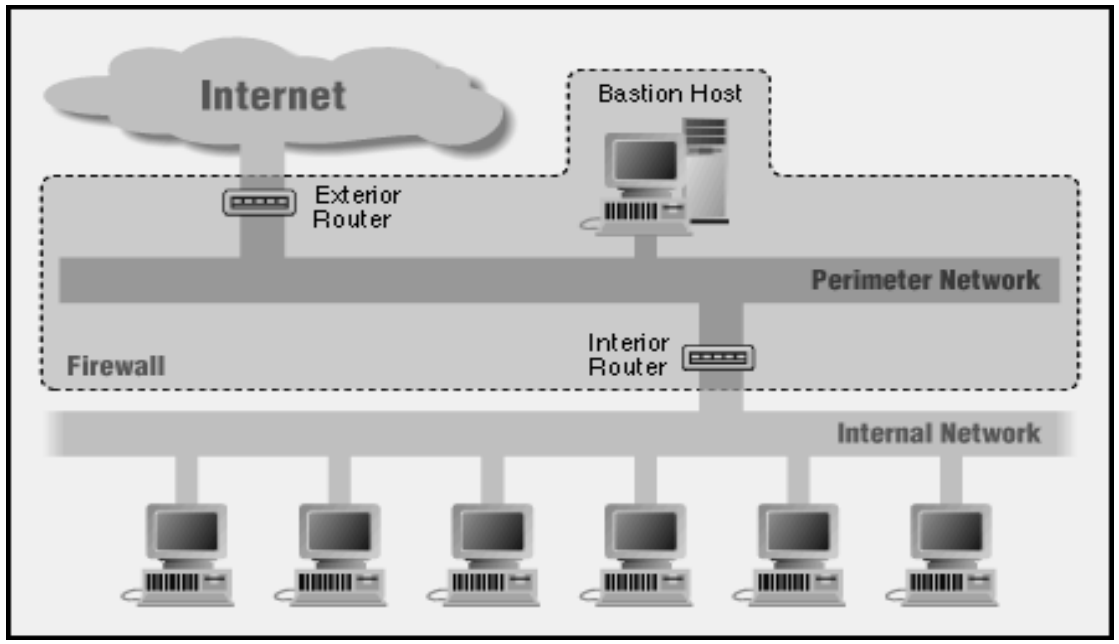


Screened Host Architecture(ต่อ)

- **Architecture นี้เหมาะสำหรับ**
  - เน็ตเวิร์กที่มีการติดต่อกับเน็ตเวิร์กภายนอกน้อย
  - เน็ตเวิร์กที่มีการป้องกันความปลอดภัยในระดับของโฮสต์เป็นอย่างดีแล้ว

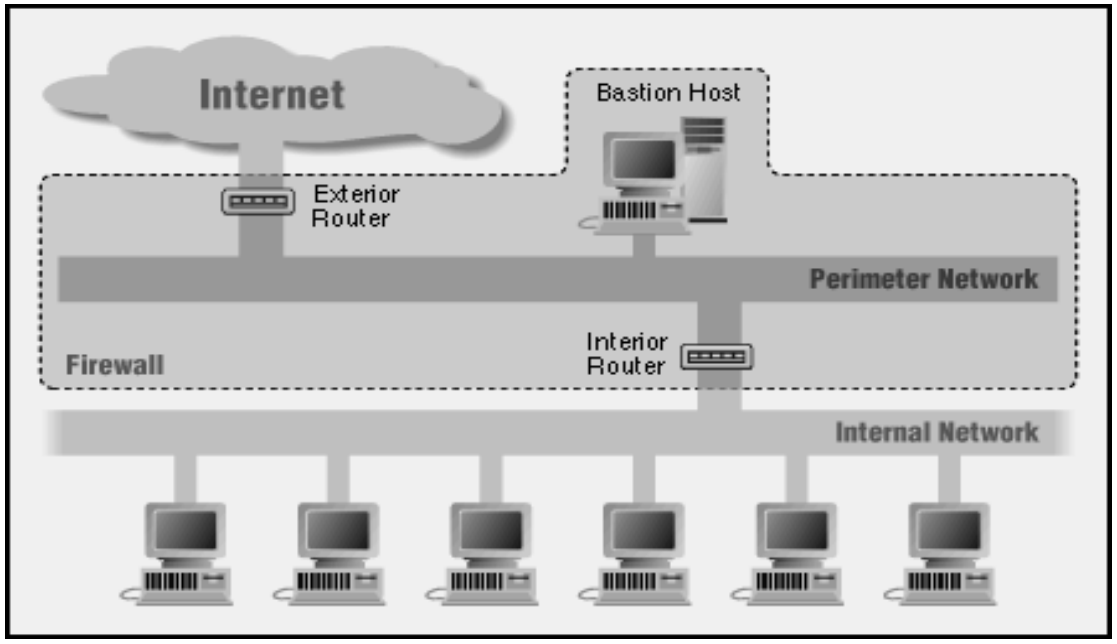
Multi Layer Architecture

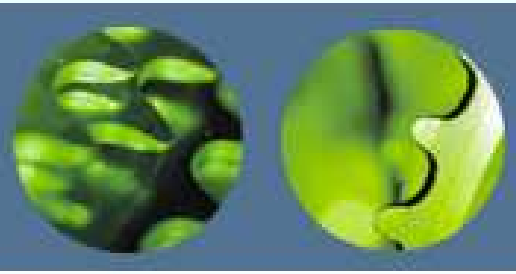
- สถาปัตยกรรมแบบหลายชั้น ไฟร์วอลล์จะเกิดขึ้นจากคอมโพเน็นต์หลายๆส่วนทำหน้าที่ประกอบกันขึ้นเป็นระบบ
- วิธีการนี้สามารถเพิ่มความปลอดภัยได้มาก เนื่องจากเป็นการลดความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น
- แต่ละชั้นนั้นมีการใช้เทคโนโลยีที่แตกต่างกัน เพื่อให้เกิดความหลากหลาย เป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง



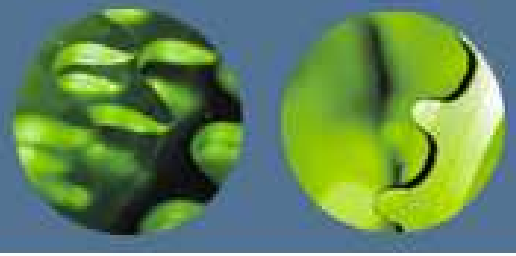
Screened Subnet Architecture

- **Screened Subnet Architecture เป็นสถาปัตยกรรมที่มีการเพิ่ม Perimeter Network เข้าไปกั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายในไม่ให้เชื่อมต่อกันโดยตรง ทำให้เน็ตเวิร์คภายในมีความปลอดภัยมากขึ้น**
- **คอมโพเน็นต์ของ Screened Subnet Architecture**
  - **Perimeter Network**
  - **Bastion Host**
  - **Interior Router**
  - **Exterior Router**





- Perimeter Network อยู่ระหว่างเน็ตเวิร์กภายนอกกับเน็ตเวิร์กภายใน ประโยชน์ของ Perimeter Network คือ การแบ่งเน็ตเวิร์กออกเป็นส่วนๆ ทำให้การไหลของข้อมูลถูกแบ่งออกเป็นส่วนๆ ตามเน็ตเวิร์ก
- Bastion Host ตั้งอยู่บน Perimeter Network ทำหน้าที่ให้บริการ Proxy กับเน็ตเวิร์กภายใน และให้บริการต่างๆ กับผู้ใช้บนอินเตอร์เน็ต
- Interior Router ตั้งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์กภายใน ทำหน้าที่ Packet Filtering ป้องกันเน็ตเวิร์กภายในจาก Perimeter Network
- Exterior Router ตั้งอยู่ระหว่างเน็ตเวิร์กภายนอกกับ Perimeter Network



End.