FIREWALL

Mr.Jantapong Boodluck

Electronic Computer Technology

King Mongkut's University of Technology North Bangkok

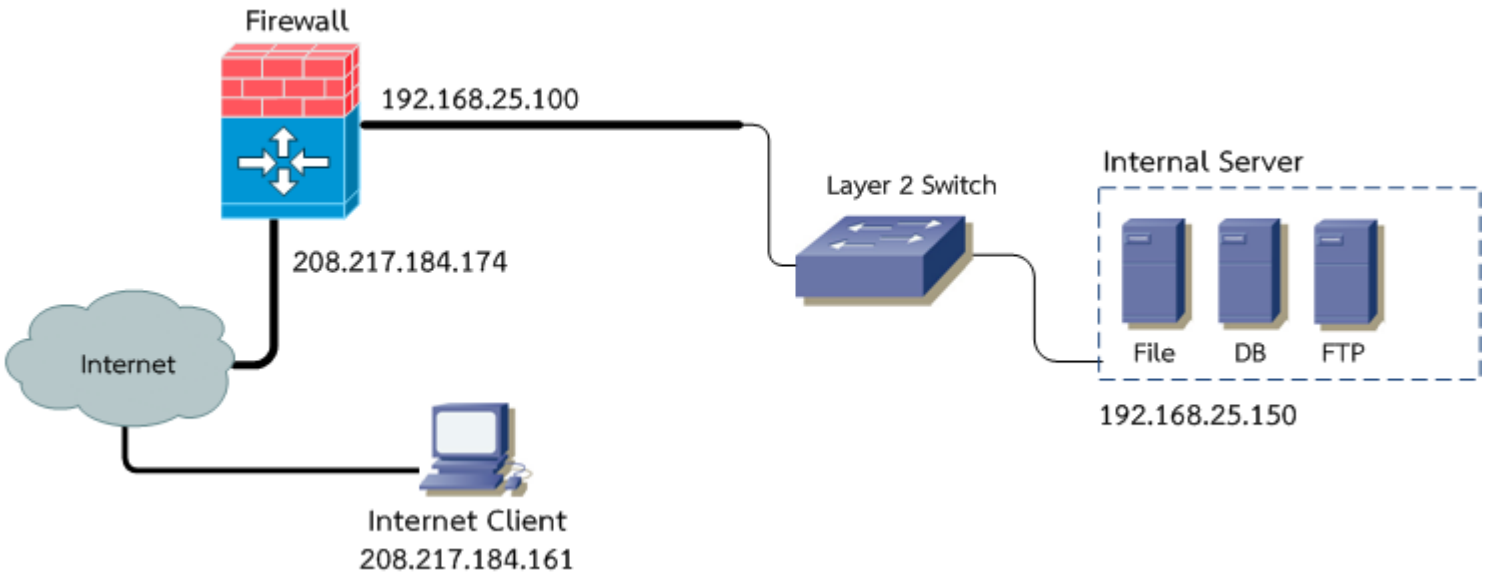
Outline

- Basic Firewall
- Type Of Firewall
- Network Security Policy
- Limitations of the Firewall
- Design Example

Basic Firewall

- **ไฟร์วอล** คือ ระบบควบคุมการเข้า-ออกเครือข่าย ซึ่งจะใช้สำหรับปกป้องเครือข่ายภายในองค์กรจากการโจมตีจากภายนอก
- **เหตุผลหลักที่มีการใช้ไฟร์วอล** ก็เพื่อให้ผู้ใช้ที่อยู่ภายในสามารถใช้บริการเครือข่ายภายในได้เต็มที่และใช้บริการเครือข่ายภายนอก เช่น อินเตอร์เน็ต ได้ด้วย
- ไฟร์วอลสามารถควบคุมการใช้เครือข่ายได้โดย**อนุญาต**หรือ**ไม่อนุญาต**ให้แพ็กเก็ตผ่านได้ ซึ่งแพ็กเก็ตที่อนุญาตให้ผ่านหรือไม่นั้นขึ้นอยู่กับนโยบายการรักษาความปลอดภัย (Security Policy) ที่กำหนดให้กับไฟร์วอล

Basic Firewall



- มีหน้าที่**ตรวจสอบข้อมูล**ที่ผ่านเข้าออกระบบ
- **ป้องกันผู้บุกรุก**ที่มาจากเครือข่ายภายนอก
- เป็นตัวคั่นกลางระหว่าง**เน็ตเวิร์กที่ไม่ไว้ใจ**และ**เน็ตเวิร์กที่ต้องการปกป้อง**
- ไฟร์วอลล์จะทำงานตาม “**กฎของไฟร์วอลล์**” ที่ผู้ดูแลระบบกำหนดไว้

Basic Firewall

- กฎไฟร์วอลล์จะกำหนดเป็นข้อๆ หรือเป็น**บรรทัด**
- มีกฎ**หลายบรรทัด**ทำให้ไฟร์วอลล์ทำงาน**ช้าลง**
- ผู้ออกแบบที่มีประสบการณ์จะออกแบบกฎให้จำนวนบรรทัดน้อย แต่มีประสิทธิภาพ
- ไฟร์วอลล์จะอยู่เกือบปลายสุดของเครือข่ายอินเทอร์เน็ต
- ไฟร์วอลล์ทำหน้าที่ส่งผ่าน (Forward) แพ็กเก็ต (Packet) ได้เหมือนกับเราเตอร์
- แต่แตกต่างคือ ไฟร์วอลล์ทำหน้าที่**กรองแพ็กเก็ต**ได้
- ส่วนเราเตอร์ต้องกำหนดค่า ACL (Access Control List)

Basic Firewall

- เมื่อมีแพ็กเก็ตวิ่งมา ไฟร์วอลล์จะตัดสินว่าควร **ให้ผ่าน** (Accept) หรือ **ทิ้งไป** (Deny)
- จะ**ตรวจสอบจากกฎที่กำหนด**ไว้
- หากตรงตามเงื่อนไขจะตัดสินตาม **Action** ว่าอนุญาต หรือไม่อนุญาต
- กฎข้อสุดท้ายมักกำหนดไว้ว่า “**ไม่อนุญาตทุกแพ็กเก็ต**” เพื่อความปลอดภัย

Benefits

ประโยชน์

- ใช้การกำหนดกฎให้กับ Firewall
- บันทึกข้อมูลที่ผ่านเข้าออกอย่างมีประสิทธิภาพ
- ป้องกันจากการเข้าถึงที่ไม่ได้รับอนุญาตจากภายนอก
- สามารถป้องกันไวรัสได้ (รุ่นใหม่ๆ)

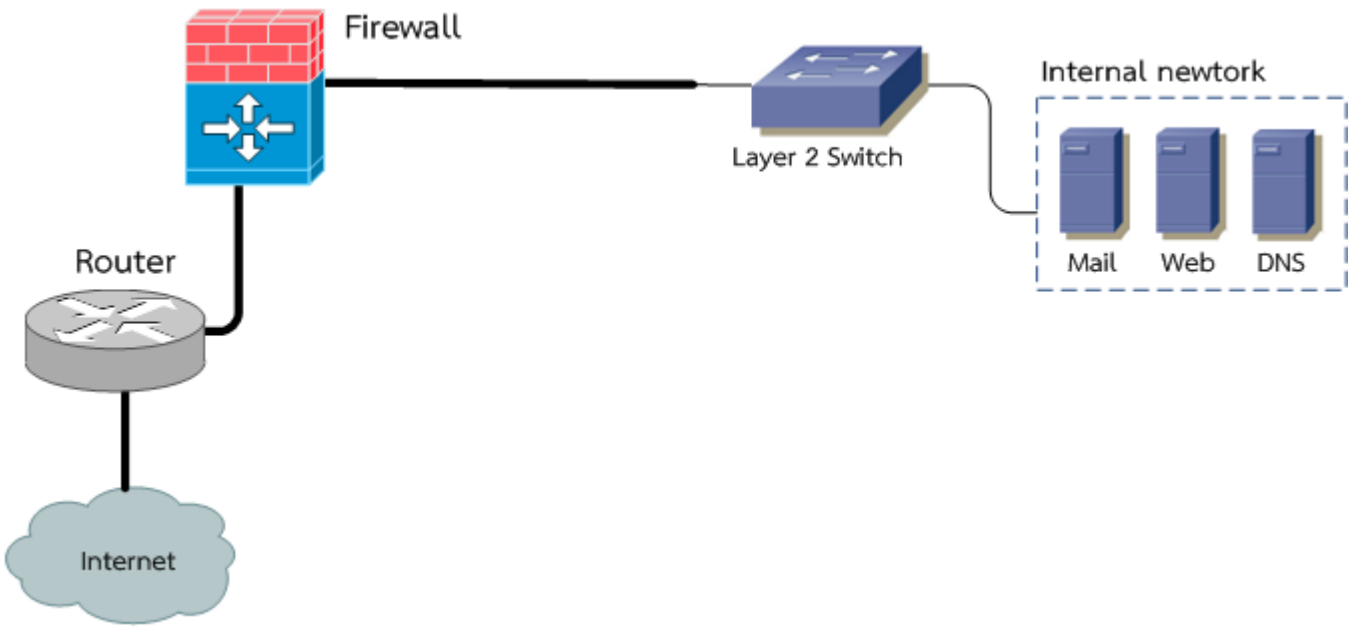
Type Of Firewall

Network Firewall

- Packet filtering Firewall
- Stateful Firewall
- Application Firewall

Personal Firewall

Packet filtering Firewall



- พิจารณาฟิลด์ต่างๆที่สำคัญบนเฮดเดอร์ของแพ็กเก็ต เช่น Protocol , Port เป็นต้น
- ตรวจสอบ IP Address และ Port ที่อยู่ต้นทาง และปลายทาง

Packet filtering Firewall

- ในการพิจารณาเฮดเดอร์ Packet Filtering จะตรวจสอบในระดับของ Network Layer และ Transport Layer

Network Layer

- ไอพีต้นทาง, ไอพีปลายทาง
- ชนิดของโปรโตคอล

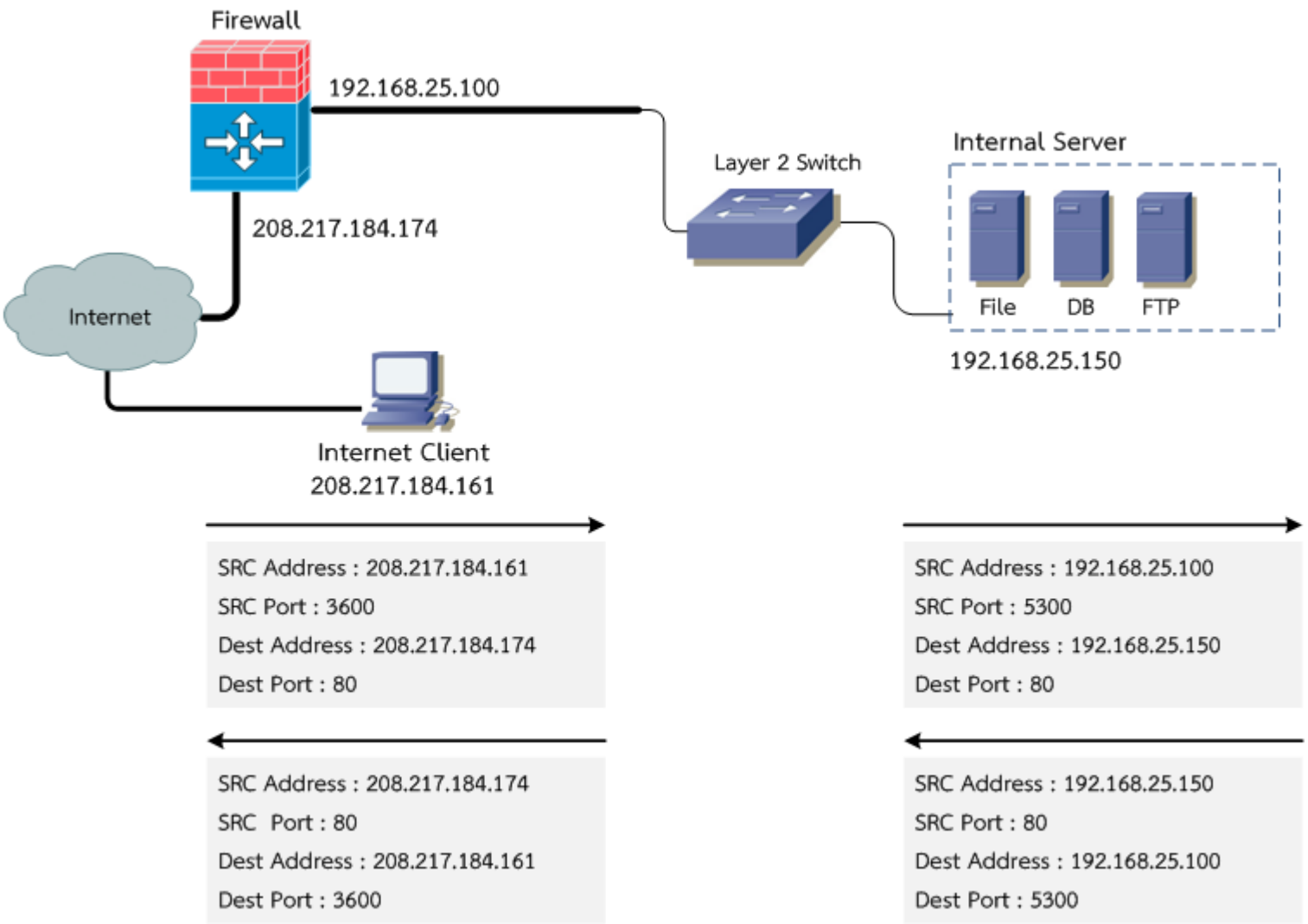
Transport Layer

- พอร์ตต้นทาง, พอร์ตปลายทาง
- แฟล็ก (Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต TCP)

Stateful Firewall

- เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering
- เพิ่มความสามารถในการพิจารณาข้อมูลใน Flag
- นำแพ็กเก็ตที่วิ่งผ่านและแพ็กเก็ตที่เคยวิ่งผ่าน เก็บใน **State-Table** มาพิจารณา
- หาก**มีใน State-Table ก็อนุญาตให้ผ่าน**ได้
- หาก**ไม่มีใน State-Table** จะต้อง**ตรวจสอบจากกฎที่ละข้อ** เมื่อพบว่าให้ผ่านได้ก็จะสร้าง State-Table ใหม่
- **ทำงานเร็วกว่า** Packet Filtering

Application Firewall Or Proxy Firewall



Application Firewall Or Proxy Firewall

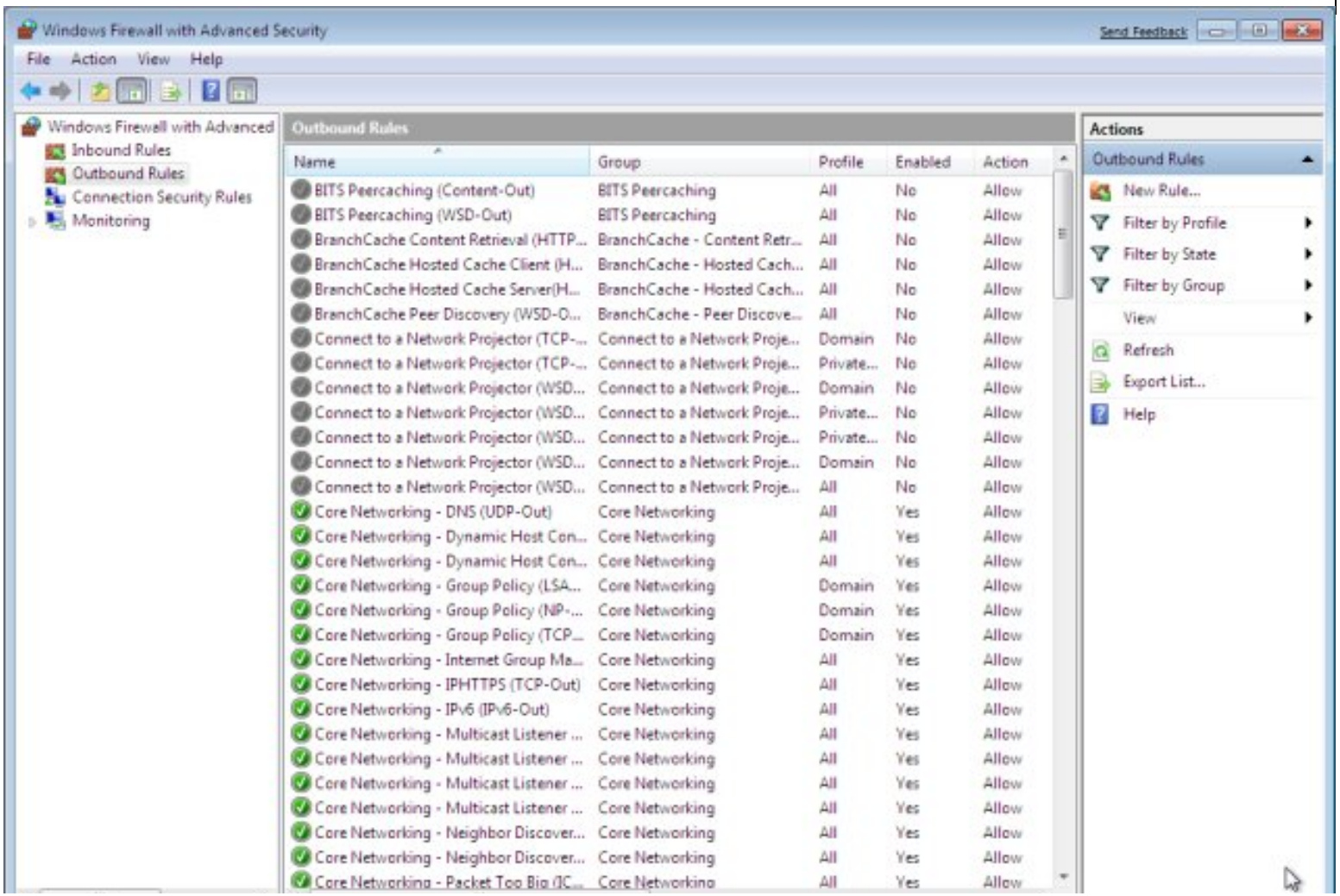
- สามารถจำกัดให้บาง IP สามารถเข้า Application ได้บางส่วนหรือทั้งหมด
- Proxy Server, Web Proxy, SMTP Proxy, Telnet Proxy
- สามารถสร้าง TCP Connection กับโฮสต์ปลายทางขึ้นเองใหม่
- ปลอดภัยมาก เพราะตรวจสอบข้อมูลในระดับ Application Layer

Application Layer เป็นเลเยอร์บนสุดที่ทำงานใกล้ชิดกับผู้ใช้ การทำงานของ เลเยอร์นี้จะเกี่ยวข้องกับโปรโตคอลต่างๆ มากมาย มีบริการทางด้านโปรแกรมประยุกต์ต่างๆ ได้แก่ E-Mail, File Transfer, HTTP เป็นต้น

Personal Firewall

- ไฟร์วอลล์เฉพาะเครื่อง
- ป้องกันการเชื่อมต่อจาก IP อื่น
- สามารถเปิดเฉพาะ Port ที่เราต้องการให้ติดต่อ
- ZoneAlarm Pro, Outpost Firewall, Norman Personal Firewall, eConceal Pro, Webroot Desktop Firewall, Injoy Firewall, SurfSecret Firewall

Personal Firewall

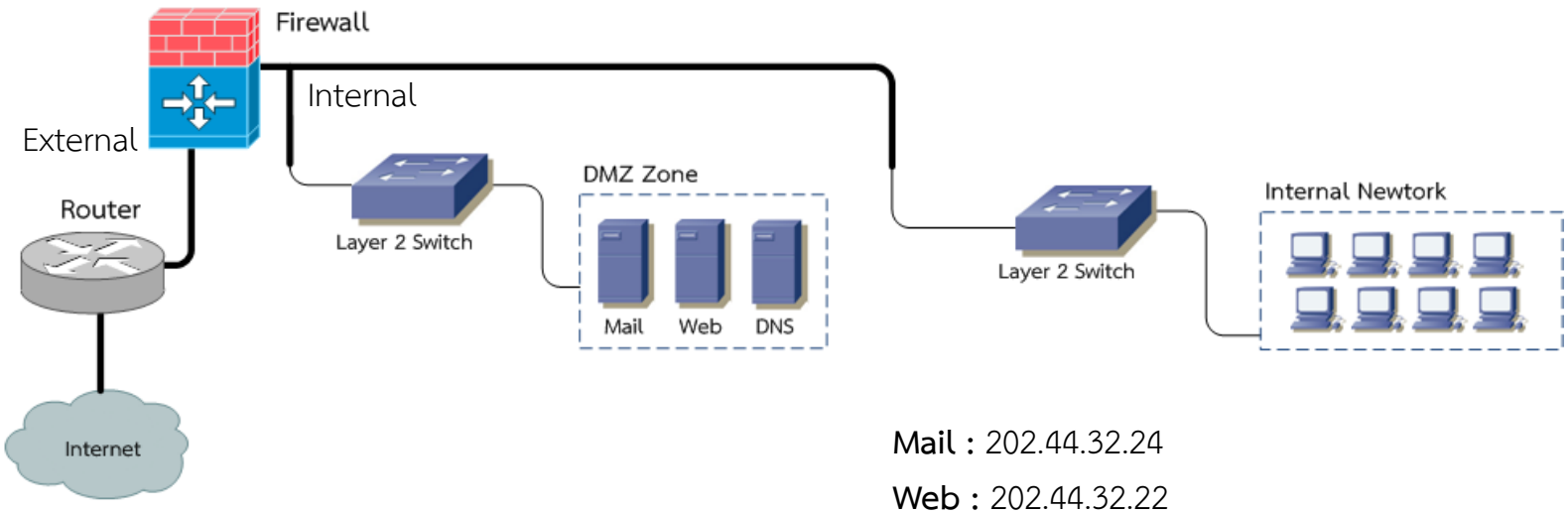


Network Security Policy

- Network Security Policy นับเป็นสิ่งที่สำคัญที่สุดสำหรับการใช้งานไฟร์วอล แม้ว่า Firewall จะมีประสิทธิภาพ หากมีนโยบายการรักษาความปลอดภัยที่หละหลวม Firewall ก็ไม่มีประโยชน์มากนัก
- ดังนั้นควรกำหนดนโยบายที่สามารถควบคุมหรือป้องกันทราฟิกที่อาจมีผลกระทบต่อการใช้งานเครือข่ายให้มากที่สุด แล้วนำไปบังคับใช้กับไฟร์วอล
- ซึ่งกฎที่บังคับใช้นโยบายการรักษาความปลอดภัยในไฟร์วอลนั้นจะเรียกว่า ACL (Access Control List) หรือ Firewall Rule

Network Security Policy

<u>ตัวอย่าง</u> การกำหนดนโยบายรักษาความปลอดภัย โดยสมมติว่าโครงสร้างของเครือข่ายเป็นดังรูปต่อไปนี้



Mail : 202.44.32.24

Web : 202.44.32.22

DNS : 202.44.32.29

Internal Network : 192.168.100.0/24

Network Security Policy

- โดย DMZ (Demilitarized Zone) ประกอบด้วย เว็บเซิร์ฟเวอร์ เมล-เซิร์ฟเวอร์ และ DNS เซิร์ฟเวอร์
- โดยผู้ใช้เครือข่ายภายใน สามารถใช้บริการจากภายนอกดังนี้ HTTP, HTTPS, FTP, Telnet, SSH, DNS, SMTP, POP3
- ส่วนผู้ใช้จากอินเทอร์เน็ตหรือภายนอกนั้นสามารถใช้บริการจาก DMZ ได้ดังนี้ DNS, HTTP, HTTPS, SMTP จากนโยบายนี้เราสามารถเขียน ACL ได้ดังนี้

Network Security Policy

Rule	Source	Destination	Service (Port)	Action	Description
1	Any	202.44.32.22	HTTP (80) HTTPS (443)	Allow	อนุญาตให้ผู้ใช้จากทั้งภายในและอินเทอร์เน็ตเข้ามาใช้บริการเว็บเซอร์เวอร์
2	Any	202.44.32.24	SMTP (25) POP3 (110) IMAP (143)	Allow	อนุญาตให้ผู้ใช้จากทั้งภายในและอินเทอร์เน็ตเข้ามาใช้บริการเมล์เซิร์ฟเวอร์

Network Security Policy

Rule	Source	Destination	Service (Port)	Action	Description
3	Any	202.44.32.29	DNS (53)	Allow	อนุญาตให้ผู้ใช้จากทั้งภายในและอินเทอร์เน็ตเข้ามาใช้บริการ DNS Server
4	202.44.32.24	Any	SMTP (25)	Allow	อนุญาตให้เมลเซิร์ฟเวอร์รับ - ส่งกับเมลเซิร์ฟเวอร์อื่นที่อยู่บนอินเทอร์เน็ตหรือภายใน
5	202.44.32.29	Any	DNS (53)	Allow	อนุญาตให้ DNS Server คิวรี DNS Server อื่นที่อยู่บนอินเทอร์เน็ตหรือภายใน

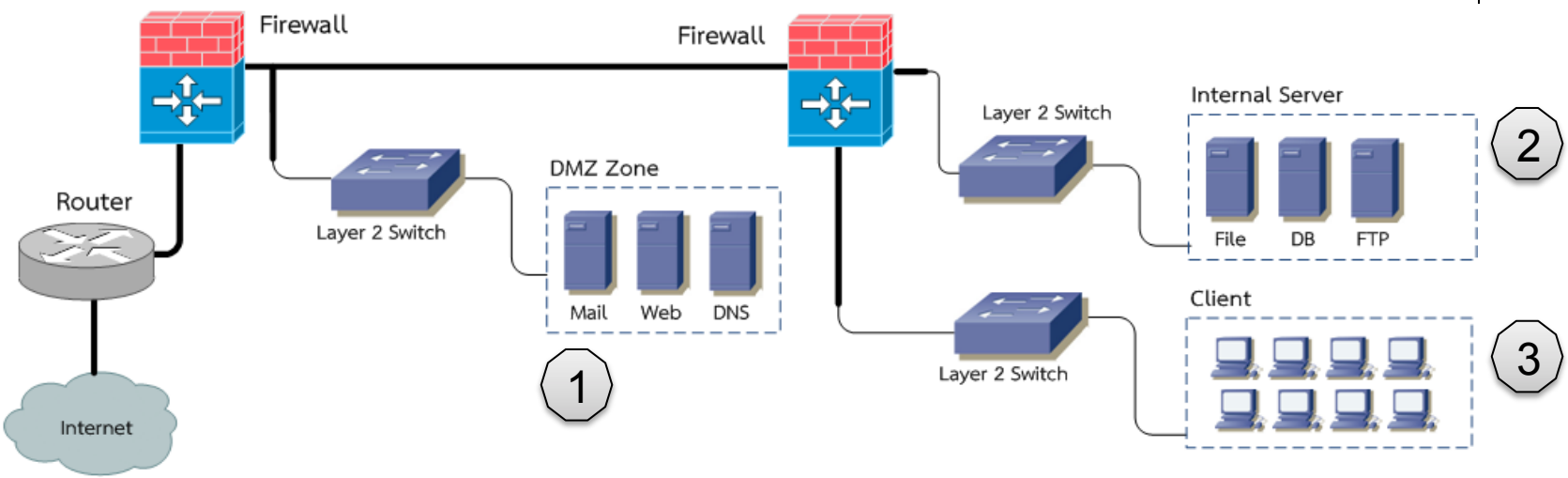
Network Security Policy

Rule	Source	Destination	Service (Port)	Action	Description
6	192.168.100.0/24	Any	HTTP (80) HTTPS (443) FTP (20-21) Telnet (23) SSH (22) SMTP (25) POP3 (110) IMAP4 (143)	Allow	อนุญาตให้ผู้ใช้ภายในเครือข่ายใช้บริการดังกล่าวจากอินเทอร์เน็ตและ DMZ
7	Any	Any	Any	Deny	ถ้าไม่ตรงกับกฎที่กำหนดข้างบนให้ละทิ้งแพ็กเก็ตนั้น

Limitations of the Firewall

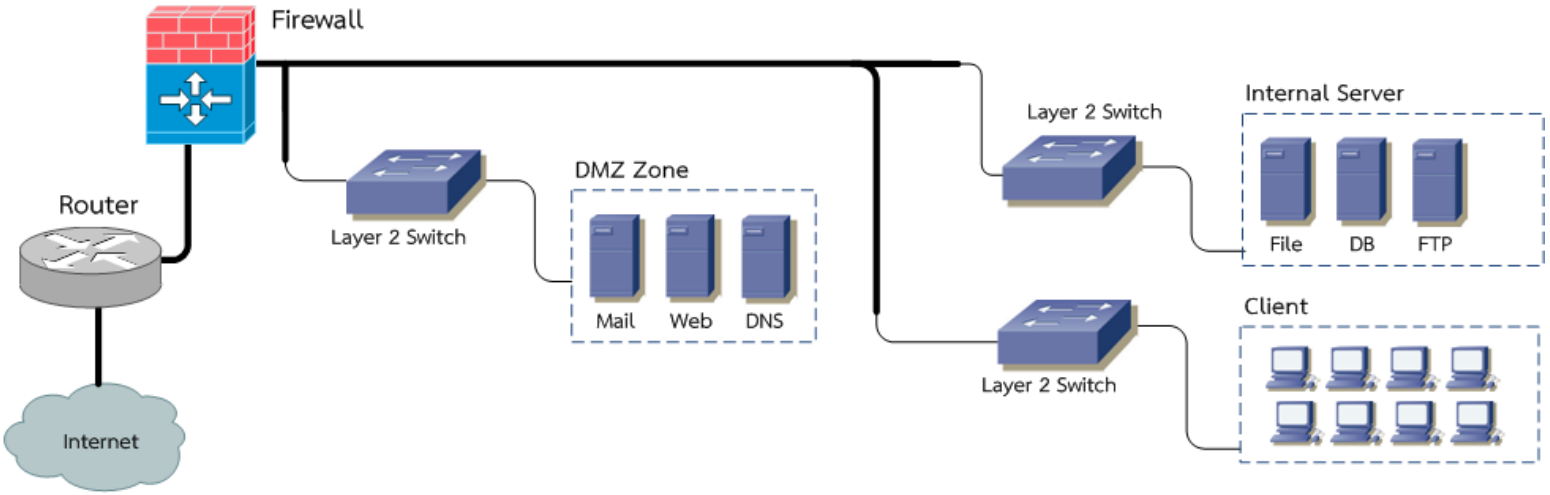
- Firewall ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่าน Firewall (เช่น การโจมตีจากภายในเครือข่ายเอง)
- ไม่สามารถป้องกันการโจมตีที่มากับ Application Protocols ต่างๆ (เรียกว่าการ Tunneling) หรือกับโปรแกรม Client ที่มีความล่อแหลมและถูกดัดแปลงให้กระทำการโจมตีได้ (โปรแกรมที่ถูกทำให้เป็น Trojan horse)

Design Example (2 Firewall)



- ใช้ไฟร์วอลล์ 2 ตัวโดยไฟร์วอลล์ตัวแรก จะทำหน้าที่กั้นระหว่างเครือข่ายภายนอกกับองค์กร และไฟร์วอลล์ตัวที่ 2 จะทำหน้าที่กั้นระหว่างเครือข่ายกลุ่มที่ 1 กลุ่มที่ 2 และกลุ่มที่ 3 โดยจะได้โครงสร้างตามรูป วิธีการออกแบบลักษณะนี้จะเรียกว่า Screening Subnet หรือบางทีก็เรียกว่า Three Homed Computer

Design Example (1 Firewall)

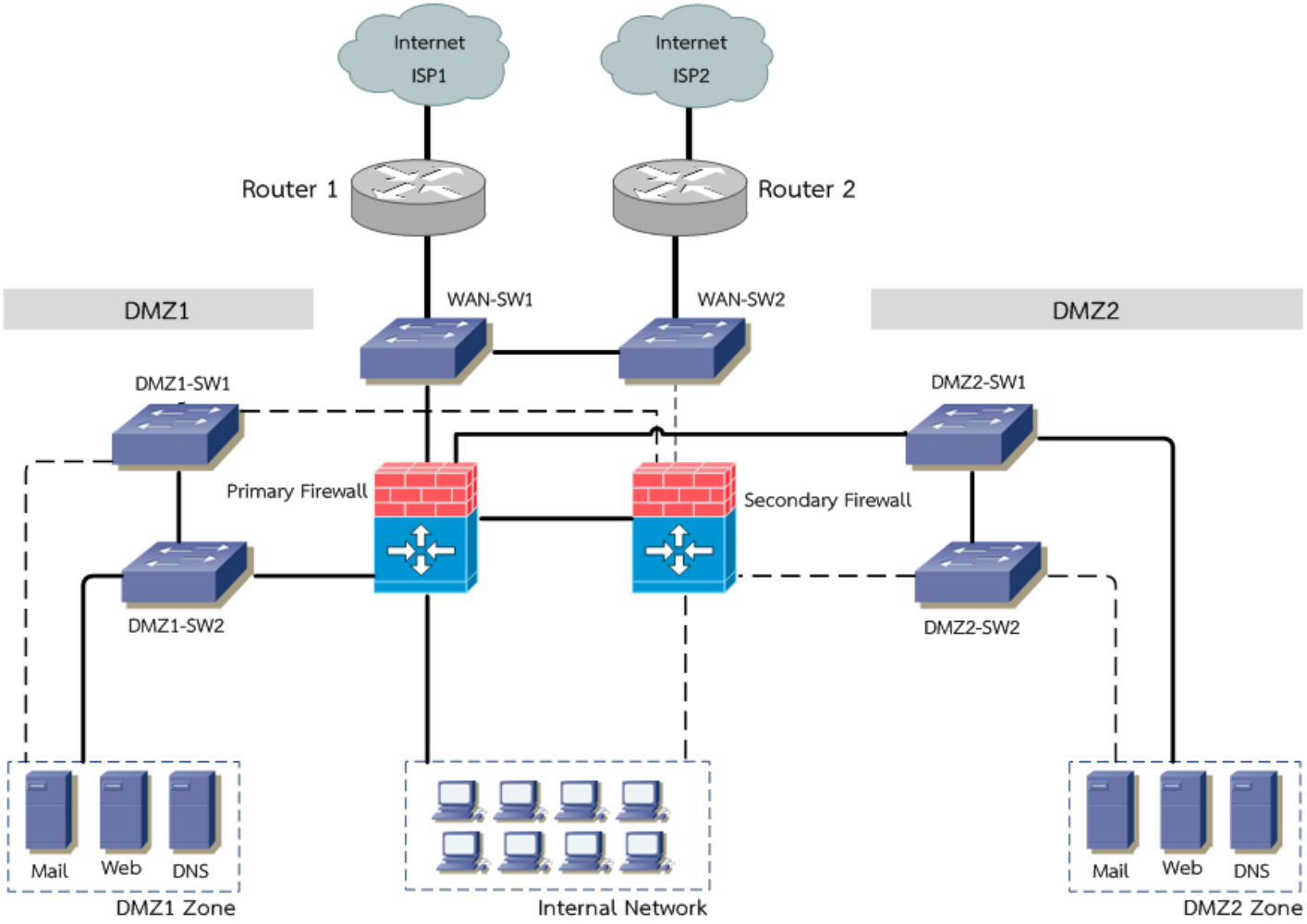


จะเห็นว่าเครือข่ายจะแบ่งออกเป็นเพียง 3 ส่วน คือ เครือข่ายภายนอกองค์กร เครือข่าย DMZ และเครือข่ายภายในองค์กร ซึ่งรวมเอาเซิร์ฟเวอร์ภายในและเครื่องไคลเอนต์เข้าไว้ด้วยกัน

Design Example

- รูปแบบนี้จัดว่าเป็นรูปแบบที่ประหยัด เพราะใช้ไฟร์วอลล์เพียงตัวเดียว แม้จะมีความเสี่ยงมากกว่าแบบที่ใช้ไฟร์วอลล์ 2 ตัวก็ตาม
- แต่หากเลือกใช้ไฟร์วอลล์ที่ดีหน่อยและมีการดูแลรักษาอย่างเคร่งครัด และถือได้ว่ามีความปลอดภัยที่เทียบเท่าได้กับไฟร์วอลล์ 2 ตัวเลยทีเดียว
- วิธีการออกแบบนี้จะเรียกว่า Screening Router หรือ Dual Homed Computer

Design Example (High Available Firewall)



Design Example

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

Resources

- อาจารย์ ธนัญชัย ตรีภาค สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons Inc, December 1995
- Security Focus
  - www.securityfocus.com