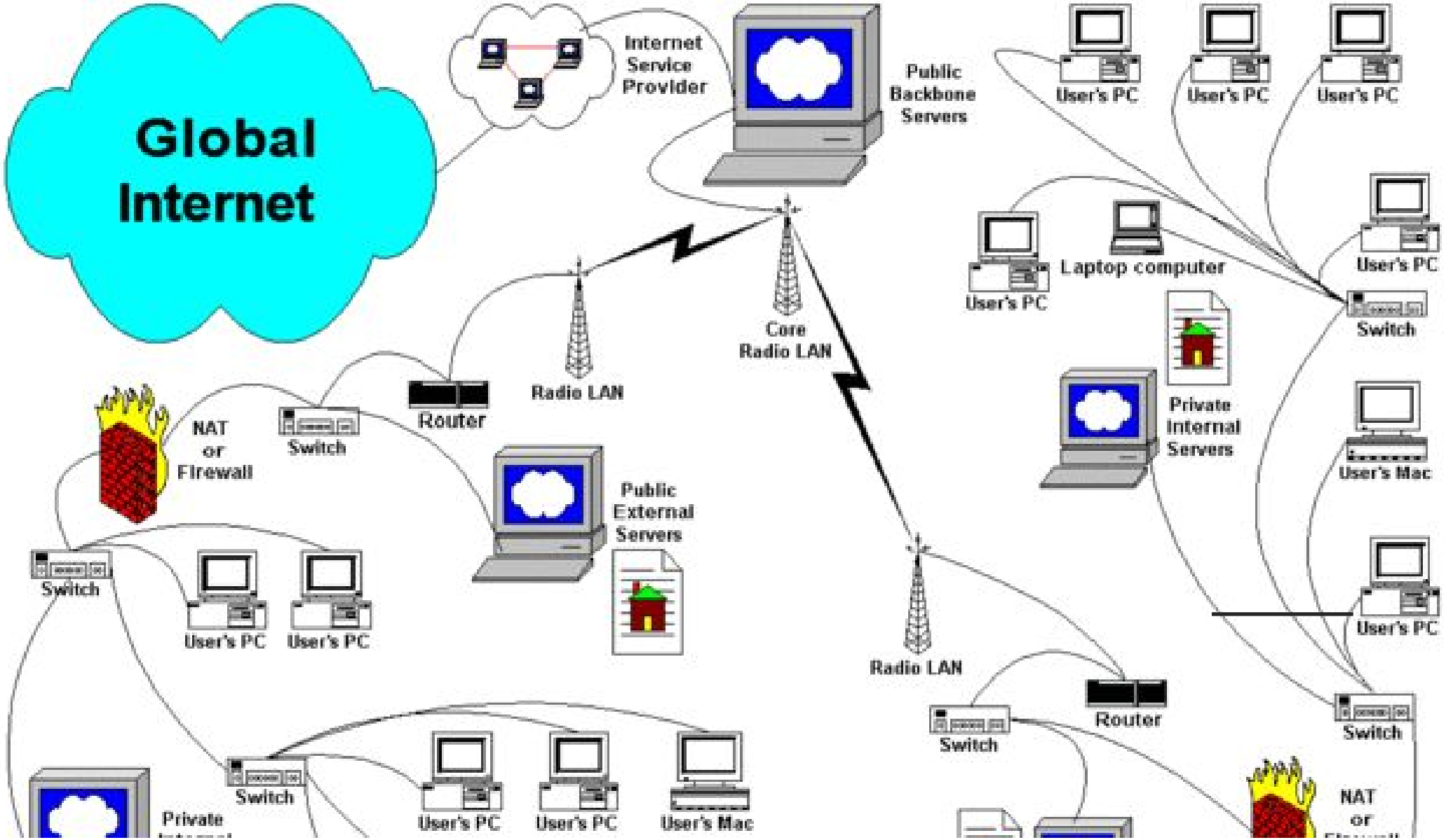
By admin school staff team

รูปการต่อ NetWork ของโรงเรียน



คำถาม
BLOCK WEB ทำไมต้อง BLOCK BLOCK ทำไม

โปรโตคอล

Protocal คืออะไร

Protocal ที่ใช้ในระบบอินเตอร์เน็ตชื่อว่าอะไร

โปรโตคอล HTTP หรือ Hypertext Transfer Protocol คืออะไร

โปรโตคอล TCP/IP หรือ Transfer Control Protocol/Internet Protocol

โปรโตคอล SMTP หรือ Simple Mail Transfer Protocol

Firewall

Firewall คืออะไร

หน้าที่ของ Firewall มีอะไรบ้าง

ประโยชน์ของ Firewall

ชนิดของ Firewall

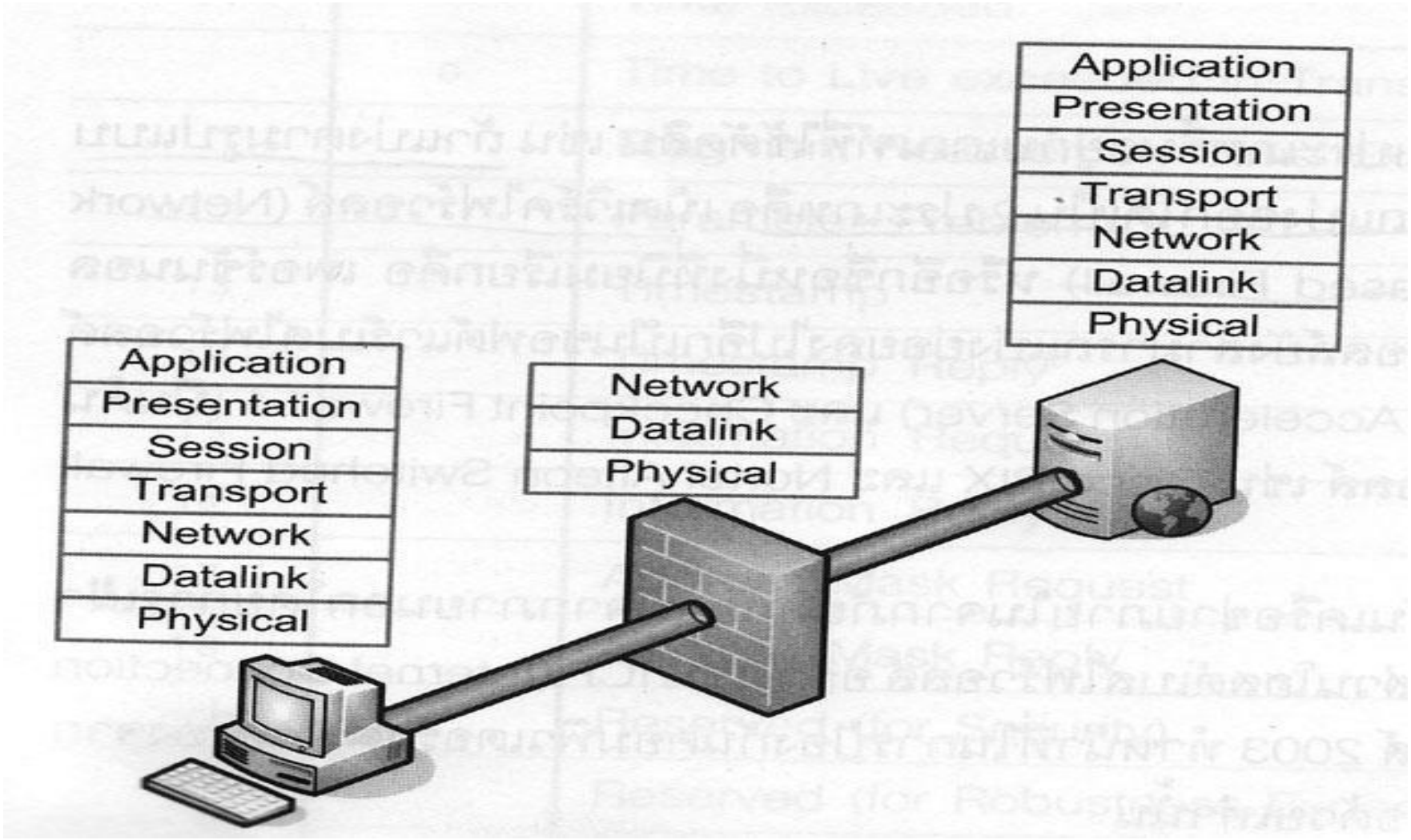
Firewall Operation

- Packet Filtering Firewall
- Stateful Inspection Firewall
- Application Proxy Firewall

Packet Filtering Firewall

- คัดกรองแพ็กเก็ตที่วิ่งผ่านโดยใช้กฎต่างๆ ที่ตั้งค่าไว้แล้ว
- โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎที่กำหนดไว้
- ทำงานแบบ Pattern Matching
- ตัดสินว่าควรจะทิ้งแพ็กเก็ตนั้นไปหรือว่าจะยอมให้แพ็กเก็ตนั้นผ่าน
- การทำงานไม่ซับซ้อนจึงเป็นการทำงานหนึ่งใน Router ในปัจจุบัน

Packet Filtering Firewall



Firewall Architectures

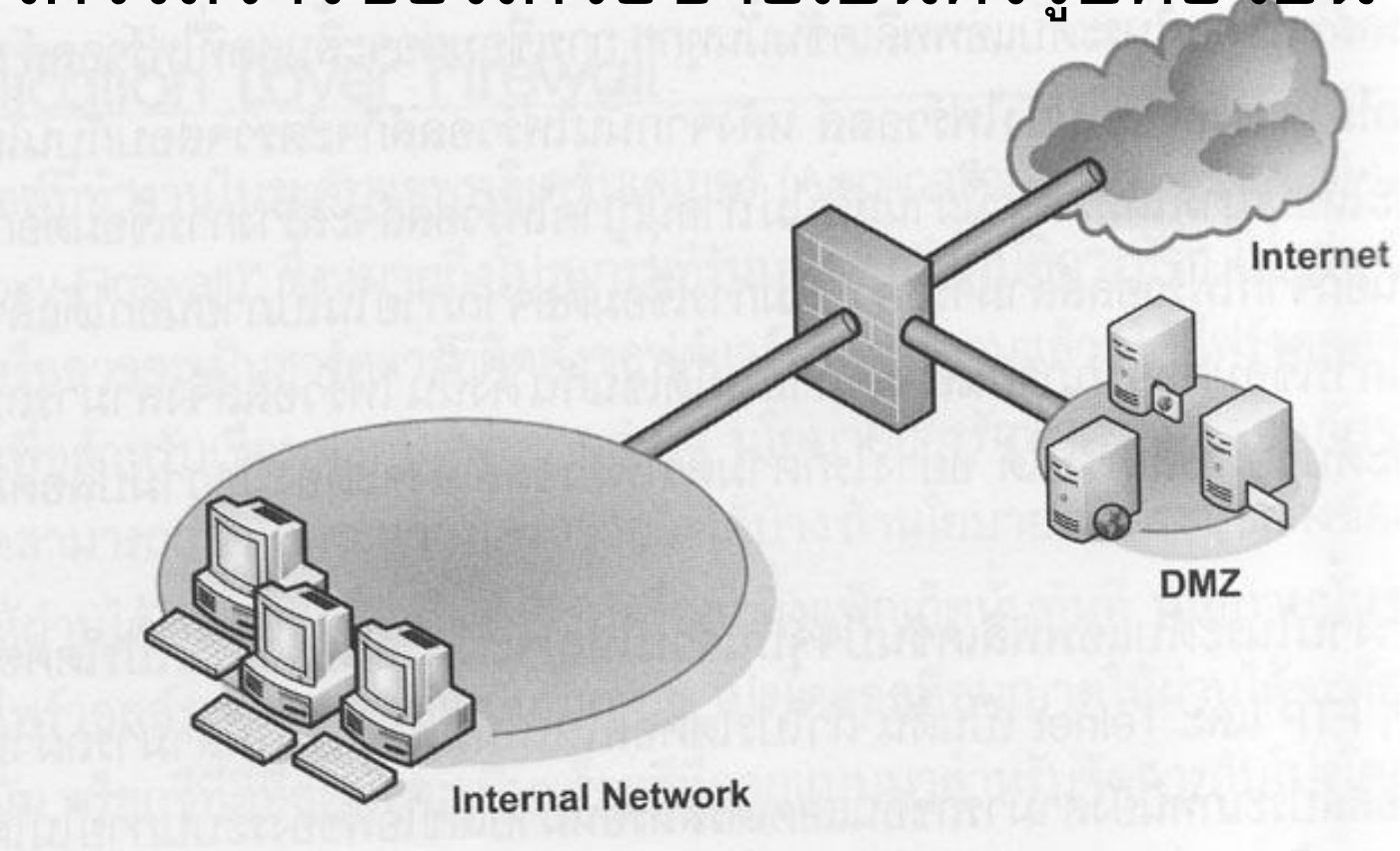
- Screening Router
- Simple Firewall
- Multi-Legged firewall
- Firewall Sandwich
- Layered Security Architecture

Network Security Policy

- Network Security Policy นับเป็นสิ่งที่สำคัญที่สุดสำหรับการใช้งานไฟร์วอล
- ควรกำหนดนโยบายที่สามารถควบคุมหรือป้องกันทราฟิกที่อาจมีผลกระทบต่อการใช้งานเครือข่ายให้มากที่สุด แล้วนำไปบังคับใช้กับไฟร์วอล
- กฎที่บังคับใช้นโยบายการรักษาความปลอดภัยในไฟร์วอลนั้นจะเรียกว่า ACL (Access Control List) หรือ Firewall Rule

Network Security Policy

- ตัวอย่างโยบายรักษาความปลอดภัย โดยสมมติว่าโครงสร้างของเครือข่ายเป็นดังรูปต่อไปนี้



Network Security Policy

- โดย DMZ (Demilitarized Zone) ประกอบด้วย เว็บเซิร์ฟเวอร์ เมลเซิร์ฟเวอร์ และ DNS เซิร์ฟเวอร์
- ผู้ใช้ภายในเครือข่ายสามารถใช้บริการคือ HTTP, HTTPS, FTP, Telnet, SSH, DNS, SMTP, POP3
- ผู้ใช้จากอินเทอร์เน็ตนั้นสามรถใช้บริการจาก DMZ ได้คือ DNS, HTTP, HTTPS, SMTP จากนโยบายนี้เราสามารถเขียน ACL ได้ดังนี้

Network Security Policy

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

Network Security Policy

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

Network Security Policy

Rule	Source	Destination	Service (Port)	Action	Description
6	Internal Network	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

ข้อจำกัดของ Firewall

- Firewall ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่าน Firewall เช่น การโจมตีจากภายในเครือข่าย
- ไม่สามารถป้องกันการโจมตีที่มากับ Application protocols, การทำ Tunneling หรือโปรแกรม Trojan horse ต่างๆ

Firewall Features

- Firewall Throughput : Mbps/Gbps
- VPN Throughput : Mbps
- Concurrent Sessions : number
- IPsec VPN Peers : number
- Interfaces : number of Gigabit Ethernet ports, SFP fiber ports, and Fast Ethernet port
- Virtual Interfaces (VLANs) : number

Firewall Features

- Scalability : VPN clustering and load balancing
- High Availability : Active/Active, Active/Standby
- Redundant Power : Supported, second power supply optional

ขอขอบคุณ

อาจารย์ ธนัญชัย ตรีภาค
ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง