

# Firewall & Policy

ดร. ธนัญชัย ตริภาค

Q : ข้อมูลที่ส่งผ่านเครือข่าย มี Header Field ที่สำคัญ  
อะไรบ้าง





## Q : การบุกรุก การโจมตี ทางเครือข่ายมีอะไรบ้าง

กลุ่มละ 5 อันพร้อม  
คำอธิบายว่าแต่ละอันมี  
ขั้นตอนการโจมตีอย่างไร

แต่ละการโจมตี มีลักษณะ  
ของ Header Field  
อย่างไรบ้าง

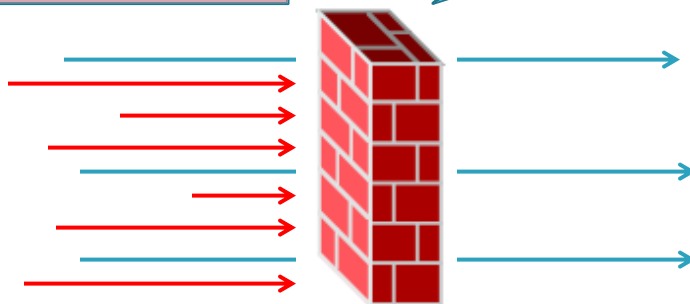
ภัยคุกคามต่างๆ กับ Header Field และลักษณะการทำงาน  
ทางเครือข่าย

ภัยคุกคามทางเครือข่าย	ลักษณะการทำงาน	Header Field ที่สำคัญ

Firewall = Network Filtering

ป้องกันภัยคุกคาม และ  
กำหนดนโยบายการเชื่อมต่อ

How smart is it ??



## รูปไหนคือ Firewall

1



2



3



4



## ลักษณะทางกายภาพของ Network Firewall

- ▶ Appliance , Switch based
- ▶ ภายนอกคล้าย Switch
- ▶ เป็นอุปกรณ์เครือข่ายที่มีหลาย Interface
- ▶ ดูจากภายนอกจะบอกได้ยากกว่าเป็น Firewall หรือ Switch ต้องตรวจสอบ Data Sheet

Host-based Firewall คืออะไร



ยกตัวอย่าง Host-based  
Firewall ที่นักศึกษาใช้

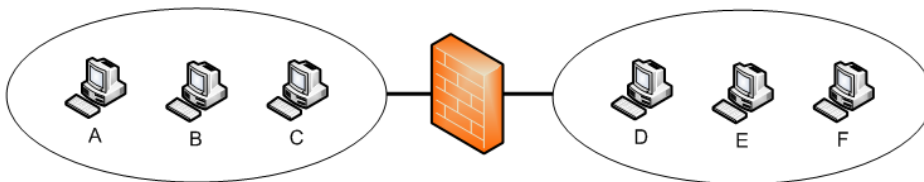
Q : Firewall ป้องกันปัญหาไวรัสได้หรือไม่



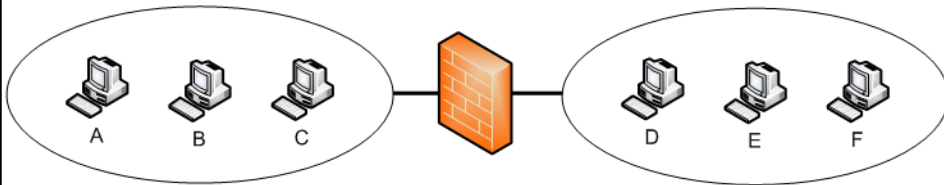
Q : Firewall ป้องกันภัยคุกคามอะไรได้บ้าง และป้องกันอะไรไม่ได้บ้าง



Q1 : Firewall ควบคุมการเชื่อมต่อจาก A->B ได้หรือไม่



Q2 : Firewall ควบคุมการเชื่อมต่อจาก A->D ได้หรือไม่



Q: Firewall ถูกพัฒนาขึ้นก่อนหรือหลังภัยคุกคาม



## ชนิดของ Firewall

- ▶ Packet Filtering
- ▶ Stateful Inspection
- ▶ Application Proxy
- ▶ Next Generation Firewall
  - Integrated System
  - Behavior-based

## การกำหนดกฎของ Firewall

- ▶ Allow All / Deny Some
- ▶ Deny All / Allow Some
- ▶ แบบไหน ปลอดภัย กว่ากัน ?

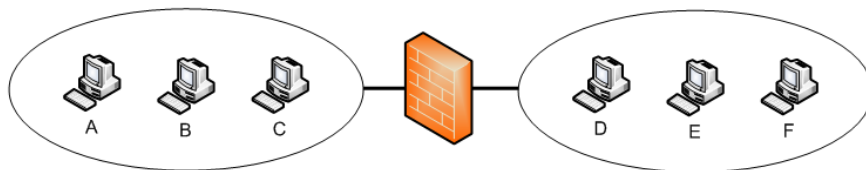




## Packet Filtering Policy

- ▶ Source IP / Source Port
- ▶ Destination IP / Destination Port
- ▶ Flag
- ▶ Action (Allow, Deny)

Q : กฎที่ป้องกันไม่ให้เครื่อง A ไปใช้ Web Server E คืออะไร



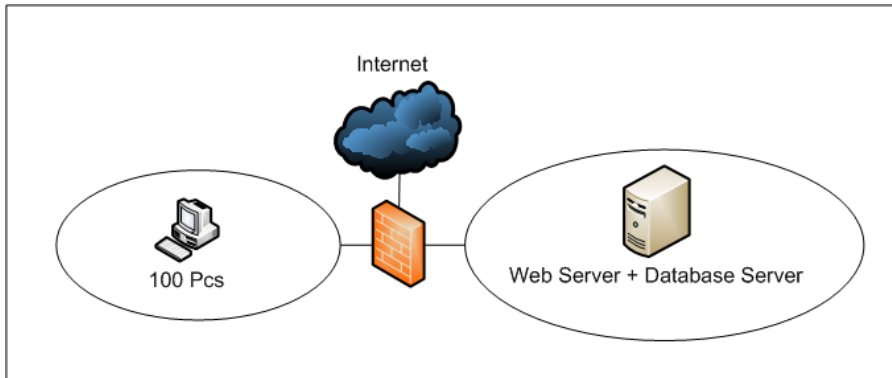
Q : Packet Filtering Firewall ใช้รักษาความปลอดภัยหรือ  
ป้องกันการโจมตีอะไรได้บ้าง ยกตัวอย่างกฎการคัดกรอง



## Stateful Inspection Policy

- ▶ Source IP / Source Port
- ▶ Destination IP / Destination Port
- ▶ Protocol
  - TCP
  - UDP
  - ICMP
  - Application Level (FTP,HTTP,Multimedia)
- ▶ State
- ▶ Action (Allow, Deny)

Q : กฎที่ป้องกันไม่ให้เครื่อง PC เล่นเกมส์ Ragnarok (TCP:5121) คืออะไร



Q : Stateful Inspection Firewall ใช้รักษาความปลอดภัยหรือป้องกันการโจมตีอะไรได้บ้าง ยกตัวอย่างกฎการคัดกรอง



## Application Proxy Policy

```

user@host# show security policies
  from-zone untrust to-zone trust {
    policy 1 {
      match {
        source-address 1.1.1.0;
        destination-address 2.2.2.0;
        application junos-http;
      }
      then {
        permit {
          application-services {
            application-firewall {
              rule-set rs1;
            }
          }
        }
      }
    }
  }
  policy 2 {
    match {
      source-address 1.1.1.0;
      destination-address 2.2.2.0;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set rs2;
          }
        }
      }
    }
  }
}

```

## Application Proxy Policy

```

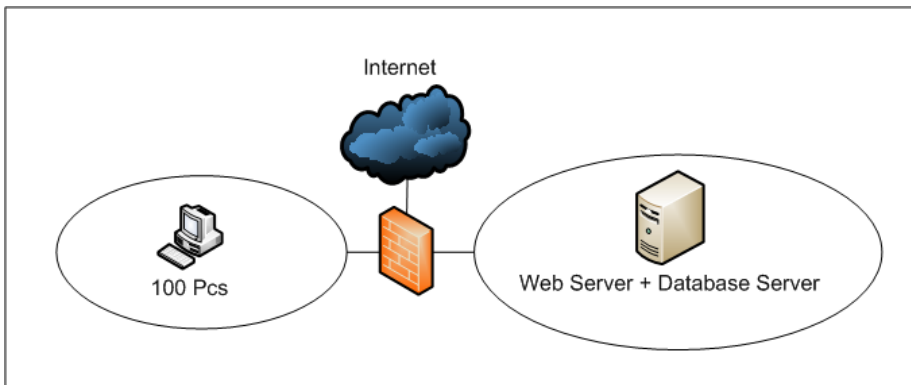
user@host# show security application-firewall
  rule-sets rs1 {
    rule r1 {
      match {
        dynamic-application [junos:KAZZA junos:EDONKEY junos:YSMS];
      }
      then {
        deny;
      }
    }
    default-rule {
      permit;
    }
  }
  rule-sets rs2 {
    rule r1 {
      match {
        dynamic-application [junos:FACEBOOK-ACCESS junos:GOOGLE-TALK junos:MEEBO junos:UNKNOWN];
      }
      then {
        permit;
      }
    }
    default-rule {
      deny;
    }
  }
}

```

## Application Proxy Policy

- ▶ Source IP
- ▶ Destination IP
- ▶ Application Protocol (HTTP,MAIL,DNS, ANY)
- ▶ Application Services  
(KAZZA,EDONKEY,FACEBOOK,GOOGLE-TALK)
- ▶ Action (Allow, Deny)

Q : กฎที่ป้องกันไม่ให้เครื่อง PC ใช้ Bittorrent คืออะไร



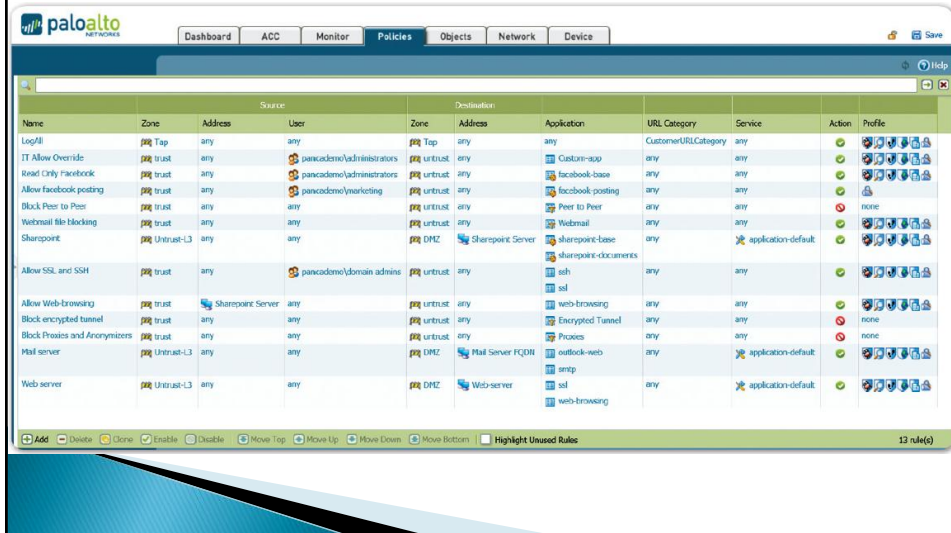
Q : Application Proxy Firewall ใช้รักษาความปลอดภัยหรือ  
ป้องกันการโจมตีอะไรได้บ้าง ยกตัวอย่างกฎการคัดกรอง



## Next Generation Firewall

- ▶ Classify all traffic, across all ports, all the time
- ▶ Reduce the threat footprint, prevent cyber attacks
- ▶ Map application traffic and associated threats to users and devices
- ▶ Applications, Content, Users, and Devices – All under control.

## Next Generation Firewall Policy



Name	Zone	Address	User	Destination	Application	URL Category	Service	Action	Profile
LogAll	Tap	any	any	Tap	any	any	any	Log	
IT Allow Override	trust	any	panwcodemo/administrators	trust	any	Custom-app	any	Allow	
Read Only Facebook	trust	any	panwcodemo/administrators	trust	any	facebook-base	any	Allow	
Allow facebook posting	trust	any	panwcodemo/marketing	trust	any	facebook-posting	any	Allow	
Block Peer to Peer	trust	any	any	trust	any	Peer to Peer	any	Deny	none
Webmail file blocking	trust	any	any	trust	any	Webmail	any	Deny	
Sharepoint	Trust-L3	any	any	DMZ	Sharepoint Server	sharepoint-base	any	Allow	
					sharepoint-documents		any	Allow	
Allow SSL and SSH	trust	any	panwcodemo/domain admins	trust	any	ssh	any	Allow	
					sftp		any	Allow	
Allow Web-browsing	trust	any	Sharepoint Server	trust	any	web-browsing	any	Allow	
Block encrypted tunnel	trust	any	any	trust	any	Encrypted Tunnel	any	Deny	none
Block Proxies and Anonymizers	trust	any	any	trust	any	Proxies	any	Deny	none
Mail server	Trust-L3	any	any	DMZ	Mail Server FQDN	outlook-web	any	Allow	
					smtp		any	Allow	
Web server	Trust-L3	any	any	DMZ	Web-server	sftp	any	Allow	
					web-browsing		any	Allow	

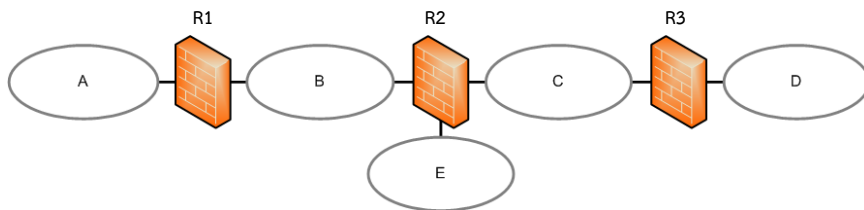
Q : Next Generation Firewall ใช้รักษาความปลอดภัยหรือ  
ป้องกันการโจมตีอะไรได้บ้าง ยกตัวอย่างกฎการคัดกรอง



กิจกรรม : สรุปความสามารถในการรักษาความปลอดภัยของ Firewall

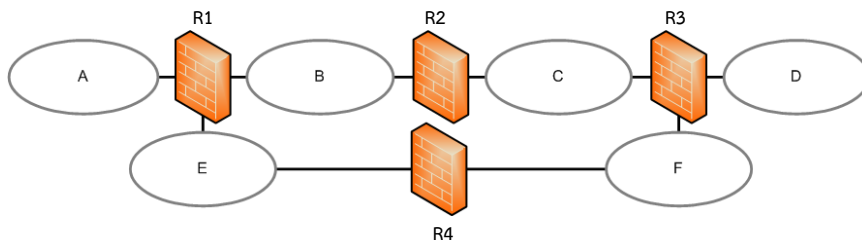
การป้องกันภัยคุกคาม	Packet Filtering	Stateful Inspection	Application Proxy	Firewall NG
???	✓	✓	✓	✓
???		✓	✓	✓
???			✓	✓
???				

Q : ถ้าต้องการป้องกันไม่ให้เครือข่าย A เชื่อมต่อกับเครือข่าย D จะต้องตั้งค่า ACL ที่อุปกรณ์ใด





Q : ถ้าต้องการป้องกันไม่ให้เครือข่าย A เชื่อมต่อกับเครือข่าย D  
จะต้องตั้งค่า ACL อย่างไร



Q : ถ้า Firewall มีกฎจำนวนมาก ควรเรียงลำดับกฎการ  
คัดกรองอย่างไร



Q : ตั้งกฎซ้ำๆ กันใน Firewall ต่างๆ มีผลเสียหรือไม่



## Firewall Zone

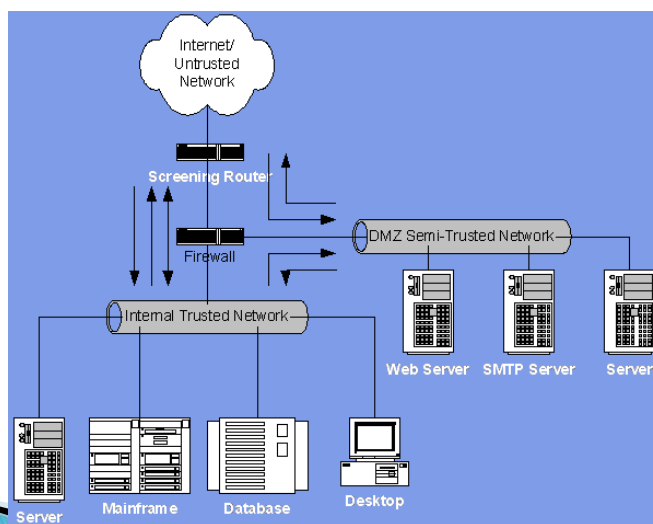
- ▶ Untrusted Zone
- ▶ DMZ Zone
- ▶ Trust Zone1, Trust Zone2, Trust Zone3, ...

แยก Zone ของเครือข่ายตามความเสี่ยง หรือ บทบาท  
แล้วนำ Firewall กันระหว่างเครือข่าย เพื่อกำหนดกฎรักษาความ  
ปลอดภัย

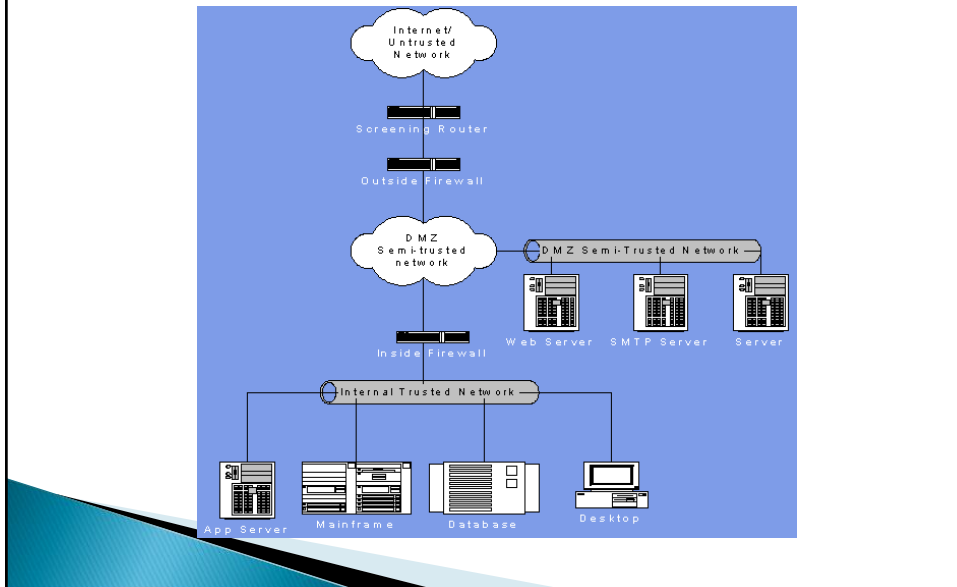
## Firewall 2 เครื่อง กับ 6 เครือข่าย จัดวางอย่างไร



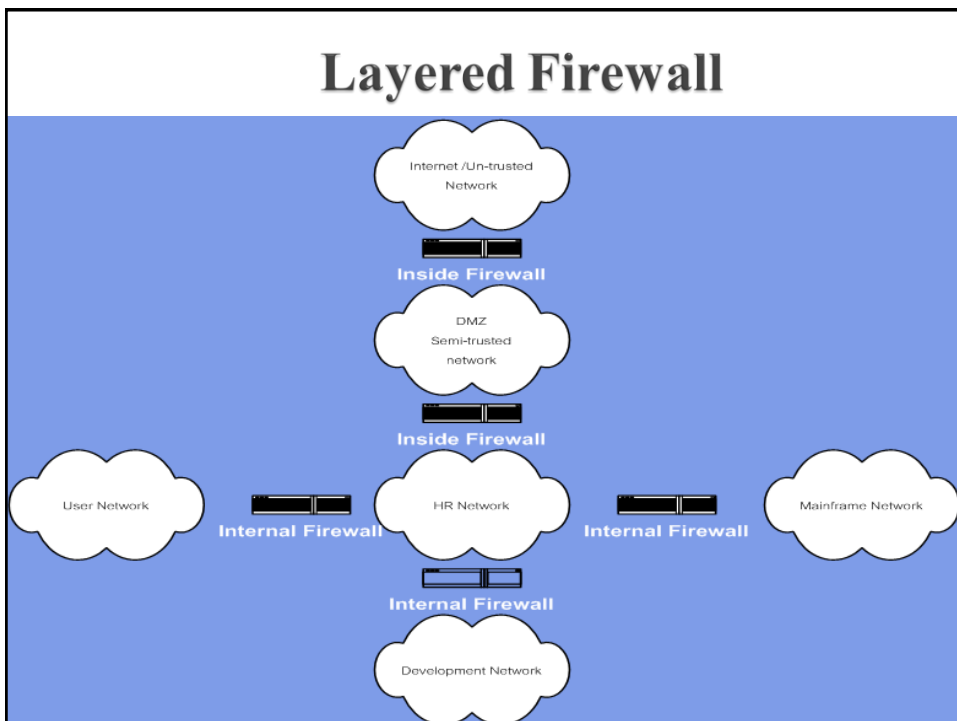
## Firewall Design : Multi-Leg

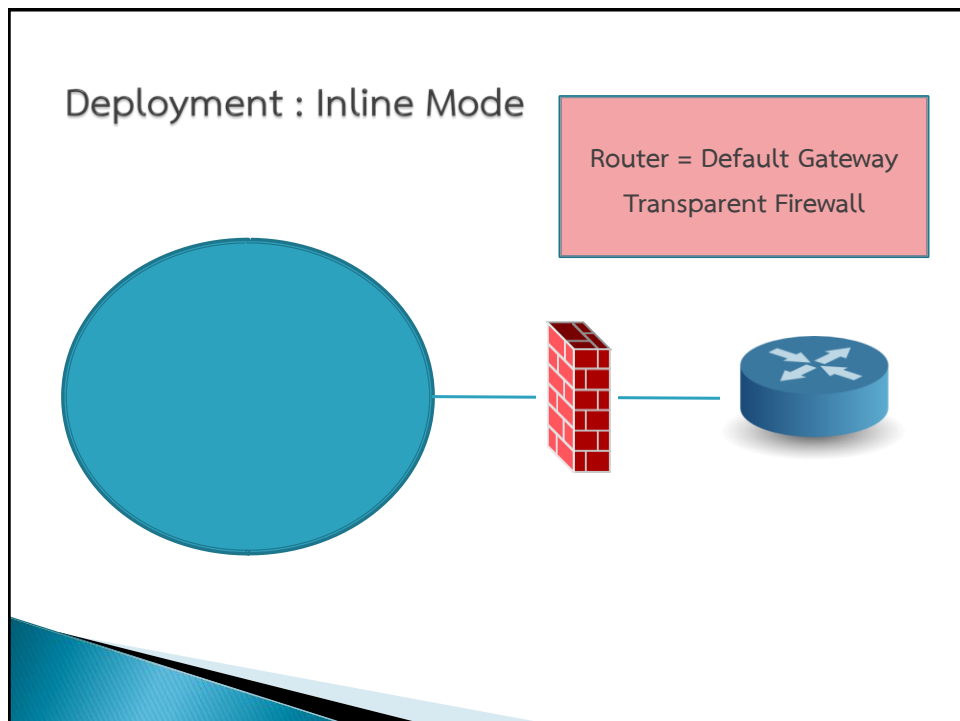
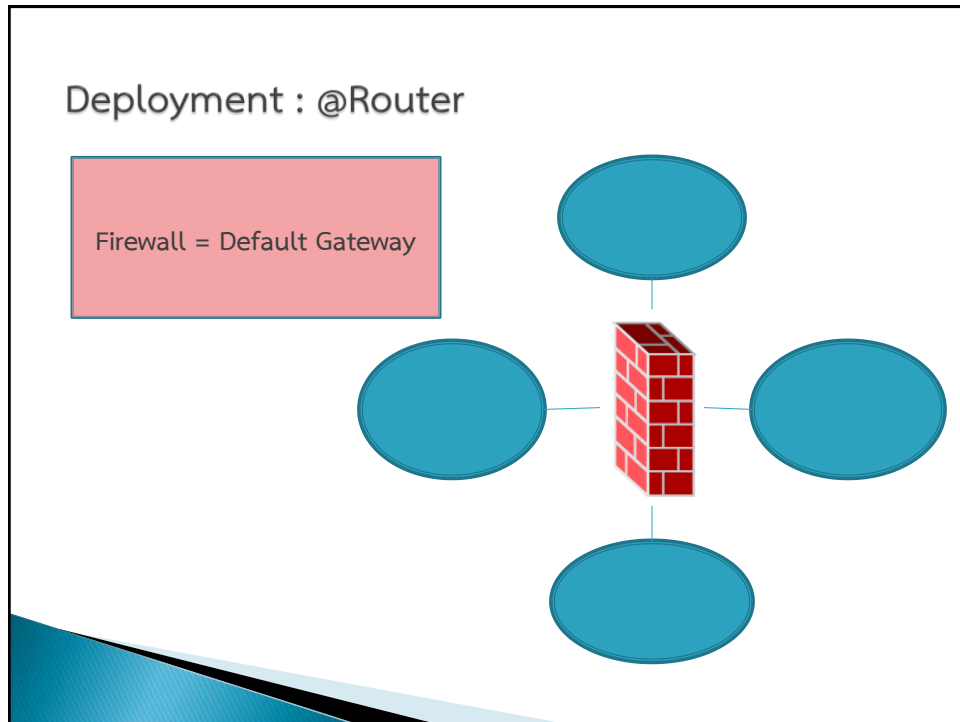


## Firewall Design : Firewall Sandwich



## Layered Firewall





## กิจกรรม

- ▶ แบ่งกลุ่ม กลุ่มละ 5-6 คน
- ▶ ออกแบบระบบเครือข่ายโดยมีไม่น้อยกว่า 6 เครือข่าย และมี Firewall อย่างน้อย 3 เครื่อง
- ▶ กำหนดบริการพื้นฐาน
- ▶ กำหนดนโยบายการรักษาความปลอดภัย
- ▶ เขียนกฎของ Firewall แต่ละเครื่อง
- ▶ การส่ง : ถ่ายรูปเครือข่ายรวม / Policy หลัก / กฎของ Firewall แต่ละตัว / สมาชิกในกลุ่ม / ภัยคุกคามที่ Firewall ป้องกันได้ / ส่งใน Facebook

สรุป / สิ่งที่ได้เรียนรู้