บทที่ 6 : Firewall Part2

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

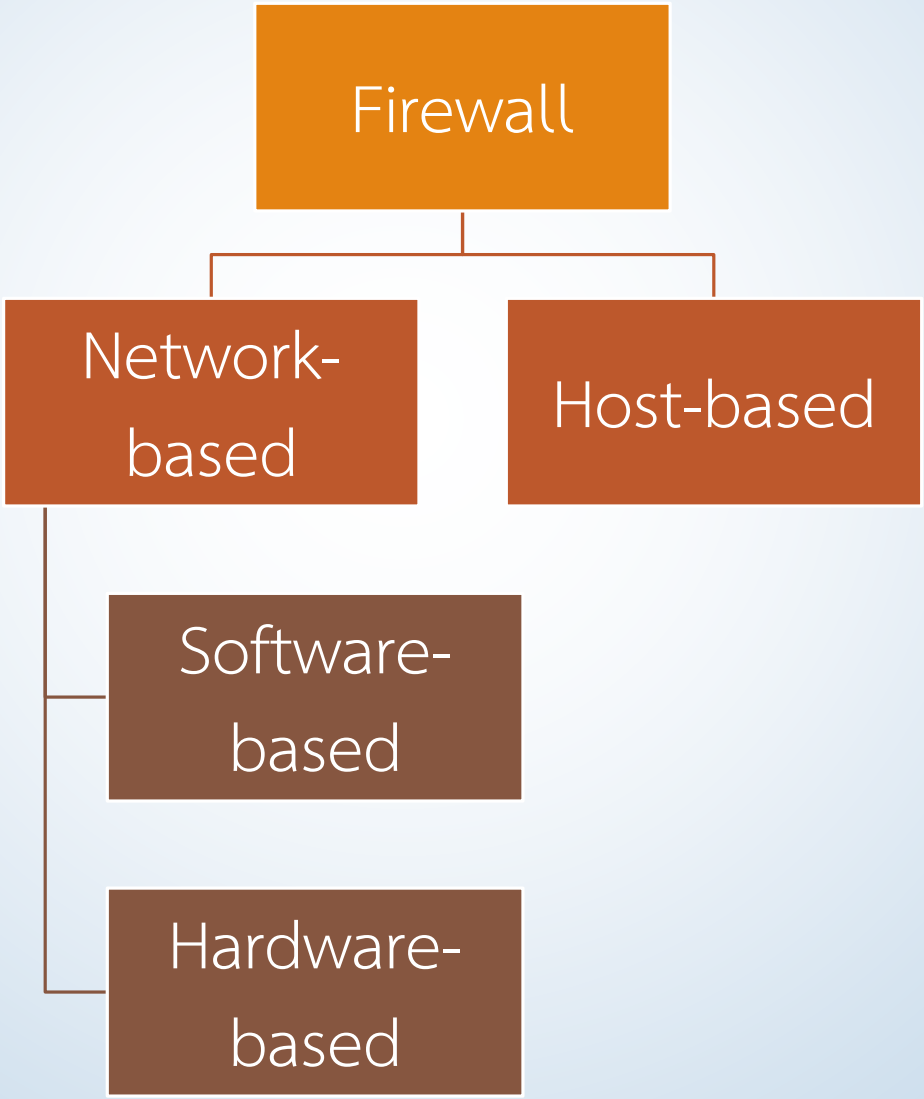
Outline

- ประเภทของไฟร์วอลล์
- นโยบายการรักษาความปลอดภัย
- Network Address Translation (NAT)

ประเภทของไฟร์วอลล์

- หากแบ่งตามรูปแบบการไหลของข้อมูลผ่านไฟร์วอลล์ จะแบ่งได้เป็น 2 ประเภท คือ
  - Network Firewall แบ่งเป็น Software-based และ Hardware-based
  - Host-based Firewall หรือ Personal Firewall

การแบ่งประเภทไฟร์วอลล์ตามการไหลของข้อมูล



ประเภทของไฟร์วอลล์ [2]

- หากแบ่งประเภทไฟร์วอลล์โดยการใช้เลเยอร์การทำงานของไฟร์วอลล์ จะแบ่งออกได้เป็น 3 ประเภท คือ
  - Packet Filtering Firewall
  - Application Layer Firewall
  - Stateful Inspection Firewall

ประเภทของไฟร์วอลล์

: Packet Filtering Firewall

- การกรองแพ็คเก็ตของไฟร์วอลล์จะทำก่อนที่จะมีการส่งผ่านแพ็คเก็ต
- แพ็คเก็ตจะถูกกรองตามรายการควบคุมการเข้าถึง (Access Control List : ACL) ที่ประกอบไปด้วยเฮดเดอร์ของไอพีแพ็คเก็ต และการอนุญาตหรือไม่อนุญาตให้ผ่าน
- โดยทั่วไปแล้วหากมีแพ็คเก็ตที่ไม่ตรงกับกฎการอนุญาตจะถือว่าห้ามผ่าน

ประเภทของไฟร์วอลล์

: Packet Filtering Firewall [2]

- ข้อมูลที่ใช้พิจารณาว่าจะให้แพ็คเก็ตผ่านหรือไม่ มาจากเฮดเดอร์ของไอพีแพ็คเก็ต ที่ประกอบไปด้วย
  - Source IP Address
  - Destination IP Address
  - ประเภทของโปรโตคอล เช่น TCP, UDP เป็นต้น
  - Source Port
  - Destination Port

ประเภทของไฟร์วอลล์

: Packet Filtering Firewall [3]

- หลักการทำงานง่ายๆของ Packet Filtering Firewall จะทำการพิจารณาแพ็คเก็ตเพื่อตรวจสอบว่าแพ็คเก็ตนั้นถูกส่งมาจากนอกเครือข่ายหรือไม่
- ถ้าแพ็คเก็ตถูกส่งมาจากนอกเครือข่าย แต่มีแอดเดรสเป็นภายใน แสดงว่าแพ็คเก็ตนั้นถูกสปูฟ (Spoof Address) และจะดรอปแพ็คเก็ตนี้ทิ้งไป

Packet Filtering Firewall

ประเภทของไฟร์วอลล์

: Stateful Inspection Firewall

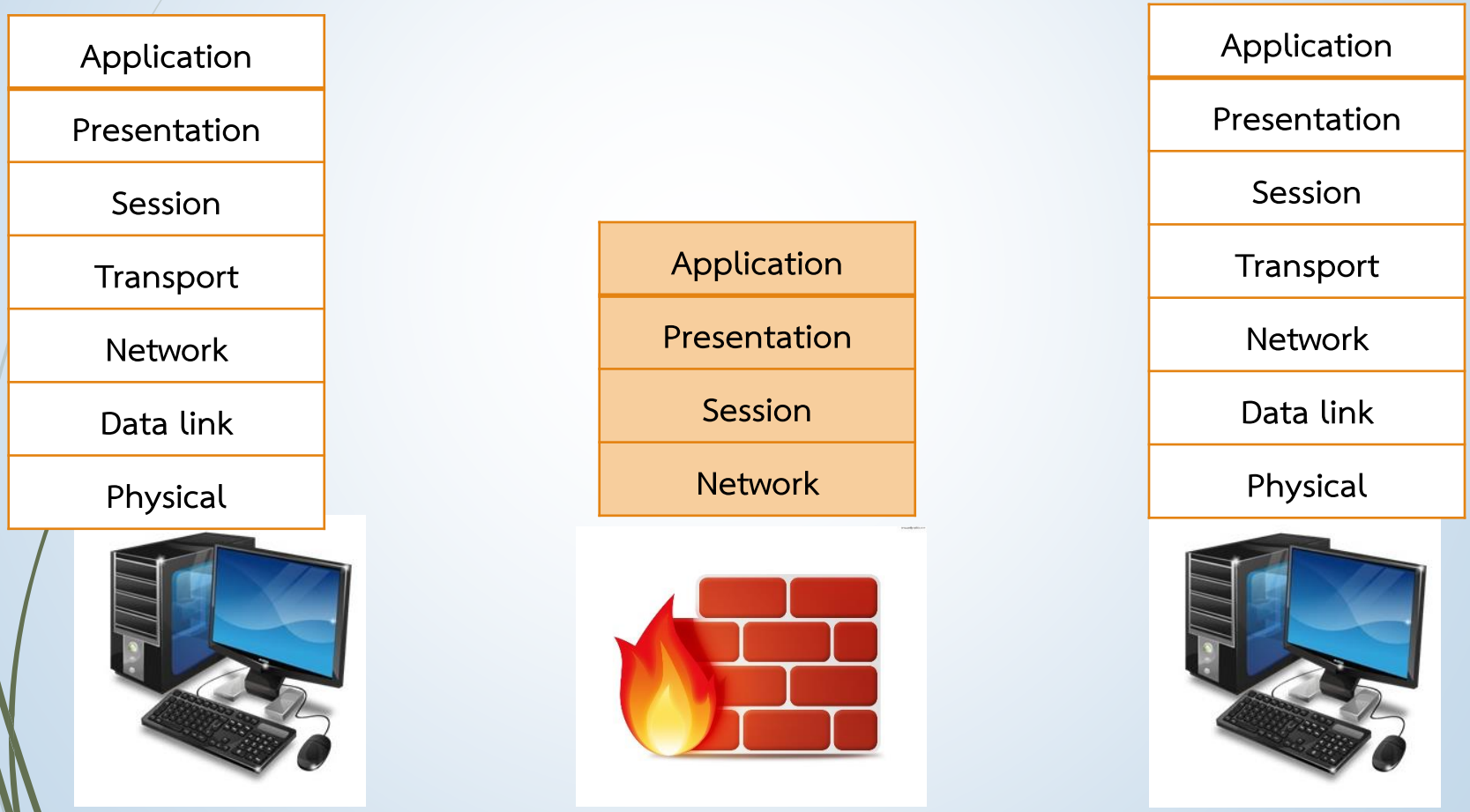
- มีหลักการทำงานทุกอย่างเช่นเดียวกับ Packet Filtering Firewall
- แต่ส่วนที่เพิ่มข้นมาคือมันจะบันทึกข้อมูลเกี่ยวกับคอนเน็คชั่นที่เกิดขึ้นลงใน State Table ก่อนที่จะส่งแพ็คเก็ตนี้ต่อให้เลเยอร์อื่น
- State Table จะเก็บข้อมูลเกี่ยวกับแอดเดรสของต้นทางและปลายทาง ประเภทโปรโตคอล หมายเลขพอร์ต

ประเภทของไฟร์วอลล์

: Stateful Inspection Firewall [2]

- เมื่อไฟร์วอลล์ได้รับแพ็คเก็ตก็จะตรวจสอบข้อมูลกับสเตทเทเบิลว่าเป็นส่วนหนึ่งของคอนเน็คชั่นที่สร้างไว้แล้วหรือไม่
- ถ้าเป็นส่วนหนึ่งของคอนเน็คชั่นจริงก็ไม่มีความจำเป็นใดๆ ที่จะต้องตรวจสอบซ้ำอีก
- วิธีการป้องกันการโจมตีแบบ DOS ที่จะส่งแพ็คเก็ตจำนวนมากเข้ามาจนทำให้สเตทเทเบิลเต็ม คือการตั้ง timeout ของแต่ละคอนเน็คชั่นเอาไว้

Stateful Inspection Firewall



ประเภทของไฟร์วอลล์

: Application Layer Firewall

- บางครั้งเรียกว่า “พร็อกซี” (Proxy Firewall) ซึ่งเป็นเครื่องมือบังคับใช้นโยบายว่าจะอนุญาตให้ทราฟิกใดสามารถส่งผ่านระหว่างเครือข่ายได้บ้าง
- โปรโตคอลที่อนุญาตให้ผ่านได้จะต้องมีพร็อกซีสำหรับโปรโตคอลนั้นโดยเฉพาะ
- พร็อกซีเป็นสเตทฟูลไฟร์วอลล์ แต่มีความแตกต่างกันคือ ***พร็อกซีเซิร์ฟเวอร์จะสร้างไอพีแพ็คเก็ตใหม่*** เพื่อส่งต่อไปยังเป้าหมาย เมื่อแพ็คเก็ตนั้นผ่านการตรวจสอบแล้ว

ประเภทของไฟร์วอลล์

: Application Layer Firewall [2]

- กระบวนการสร้างการเชื่อมต่อของพร็อกซีไฟร์วอลล์
- 1) เริ่มจากไคลเอนต์ส่งการร้องขอไปยังไฟร์วอลล์
- 2) ไฟร์วอลล์จะตรวจสอบกับนโยบายรักษาความปลอดภัยว่าอนุญาตให้ผ่านหรือไม่
- 3) ถ้าอนุญาต ไฟร์วอลล์จะสร้างการเชื่อมต่อกับเซิร์ฟเวอร์แทนไคลเอนต์เอง

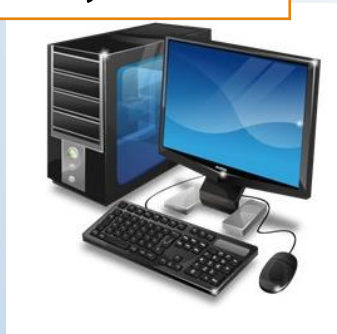
ประเภทของไฟร์วอลล์

: Application Layer Firewall [3]

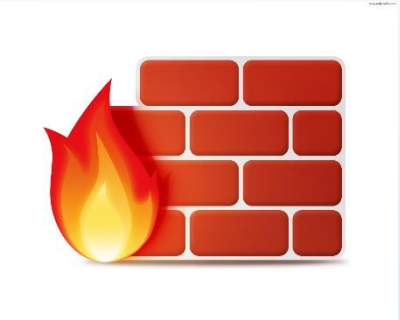
- พร็อกซีไฟร์วอลล์สามารถควบคุมกันเชื่อมต่อจากภายนอกได้เช่นกัน โดยเครื่องที่อยู่ภายนอกจะมองเห็นเฉพาะหมายเลขไอพีของไฟร์วอลล์เท่านั้น ไม่สามารถเห็นเครื่องที่อยู่ภายในได้

Application Layer Firewall

Application
Presentation
Session
Transport
Network
Data link
Physical



Application



Application
Presentation
Session
Transport
Network
Data link
Physical

นโยบายการรักษาความปลอดภัย

- สิ่งที่สำคัญที่สุดในการใช้งานไฟร์วอลล์คือการกำหนดนโยบายการรักษาความปลอดภัย (Network Security Policy)
- เมื่อกำหนดนโยบายแล้วจึงนำนโยบายไปบังคับใช้ในไฟร์วอลล์
- กฎที่บังคับใช้ในไฟร์วอลล์จะเรียกว่า “ACL” (Access Control List) หรือไฟร์วอลล์รูล (Firewall Rule)
- ถ้าแพ็คเก็ตที่พิจารณาไม่ตรงกับกฎใดใน ACL เลย ไฟร์วอลล์ก็จะทำการดร็อปแพ็คเก็ตนั้นทิ้งไป

Network Address Translation (NAT)

- NAT ไม่ใช่เทคโนโลยีของไฟร์วอลล์ แต่ไฟร์วอลล์ส่วนใหญ่จะมีฟังก์ชัน NAT อยู่
- NAT เป็นเทคโนโลยีที่ใช้ในการแก้ปัญหาหมายเลขไอพีที่ใช้งานบนอินเทอร์เน็ตไม่เพียงพอ เพราะเมื่อเชื่อมต่อกับอินเทอร์เน็ตคอมพิวเตอร์จะต้องมีหมายเลขไอพีจริง
- จะมีองค์กรกลางทำหน้าที่จัดการเกี่ยวกับการแจกจ่ายไอพี โดยจะจ่ายเป็นบล็อคไปให้ผู้บริการอินเทอร์เน็ต

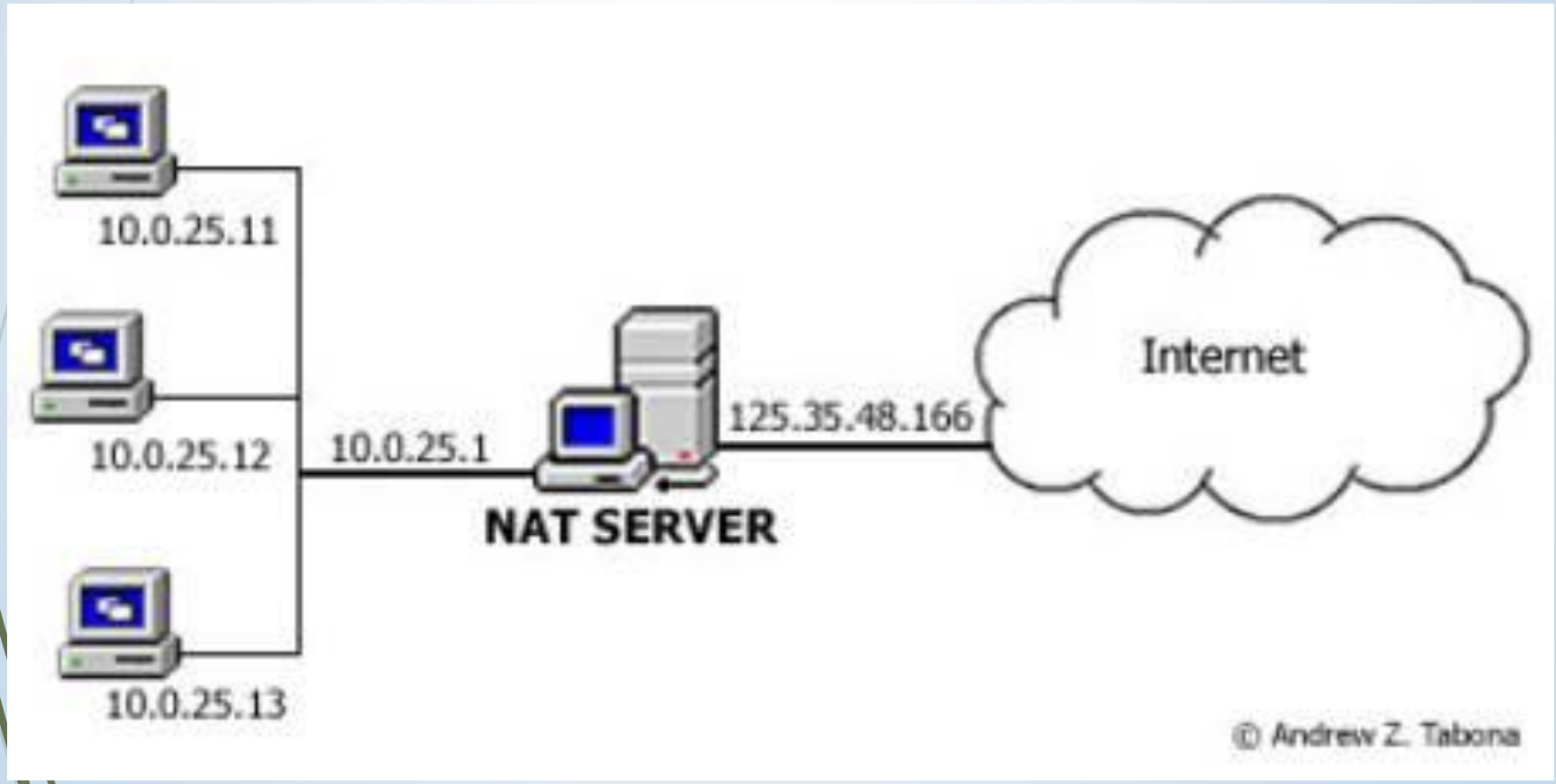
Network Address Translation (NAT) [2]

- องค์กรส่วนใหญ่จะแก้ปัญหาโดยการกำหนดให้คอมพิวเตอร์ทุกเครื่องในเครือข่ายใช้หมายเลขไอพีจริงเพียงไอพีเดียว โดยการใช้ NAT ส่วนคอมพิวเตอร์ภายในจะใช้ Private IP เช่น 10.0.0.0/8 172.16.0.0/12 192.168.0.0.16

Network Address Translation (NAT) [3]

- หลักการทำงานคล้ายกับ Stateful Inspection Firewall แต่มีส่วนเพิ่มเติมคือ เมื่อ NAT ได้รับแพ็คเก็ตจากคอมพิวเตอร์ภายในที่ต้องการส่งต่อไปยังอินเทอร์เน็ต มันจะเปลี่ยนไอพีแอดเดรสของต้นทางให้เป็นไอพีจริงของไฟร์วอลล์แล้วค่อยส่งไป
- เมื่อเซิร์ฟเวอร์ที่อยู่บนอินเทอร์เน็ตตอบกลับมา ก็จะตอบกลับมายังแอดเดรสของไฟร์วอลล์นี้

Network Address Translation (NAT)



Network Address Translation (NAT) [4]

ข้อจำกัดของ NAT

- NAT จะสามารถแทนค่าได้เฉพาะส่วนแพ็คเก็ตเฮดเดอร์เท่านั้น ทำให้มีบางแอพพลิเคชั่นที่ทำงานผ่าน NAT ไม่ได้ เช่น FTP และแอพพลิเคชั่นประเภท Audio/Video
- หากผู้โจมตีมีวิธีทำให้ผู้ใช้ภายในเริ่มสร้างการเชื่อมต่อไปหาผู้โจมตีก่อน ก็จะทำให้ผู้โจมตีสามารถเจาะเข้ามาในระบบได้

Network Address Translation (NAT) [5]

Reverse NAT

- เป็นบริการที่ทำให้ผู้ใช้ที่อยู่บนอินเทอร์เน็ตสามารถเข้ามาใช้งานเซิร์ฟเวอร์ที่อยู่ภายในได้
- หลักการทำงานคือ ไฟร์วอลล์จะทำหน้าที่บริการแทนเซิร์ฟเวอร์ที่อยู่ภายใน โดยเมื่อได้รับการร้องขอมายังหมายเลขไอพีจริงของเซิร์ฟเวอร์ ไฟร์วอลล์จะทำการร้องขอข้อมูลไปยังเซิร์ฟเวอร์นั้น แล้วจึงส่งต่อข้อมูลกลับไปยังไคลเอนต์ที่อยู่บนอินเทอร์เน็ต โดยจะเปลี่ยนไอพีต้นทางเป็นไอพีของไฟร์วอลล์