บทที่ 6 : Firewall Part3

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Outline

- ผลิตภัณฑ์ไฟร์วอลล์
  - Linux Firewall
  - Check Point Firewall–1
- ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์
  - Host-based or Network-based
  - Hardware or Software
  - ฟีเจอร์ที่สำคัญของไฟร์วอลล์

ผลิตภัณฑ์ไฟร์วอลล์

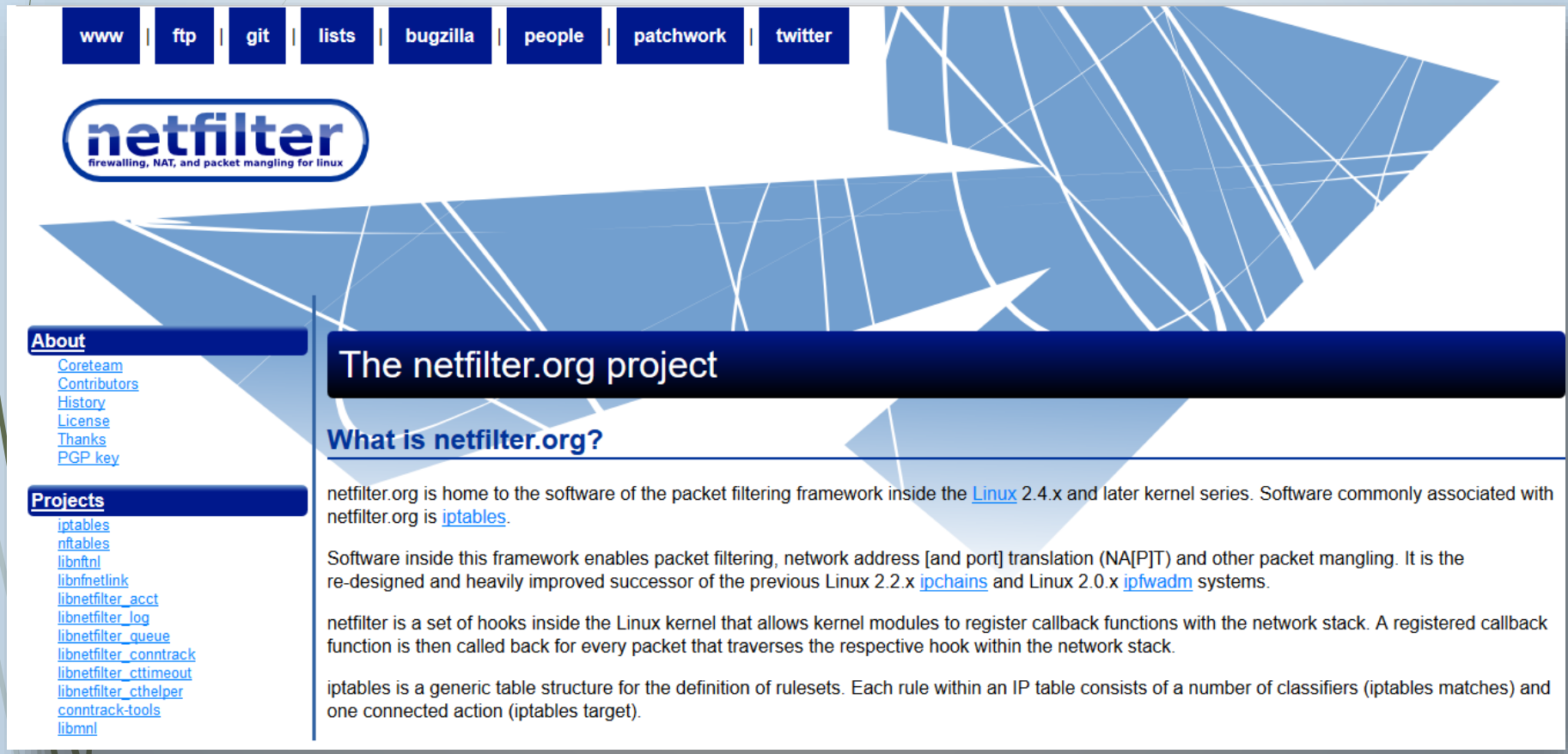
- ผลิตภัณฑ์ไฟร์วอลล์ที่มีขายตามท้องตลาดมีมากมายหลายยี่ห้อ ในหัวข้อนี้จะกล่าวถึงผลิตภัณฑ์ไฟร์วอลล์ที่ได้รับความนิยม เช่น
  - Linux Firewall : iptables
  - Check Point Firewall–1

ผลิตภัณฑ์ไฟร์วอลล์

: Linux Firewall : iptables

- ลินุกซ์เป็นระบบปฏิบัติการโอเพ่นซอร์สที่ได้รับความนิยมอย่างมาก เพราะไม่ต้องเสียค่าลิขสิทธิ์
- ไฟร์วอลล์ที่ติดมากับลินุกซ์ คือ iptables ซึ่งสามารถทำ Packet Filtering และ NAT ได้
- ไฟร์วอลล์ iptables พัฒนาอยู่ภายใต้โครงการ netfilter.org

www.netfilter.org



ผลิตภัณฑ์ไฟร์วอลล์

: Linux Firewall : iptables [2]

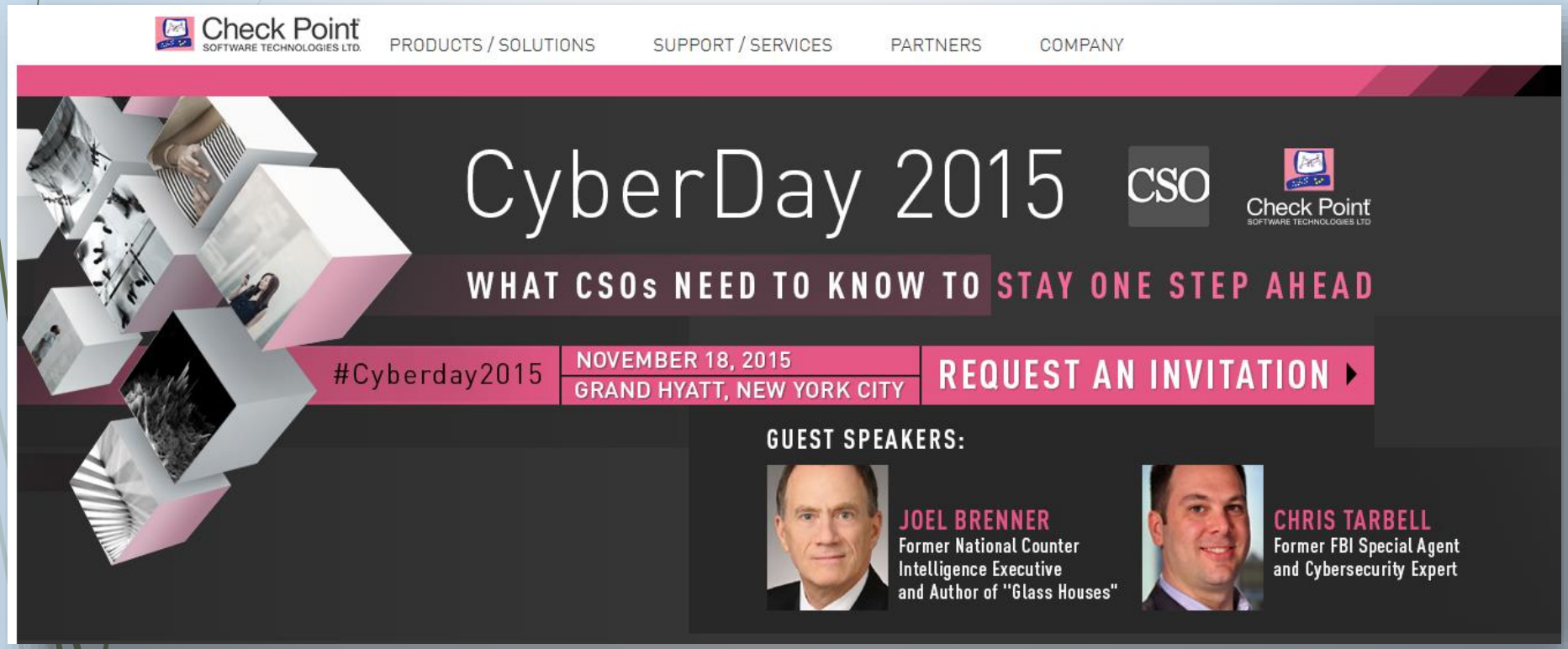
- ฟีเจอร์ที่สำคัญ
  - Packet Filtering (IPv4 และ IPv6)
  - Stateful Packet Filtering (IPv4)
  - รองรับ NAT และ NAPT (Network Address and Port Translation)
- ปกติแล้วการตั้งค่าไฟร์วอลล์บนลินุกซ์จะใช้คำสั่งแบบ Command Line ซึ่งยากต่อการใช้งาน จึงมีโปรแกรมแบบ GUI ช่วยให้การใช้งานง่ายยิ่งขึ้น เช่น firewall builder บนเว็บไซต์ www.fwbuilder.org

ผลิตภัณฑ์ไฟร์วอลล์

: Check Point Firewall-1

- เป็นไฟร์วอลล์ที่ได้รับความนิยมมากอีกตัวหนึ่ง สามารถป้องกันการโจมตีได้อย่างมีประสิทธิภาพ
- สามารถตรวจสอบแพ็คเก็ตได้ตั้งแต่ระดับเน็ตเวิร์คไปจนถึงชั้นแอพพลิเคชั่น
- มีฟีเจอร์ที่สำคัญ เช่น ระบบควบคุมการเข้าถึง การตรวจสอบเนื้อหาข้อมูล การพิสูจน์ทราบตัวตนผู้ใช้ รองรับการทำ NAT และ VPN ฯลฯ

เว็บไซต์ของบริษัท Check Point



ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

- ไฟร์วอลล์ปกติจะมีโครงสร้างง่ายๆ ทำหน้าที่กรองแพ็คเก็ตที่วิ่งผ่านเครือข่าย และตัดสินใจว่าจะให้แพ็คเก็ตนั้นๆ ผ่านไปได้หรือไม่โดยการตรวจดูเฮดเดอร์ของแพ็คเก็ตในเลเยอร์ 3 และ 4
- ไฟร์วอลล์ระดับสูงจะสามารถกรองแพ็คเก็ตในระดับแอพพลิเคชั่นได้ ซึ่งจะสามารถกำจัดสแปมเมล ไวรัส หรือเนื้อหาที่ไม่เหมาะสมได้

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์ [2]

- ไฟร์วอลล์ในปัจจุบันจะทำหน้าที่มากกว่า “ยาม” คือมีการเพิ่มฟีเจอร์ใหม่ๆเข้ามา ซึ่งบางฟีเจอร์ก็ไม่ใช่ฟังก์ชันของไฟร์วอลล์โดยตรง เช่น VPN, Gateway, Web Cache
- ไฟร์วอลล์แบบมัลติฟังก์ชันนี้ เป็นที่แพร่หลายอย่างมากในปัจจุบัน

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

: Host-based or Network-based

- Host-based Firewall หรือ Personnal Firewall มีหลักการทำงานง่ายๆ ทำหน้าที่ปกป้องคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง
- Network-based Firewall สามารถปกป้องคอมพิวเตอร์ภายในเครือข่ายได้หลายเครื่อง ส่วนใหญ่จำทำได้เพียง Packet Filtering ฒีน้อยมากที่กรองแพ็คเก็ตระดับแอพพลิเคชั่นได้

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

: Host-based or Network-based [2]

- Enterprise Firewall ออกแบบมาสำหรับเครือข่ายขนาดใหญ่และซับซ้อน แต่มีราคาแพงกว่าสองแบบแรกมาก มีฟีเจอร์ชั้นสูง เช่น
  - VPN
  - บริหารจัดการไฟร์วอลล์หลายๆเครื่องได้จากที่เดียว
  - Traffic Monitoring
  - กำหนดนโยบายไปยังแต่ละยูสเซอร์ได้
  - มีความน่าเชื่อถือสูง

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

: Host-based or Network-based [3]

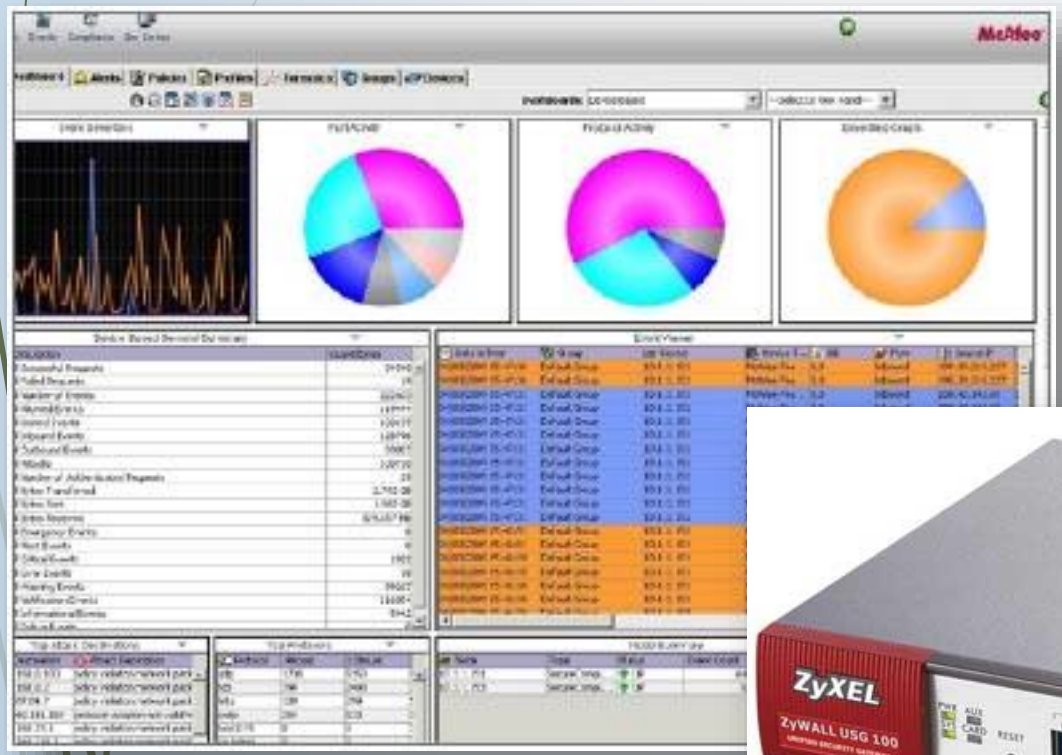
- ราคาของ Host-based Firewall อาจอยู่ประมาณหลักพันบาท ส่วน Enterprise Firewall อาจสูงถึงหลักล้าน
- ไฟร์วอลล์ที่นิยมสำหรับองค์กรทั่วไปจะอยู่ประมาณห้าหมื่นถึงสองแสนบาท แต่จะมีค่าใช้จ่ายเพิ่มขึ้นหากต้องการซื้อฟีเจอร์อื่นๆเพิ่ม
- *การจะเลือกใช้ไฟร์วอลล์ประเภทใดๆ ควรดูจากบริบทขององค์กร นโยบาย และค่าใช้จ่ายเป็นหลัก*

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

: Hardware or Software Firewall

- คำว่าฮาร์ดแวร์ไฟร์วอลล์และซอฟต์แวร์ไฟร์วอลล์เป็นคำที่ใช้แบ่งแยกระหว่างไฟร์วอลล์ที่ติดตั้งมาก่อนบนฮาร์ดแวร์เฉพาะ กับซอฟต์แวร์ไฟร์วอลล์ที่ติดตั้งได้กับระบบปฏิบัติการทั่วไป
- ข้อดีของฮาร์ดแวร์ไฟร์วอลล์คือผู้ใช้ไม่ต้องกังวลเกี่ยวกับการติดตั้งซอฟต์แวร์และการคอนฟิกต่างๆ ส่วนข้อเสียคือเราจะต้องผูกติดกับผลิตภัณฑ์ของบริษัทนั้นเพียงบริษัทเดียว

Software Firewall และ Hardware Firewall



ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

: ฟีเจอร์ที่สำคัญของไฟร์วอลล์

สิ่งที่ควรพิจารณาในการเลือกซื้อไฟร์วอลล์ คือ

- เราต้องการซอฟต์แวร์ไฟร์วอลล์หรือฮาร์ดแวร์ไฟร์วอลล์
- ในองค์กรมีความต้องการใช้งานพร้อมกันกี่คน
- มีความต้องการเชื่อมต่อ VPN พร้อมกันกี่คน และจะใช้ VPN โปรโตคอลใดบ้าง
- ต้องการเชื่อมต่อเข้ากับ SharePoint Server หรือไม่

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์
: ฟีเจอร์ที่สำคัญของไฟร์วอลล์ [2]

- ต้องการใช้ User Interface แบบ Command Line หรือ GUI หรือ Web-based ซึ่งขึ้นอยู่กับชอบและความสามารถของ Admin
- ต้องการไฟร์วอลล์ที่มีความเชื่อถือได้สูงหรือไม่

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์
: ฟีเจอร์ที่สำคัญของไฟร์วอลล์ [3]

ฟีเจอร์ที่อาจต้องจ่ายเงินเพิ่ม เช่น

- Web Caching
- ระบบบริหารจากศูนย์กลางและรายงานต่างๆ
- Spam Filtering หรือ URL Filtering
- Load Balancing หรือ Failover
- การสแกนไวรัส

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์
: ฟีเจอร์ที่สำคัญของไฟร์วอลล์ [4]

- สิ่งที่ควรพิจารณาอีกอย่างหนึ่งคือ “ทรูพุต” (Throughput) หมายถึงอัตราการถ่ายโอนข้อมูล
- ไฟร์วอลล์ที่มีกระบวนการรักษาความปลอดภัยที่มากเกินไปจะส่งผลให้ทรูพุตต่ำ ซึ่งส่งผลต่อประสิทธิภาพโดยรวมของระบบ