



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
 - ▶ ฟังก์ชันที่สำคัญของไฟร์วอลล์



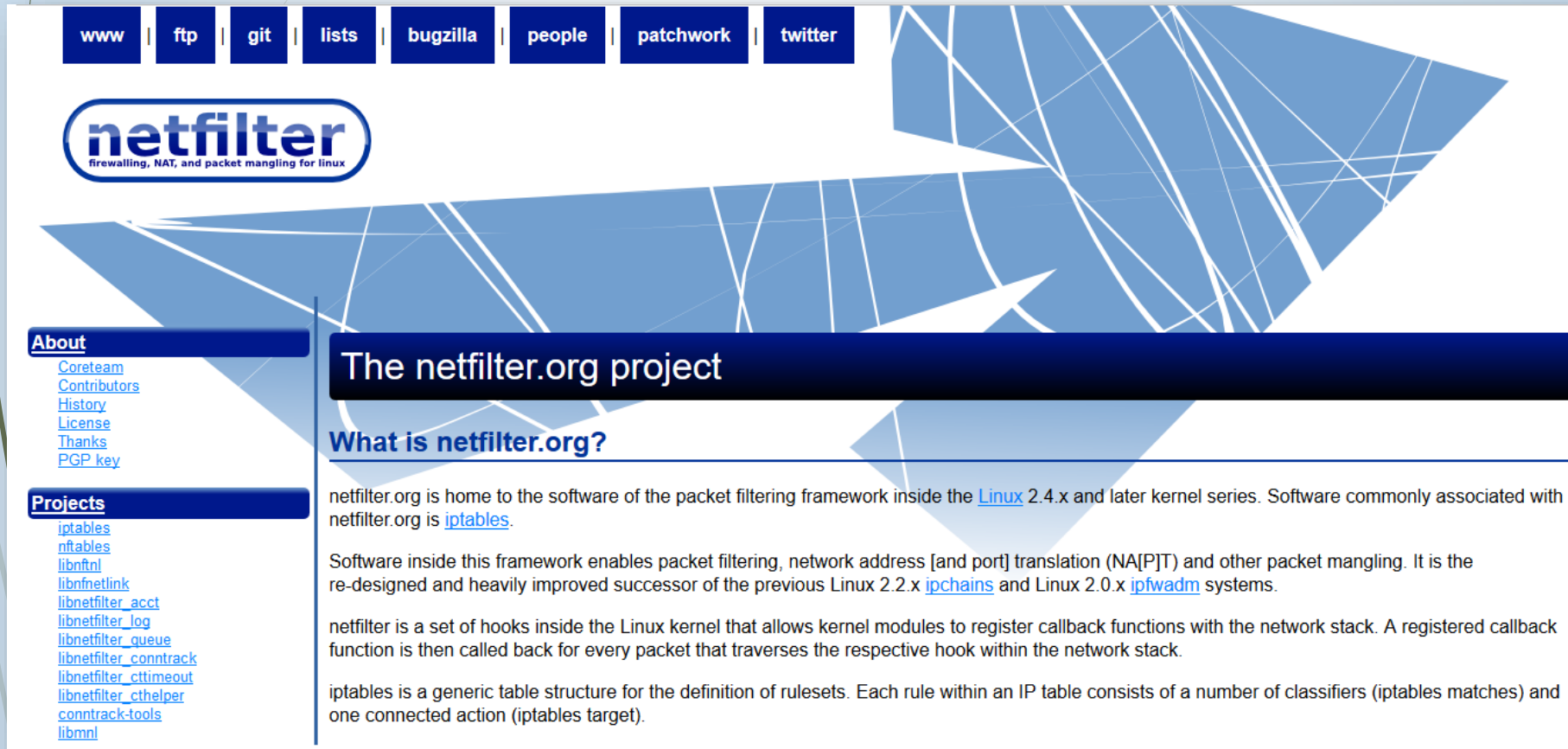
ผลิตภัณฑ์ไฟร์วอลล์

- ▶ ผลิตภัณฑ์ไฟร์วอลล์ที่มีขายตามท้องตลาดมีมากมายหลายยี่ห้อ ในหัวข้อนี้จะกล่าวถึงผลิตภัณฑ์ไฟร์วอลล์ที่ได้รับ ความนิยม 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 | ftp | git | lists | bugzilla | people | patchwork | twitter

netfilter
firewalling, NAT, and packet mangling for linux

About

- [Coreteam](#)
- [Contributors](#)
- [History](#)
- [License](#)
- [Thanks](#)
- [PGP key](#)

Projects

- [iptables](#)
- [nftables](#)
- [libnftnl](#)
- [libnftnetlink](#)
- [libnetfilter_acct](#)
- [libnetfilter_log](#)
- [libnetfilter_queue](#)
- [libnetfilter_conntrack](#)
- [libnetfilter_cttimeout](#)
- [libnetfilter_cthelper](#)
- [conntrack-tools](#)
- [libmnl](#)

The netfilter.org project

What is netfilter.org?

netfilter.org is home to the software of the packet filtering framework inside the [Linux 2.4.x](#) and later kernel series. Software commonly associated with netfilter.org is [iptables](#).

Software inside this framework enables packet filtering, network address [and port] translation (NA[P]T) and other packet mangling. It is the re-designed and heavily improved successor of the previous Linux 2.2.x [ipchains](#) and Linux 2.0.x [ipfwadm](#) systems.

netfilter is a set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack.

iptables is a generic table structure for the definition of rulesets. Each rule within an IP table consists of a number of classifiers (iptables matches) and one connected action (iptables target).

ผลิตภัณฑ์ไฟร์วอลล์

: Linux Firewall : iptables [2]

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

ผลิตภัณฑ์ไฟร์วอลล์

: Check Point Firewall-1

- ▶ เป็นไฟร์วอลล์ที่ได้รับความนิยมมากอีกตัวหนึ่ง สามารถป้องกันการโจมตีได้อย่างมีประสิทธิภาพ
- ▶ สามารถตรวจสอบแพ็คเก็ตได้ตั้งแต่ระดับเน็ตเวิร์คไปจนถึงชั้นแอปพลิเคชัน
- ▶ มีฟีเจอร์ที่สำคัญ เช่น ระบบควบคุมการเข้าถึง การตรวจสอบเนื้อหาข้อมูล การพิสูจน์ทราบตัวตนผู้ใช้ รองรับการทำให้ NAT และ VPN ฯลฯ

เว็บไซต์ของบริษัท Check Point



PRODUCTS / SOLUTIONS

SUPPORT / SERVICES

PARTNERS

COMPANY

CyberDay 2015



WHAT CSOs NEED TO KNOW TO **STAY ONE STEP AHEAD**

#Cyberday2015

NOVEMBER 18, 2015

GRAND HYATT, NEW YORK CITY

REQUEST AN INVITATION ▶

GUEST SPEAKERS:



JOEL BRENNER

Former National Counter Intelligence Executive and Author of "Glass Houses"



CHRIS TARBELL

Former FBI Special Agent and Cybersecurity Expert

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

- ▶ ไฟร์วอลล์ปกติจะมีโครงสร้างง่ายๆ ทำหน้าที่กรองแพ็คเก็ตที่วิ่งผ่านเครือข่าย และตัดสินใจว่าจะให้แพ็คเก็ตนั้นๆ ผ่านไปได้หรือไม่โดยการตรวจดูแฮดเดอร์ของแพ็คเก็ตในเลเยอร์ 3 และ 4
- ▶ ไฟร์วอลล์ระดับสูงจะสามารถกรองแพ็คเก็ตในระดับแอปพลิเคชันได้ ซึ่งจะสามารถกำจัดสแปมเมล ไวรัส หรือเนื้อหาที่ไม่เหมาะสมได้

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์ [2]

- ▶ ไฟร์วอลล์ในปัจจุบันจะทำหน้าที่มากกว่า “ยาม” คือมีการเพิ่มพีเจอร์ใหม่ๆ เข้ามา ซึ่งบางพีเจอร์ก็ไม่ใช่ฟังก์ชันของไฟร์วอลล์โดยตรง เช่น VPN, Gateway, Web Cache
- ▶ ไฟร์วอลล์แบบมัลติฟังก์ชันนี้ เป็นที่แพร่หลายอย่างมากในปัจจุบัน

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

: Host-based or Network-based

- ▶ Host-based Firewall หรือ Personal Firewall มีหลักการทำงานง่ายๆ ทำหน้าที่ปกป้องคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง
- ▶ Network-based Firewall สามารถปกป้องคอมพิวเตอร์ภายในเครือข่ายได้หลายเครื่อง ส่วนใหญ่ทำได้เพียง Packet Filtering ใช้น้อยมากที่กรองแพ็คเก็ตระดับแอปพลิเคชันได้

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]

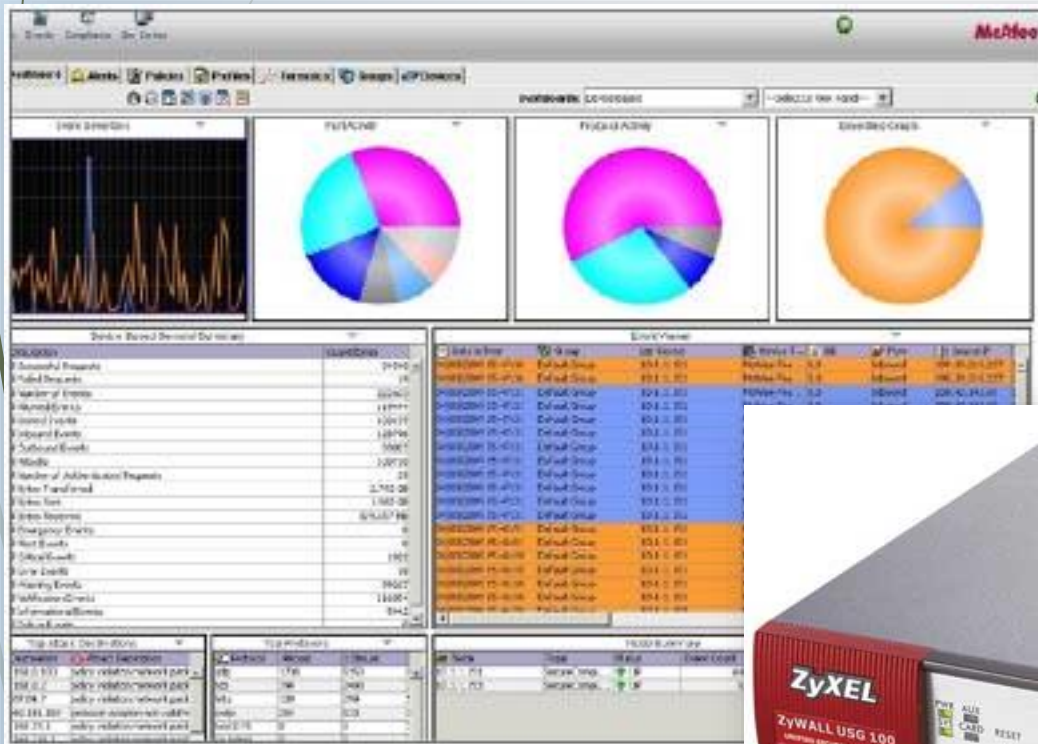
- ▶ ราคาของ Host-based Firewall อาจอยู่ประมาณหลักพันบาท ส่วน Enterprise Firewall อาจสูงถึงหลักล้าน
- ▶ ไฟร์วอลล์ที่นิยมสำหรับองค์กรทั่วไปจะอยู่ประมาณห้าหมื่นถึงสองแสนบาท แต่จะมีค่าใช้จ่ายเพิ่มขึ้นหากต้องการซื้อฟีเจอร์อื่นๆเพิ่ม
- ▶ การจะเลือกใช้ไฟร์วอลล์ประเภทใดๆ ควรดูจากบริบทขององค์กร นโยบาย และค่าใช้จ่ายเป็นหลัก

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์

: Hardware or Software Firewall

- ▶ คำว่าฮาร์ดแวร์ไฟร์วอลล์และซอฟต์แวร์ไฟร์วอลล์เป็นคำที่ใช้แบ่งแยกระหว่างไฟร์วอลล์ที่ติดตั้งมาก่อนบนฮาร์ดแวร์ เฉพาะ กับซอฟต์แวร์ไฟร์วอลล์ที่ติดตั้งได้กับระบบปฏิบัติการทั่วไป
- ▶ ข้อดีของฮาร์ดแวร์ไฟร์วอลล์คือผู้ใช้ไม่ต้องกังวลเกี่ยวกับการติดตั้งซอฟต์แวร์และการคอนฟิกต่างๆ ส่วนข้อเสียคือเราจะต้องผูกติดกับผลิตภัณฑ์ของบริษัทนั้นเพียงบริษัทเดียว

Software Firewall และ Hardware Firewall



ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์ : พีเจอร์ที่สำคัญของไฟร์วอลล์

สิ่งที่ควรพิจารณาในการเลือกซื้อไฟร์วอลล์ คือ

- ▶ เราต้องการซอฟต์แวร์ไฟร์วอลล์หรือฮาร์ดแวร์ไฟร์วอลล์
- ▶ ในองค์กรมีความต้องการใช้งานพร้อมกันกี่คน
- ▶ มีความต้องการเชื่อมต่อ VPN พร้อมกันกี่คน และจะใช้ VPN โพรโตคอลใดบ้าง
- ▶ ต้องการเชื่อมต่อเข้ากับ SharePoint Server หรือไม่

ข้อพิจารณาในการเลือกซื้อไฟร์วอลล์ : พีเจอร์ที่สำคัญของไฟร์วอลล์ [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 : พีเจอร์ที่สำคัญของไฟร์วอลล์ [4]

- ▶ สิ่งที่ต้องพิจารณาอีกอย่างหนึ่งคือ “ทROUGHPUT” (Throughput) หมายถึงอัตราการถ่ายโอนข้อมูล
- ▶ ไฟร์วอลล์ที่มีกระบวนการรักษาความปลอดภัยที่มากเกินไปจะส่งผลให้ทROUGHPUTต่ำ ซึ่งส่งผลต่อประสิทธิภาพโดยรวมของระบบ