การใช้ iptables สำหรับ share internet connection และใช้เป็น firewall

เหมาะสำหรับผู้ที่มีเครื่องคอมพิวเตอร์จำนวนมากในความดูแล และ/หรือมีการเชื่อมต่อกับอินเทอร์เน็ต มีเครื่องเซิร์ฟเวอร์เปิดให้บริการกับสาธารณชน เช่น web service, ftp service, mail service เป็นต้น และต้องการเพิ่มความปลอดภัยให้กับระบบ เนื่องจาก firewall ทำหน้าที่ควบคุมการเข้าออกของข้อมูลใน port ที่ได้รับอนุญาตเท่านั้น ดังนั้นผู้ที่จะเขียน rule ของ firewall ได้ต้องมีความรู้เกี่ยวกับ TCP/IP พอสมควร และขอย้ำตรงนี้อีกว่า firewall ไม่ใช่อุปกรณ์ป้องกันการบุกรุกระบบที่สมบูรณ์ 100% เพราะการโจมตีที่เกิดขึ้นในปัจจุบันนั้นมักจะโจมตีผ่าน port ที่เป็นที่รู้จัก เช่น 21, 22, 25, 53, 80 ซึ่ง firewall มักจะอนุญาตให้ข้อมูลเข้าออกผ่านทาง port เหล่านี้เสมอ ดังนั้นควรใช้เครื่องมืออื่นๆ ช่วย การใช้ iptables จะต้องสร้าง chain ให้ระบบโดยเขียน Parameter ต่อท้ายซึ่งมี Parameter หลักที่จำเป็นดังนี้

-A หมายถึง การเพิ่ม Chain ให้ระบบ
-F หมายถึง สั่งลบ Chain เดิมที่เคยสร้างไว้ทั้งหมด
-N หมายถึง ตั้งชื่อ Chain ใหม่
-P หมายถึง การกำหนด Policy
-X หมายถึง ลบชื่อ Chain
-I หมายถึง เพิ่ม rule ใหม่ ใน chain
-s หมายถึง (Source) IP Address ต้นทาง
-d หมายถึง (Destination) IP Address ปลายทาง
-p หมายถึง Protocal เช่น tcp, udp, icmp
- -dport หมายถึง (Destination Port) หมายเลขหรือชื่อ Port ปลายทาง
- -sport หมายถึง (Source Port) หมายเลขหรือชื่อ Port ต้นทาง
-j หมายถึง การกำหนดให้เชื่อมต่อกันระหว่างต้นทาง (Source) กับปลายทาง (Destination) ที่นิยมใช้คือ ACCEPT, REJECT, DENY, MASQUERADE และ REDIRECT
-o หมายถึง packet ที่จะ match กับ rule นี้กำลังจะเดินผ่าน interface ที่ระบุไว้ เช่น -o eth0
-i หมายถึง packet ที่จะ match กับ rule นี้ต้องเข้ามาจาก interface ที่กำหนด เช่น -i eth0
-m หมาย ถึง เป็น option ที่ใช้กรอง packet ที่ถูกส่งเข้ามา – ออกไป ของ eth0 หรือ ppp0
Input คือ ส่วนที่ใช้รับค่าต่างๆ จากภายนอกเข้า Server
Output คือ ส่วนที่ส่งค่าต่างๆ ออกจาก Server ไปยังภายนอก
Forward คือ ส่วนที่ต้องการให้ลูกข่ายติดต่อออกไปภายนอก Server

The State Match
รูปแบบการใช้งาน: -m state หรือ – -match state เป็นโมดูลที่ใช้ประโยชน์ได้เป็นอย่างดี มี options ให้ใช้งานดังนี้
NEW รูปแบบการใช้งาน : **-m state –state new** หรือ **–match state –state new**
หมายถึง packet ที่เป็นตัวสร้าง connection ใหม่
ESTABLISHED รูปแบบการใช้งาน: **-m state –state established** หรือ **–match state –state** established
หมายถึง packet ที่เกี่ยวข้องกันกับ connection ที่สร้างไว้แล้ว เช่น echo-reply packet หรือ packet ที่ส่งข้อมูลออกไปจาก web server เมื่อมี request web service เข้ามา

RELATED รูปแบบการใช้งาน: **-m state –state related** หรือ **–match state –state related**
เป็น packet ที่เกี่ยวข้องกับ connection ที่สร้างไว้แล้ว แต่ไม่ใช่ส่วนหนึ่งส่วนใดของ connection นั้น เช่น FTP data packet (port 20) ที่เกิดขึ้นจากการใช้คำสั่งใน FTP command (port 21)
INVALID รูปแบบการใช้งาน: **-m state –state invalid** หรือ **–match state –state invalid**
เป็น packet ที่ไม่เกี่ยวข้องกับส่วนอื่นเลย เช่น icmp echo-reply ที่เกิดขึ้น โดยที่ไม่มีเครื่องได้ในระบบส่ง echo-request ออกไปเลย (กรณีเช่นนี้เกิดขึ้นได้เนื่องจากอาจจะโดนโจมตีแบบ Smurf attack)

วิธีการ set iptables สำหรับ share internet และการทำ firewall
ให้ลบ rule ทั้งหมดที่มีทุก chain ใน file **/etc/sysconfig/iptables**
iptables –flush
iptables -t nat –F *(ลบ chain nat table ที่ใช้สำหรับการแปลงแอดเดรส)*
iptables -t mangle –F *(ลบ chain mangle table ที่ใช้สำหรับการเปลี่ยนแปลงหรือแก้ไข packet)*
iptables -t filter –F *(ลบ chain filter table ที่ใช้สำหรับกรอง packet)*
iptables –X *(ลบ chain ที่ไม่มี rule ซึ่งสามารถลบ user-define chain ที่ไม่มี rule ได้)*

โหลด module ที่จำเป็นต้องใช้ในการ share internet connection โดยใช้คำสั่ง insmod ในการ load module
insmod ip_tables
insmod ip_conntrack
insmod ip_conntrack_ftp
insmod iptable_nat
insmod ip_nat_ftp

เปิดการทำงานของ Masquerading และการ forward packet (การทำ MASQUERADE เป็นการทำให้ Server สามารถ Share Internet ให้เครื่องลูกข่ายเข้าใช้งาน Internet ได้)
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE *(ทำ MASQUERADE สำหรับทุก packet ที่วิ่งผ่าน ppp0)*
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE *(ทำ MASQUERADE สำหรับทุก packet ที่วิ่งผ่าน eth0)*
iptables -A FORWARD -i eth0 -j ACCEPT *(packet ถูกส่งเข้ามายัง FORWARD chain โดยวิ่งผ่าน eth0)*
echo 1 > /proc/sys/net/ipv4/ip_forward *(เพื่อกำหนดให้ IP forwarding เป็น Enable เพื่อให้ Linux box สามารถ forward ip packet ได้)*
ยอมให้ connections ที่ผ่าน rule แล้วไม่ต้องถูกตรวจสอบจาก firewall อีก
iptables -A FORWARD -i ppp0 -o eth0 -m state –state ESTABLISHED,RELATED -j ACCEPT *(เป็นคำสั่งที่ทำให้ iptables นี้ตรวจสอบ packet ว่ามีเป็นส่วนหนึ่งของ connection ที่สร้างไว้แล้วหรือไม่ (ESTABLISHED) ถ้าใช่ก็จะปล่อยให้ผ่านไป (ACCEPT) โดยการส่งข้อมูลเข้าผ่านทาง ppp0 (Modem) และให้ส่งข้อมูลออกทาง eth0 (Lan Card) โดยมีความสัมพันธ์ (related) กันระหว่าง ppp0 กับ eth0)*
iptables -A FORWARD -i eth0 -o ppp0 -m state –state ESTABLISHED,RELATED -j ACCEPT
(เป็นคำสั่งที่ทำให้ iptables นี้ตรวจสอบ packet ว่ามีเป็นส่วนหนึ่งของ connection ที่สร้างไว้แล้วหรือไม่

(ESTABLISHED) ถ้าใช่ก็จะปล่อยให้ผ่านไป (ACCEPT) โดยการส่งข้อมูลเข้าผ่านทาง eth0 (LanCard) และให้ส่งข้อมูลออกทาง ppp0 (Modem) โดยมีความสัมพันธ์ (related) กันระหว่าง ppp0 กับ eth0)

ยอมให้มีการเชื่อมโยงกันทุกประเภทภายในเครือข่าย (internal network)

iptables -A INPUT -s 192.169.0.0/16 -d 192.169.0.0/16 -j ACCEPT *(เป็นการรับข้อมูลเข้าโดยมี source IP (ต้นทาง) ที่ 192.169.0.0/16 และ destination IP (ปลายทาง) ที่ 192.169.0.0/16)*

iptables -A OUTPUT -s 192.169.0.0/16 -d 192.169.0.0/16 -j ACCEPT

(เป็นการส่งข้อมูลออกโดยมี source IP (ต้นทาง) ที่ 192.169.0.0/16 และ destination IP (ปลายทาง) ที่ 192.169.0.0/16) ##(หมายเลขIP/netmask)

ยอมให้มีการ forward packet จากเครื่องลูกข่าย (clients) ไปยังภายนอก network ที่อยู่

iptables -A FORWARD -m state –state NEW -i eth0 -j ACCEPT *(packet ที่เป็นตัวสร้าง connection ใหม่ โดยให้ส่งข้อมูลเข้าทาง eth0 (Lan Card))*

iptables -A FORWARD -m state –state ESTABLISHED,RELATED -j ACCEPT *(เป็นคำสั่งที่ทำให้ iptables สามารถทำงานได้ในรูปแบบของ stateful inspection ที่แท้จริง โดย rule นี้จะตรวจสอบ packet ว่ามีเป็นส่วนหนึ่งของ connection ที่สร้างไว้แล้วหรือไม่ (ESTABLISHED) ถ้าใช่ก็จะปล่อยให้ผ่านไป (ACCEPT) และในกรณีที่เครื่องภายในเครือข่ายเรียกใช้ ftp ไปยังเครื่องอื่นในอินเทอร์เน็ตนั้น คำสั่งที่ส่งไปจะใช้ destination port เป็น 21 แต่ data port ที่ใช้สำหรับรับส่งข้อมูลใน ftp นั้นเป็น port 20 ซึ่ง port ที่เกิดขึ้นนี้ถือว่ามีความสัมพันธ์ (related) กับ port 21 ดังนั้นจึงสามารถรับส่งไฟล์ผ่าน port 20 ได้โดยไม่จำเป็นต้องสร้าง rule เพิ่มเติมแต่อย่างใด)*

iptables -I FORWARD -i ppp0 -d 0.0.0.0 -j ACCEPT *(เพิ่ม chain ให้ส่ง packet เข้ามาทาง ppp0 และ destination IP ปลายทางที่ 0.0.0.0)*

iptables -I FORWARD -s 192.169.0.0/16 -d 0.0.0.0 -j ACCEPT *(เพิ่ม chain ให้ส่ง packet เข้ามาทาง Source IP ที่ 192.169.0.0/16 และ destination ปลายทางที่ 0.0.0.0)*

ให้ยอมรับ Stateful Traffic คือ การส่ง packet ผ่านชั้น Network ตาม OSI Model 7 Layer ต้องศึกษาเรื่อง OSI Model 7 Layer

iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT

สมมติว่าต้องการให้การเข้าถึง SSH เข้าใช้ได้เฉพาะวันจันทร์ถึงวันศุกร์ระหว่างเวลา 09:00 ถึง 18:00

iptables -A INPUT -p tcp -s 0/0 --sport 513:65535 -d 202.54.1.20 --dport 22 -m state --state NEW,ESTABLISHED -m time --timestart 09:00 --timestop 18:00 --days Mon,Tue,Wed,Thu,Fri -j ACCEPT

อนุญาต traffic จาก loopback interface

iptables -A INPUT -i lo -j ACCEPT *(เป็นการรับข้อมูลเข้า Server ทาง Loopback ของ Lancard)*

iptables -A OUTPUT -o lo -j ACCEPT *(เป็นการส่งข้อมูลออกจาก Server ทาง Loopback ของ Lancard)*

การ ทำ redirect นั้นเป็นหนึ่งในรูปแบบของการทำ Destination NAT แบบพิเศษ เช่น เปลี่ยน web traffic ธรรมดาให้ผ่านไปยัง squid proxy (transparent) redirect พอร์ต 80 ไปยังพอร์ต 8080 เพื่อให้การใช้ WWW ผ่าน squid proxy

iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 80 -j REDIRECT –to-port 8080

จำเป็นต้องมีการ set ที่ squid เพิ่มเติมด้วย

เซ็ต default policy ของ INPUT traffic ให้เป็น drop ยกเว้นจะมีการกำหนด rule เป็นอย่างอื่น

iptables -P INPUT DROP *(packet ถูกส่งเข้ามาและไม่ match กับ rule ใดๆ มันก็จะถูก DROP ทันที)*

ไม่อนุญาตให้มี INPUT connection จากภายนอก (ยกเว้น 192.169.0.0/16)
iptables -A INPUT -s ! 192.169.0.0/16 -p all -j DROP *(packet ที่ถูกส่งเข้ามายัง server อนุญาตให้ส่งได้เฉพาะเครื่องที่มี IP อยู่ในช่วง 192.169.0.0/16 เท่านั้น IP อื่นไม่อนุญาต)*
เซ็ต policy ของ OUTPUT traffic เป็น ACCEPT ยกเว้นจะมีการกำหนด rule เป็นอย่างอื่น
iptables -P OUTPUT ACCEPT *(packet ถูกส่งออกไปไม่ match กับ rule ใดๆ มันก็จะถูก DROP ทันที)*
ห้าม connection ไปยังภายนอกจากพอร์ต 31337, 31335, 27444, 27665, 20034, 9704, 1433, 2049, 2432, 5999, 6068, 6900 ซึ่งส่วนใหญ่พอร์ตเหล่านี้จะเป็นพอร์ตที่ backdoor ใช้
iptables -A OUTPUT -o eth0 -p tcp –dport 31337 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 31335 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 27444 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 27665 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 20034 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 9704 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 1433 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 2049 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 2432 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 5999 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 6068 -j DROP
iptables -A OUTPUT -o eth0 -p tcp –sport 6900 -j DROP

save rule ที่สร้างขึ้นมาใหม่ และ restart iptables
service iptables save
service iptables restart
หลังจากใช้ rules ใหม่ของ iptables แล้วแต่ถ้ายังใช้ www ไม่ได้อาจอาจจะต้อง restart squid ใหม่
โดยใช้คำสั่ง
service squid stop
service squid start
หรืออาจจะต้องรีบูตเครื่องใหม่ด้วย

- **แก้ไฟล์ /etc/sysctl.conf**

Controls IP packet forwarding
net.ipv4.ip_forward = 1 (เซ็ตให้เป็น enable IP forwarding เป็นการกำหนดให้ policy เป็น ACCEPT ทำให้ packet สามารถถูก forward ไปยังจุดหมายที่ต้องการได้) สำหรับการใช้งาน iptables ในการใช้งาน Internet สามารถที่จะกำหนดขอบเขตในการทำงานเพิ่มเติมได้ ซึ่งจะช่วยในการป้องกันการบุกรุกจากผู้ที่ไม่หวังดีได้ ตามความพอใจของ Admin ที่ดูแลระบบและการใช้งาน Internet ภายในองค์กร

สร้าง Shell สำหรับ firewall.iptables ทำงานทุกครั้งเมื่อเปิดเครื่อง

เพิ่มคำสั่งใน /etc/rc.local ทั้งนี้ไฟล์ firewall.iptables ต้องอยู่ใน /etc

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
sh /etc/firewall.iptables
```

แก้ไขไฟล์ /etc/resolv.conf

```
search nakorn.ac.th
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Clear Cache Squid ควรสร้างไว้เป็นไฟล์ /etc/clearsquid.sh และตั้งการทำงานใน crontab

```
# /etc/init.d/squid stop                    หรือ service squid stop
# cd /var/spool/squid/
#  rm  -Rf  *
#  squid –z
# /etc/init.d/squid start                   หรือ service squid start
```

● ติดตั้ง Squid ทำ Proxy Server แบบ Transparent

To configure squid proxy as transparent proxy you need to edit squid.conf file in /etc/squid/squid.conf as follow:

```
acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl localnet src 192.169.0.0/16          #หรือ acl localnet src 192.169.0.0/255.255.0.0
acl SSL_ports port 443 563
acl Safe_ports port 80        # http
acl Safe_ports port 21        # ftp
acl Safe_ports port 443       # https
acl Safe_ports port 70        # gopher
acl Safe_ports port 210       # wais
acl Safe_ports port 1025-65535    # unregistered ports
```

```
acl Safe_ports port 280        # http-mgmt
acl Safe_ports port 488        # gss-http
acl Safe_ports port 591        # filemaker
acl Safe_ports port 777        # multiling http
acl CONNECT method CONNECT

http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

http_access allow localnet
http_access allow localhost
http_access deny all
http_reply_access allow localnet
http_reply_access deny all

icp_access allow localnet
icp_access deny all

http_port 8080 transparent

hierarchy_stoplist cgi-bin ?

cache_mem 256 MB
cache_dir ufs /var/spool/squid 4096 16 256  # หรือ cache_dir ufs /usr/local/squid/cache 100 16
256
cache_mgr admin@email.com
cache_effective_user squid
cache_effective_group squid

access_log /var/log/squid/access.log squid

refresh_pattern ^ftp:          1440    20%     10080
refresh_pattern ^gopher:    1440      0%     1440
refresh_pattern (cgi-bin|\?)       0      0%     0
refresh_pattern .                  0     20%     4320

visible_hostname nakorn.ac.th                    # your full hostname

icp_port 3130
always_direct    allow    all
```

forwarded_for off

coredump_dir /var/spool/squid

The most important line is “http_port 8080 transparent” : This line means, Squid proxy run as transparent proxy at port 8080 (by default 3128). Later you need to edit the iptables to bypass every request/response connection through this port.
กรณีที่กำหนดเป็น cache_dir ufs /usr/local/squid/cache 100 16 256 ต้องสร้าง directory /usr/local/squid/cache และเปลี่ยนความเป็นเจ้าของด้วย chown squid:squid /usr/local/squid/cache

Create swap directory squid
[root@Centos6 ~]# squid –zD

Block File & WEB for squid

```
acl blockx url_regex ‘/etc/block.txt’                 # url of web to block เช่น http://sex.com
acl blocklist_files urlpath_regex –i ‘/etc/files.txt’ # file or extension to block เช่น .torrent$
acl morning time M T W H F 8:30-12:00                 # set time to block in morning
acl lunch time M T W H F 13:00-16:00                  # set time to block in lunch

http_access deny blockx morning
http_access deny blockx lunch
http_access deny blocklist_files morning
http_access deny blocklist_files lunch

deny_info http://192.169.0.1/block.html morning   # if when block goto url
deny_info http://192.169.0.1/block.html lunch     #if when block goto url
```

• Iptables Configurations

To make Squid as the transparent proxy (“man in the middle”), you need to configure the **iptables**. I got this script to help you:

```
#!/bin/sh
# ------------------------------------------------------------------------------
# See URL: http://www.cyberciti.biz/tips/linux-setup-transparent-proxy-squid-howto.html
# (c) 2006, nixCraft under GNU/GPL v2.0+<br />
# ------------------------------------------------------------------------------
# squid server IP
SQUID_SERVER="192.169.0.1"
```

```
# Interface connected to Internet
INTERNET="eth0"

# Interface connected to LAN
LAN_IN="eth1"
# Squid port
SQUID_PORT="3128"

# DO NOT MODIFY BELOW
# Clean old firewall
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables –X

# Load IPTABLES modules for NAT and IP conntrack support
modprobe ip_conntrack
modprobe ip_conntrack_ftp
# For win xp ftp client
#modprobe ip_nat_ftp
echo 1 > /proc/sys/net/ipv4/ip_forward

# Setting default filter policy
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
# Unlimited access to loop back
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Allow UDP, DNS and Passive FTP
iptables -A INPUT -i $INTERNET -m state --state ESTABLISHED,RELATED -j ACCEPT
# set this system as a router for Rest of LAN
iptables --table nat --append POSTROUTING --out-interface $INTERNET -j MASQUERADE
iptables --append FORWARD --in-interface $LAN_IN -j ACCEPT
```

 # unlimited access to LAN
iptables -A INPUT -i $LAN_IN -j ACCEPT
iptables -A OUTPUT -o $LAN_IN -j ACCEPT

 # DNAT port 80 request comming from LAN systems to squid 3128 ($SQUID_PORT) aka transparent proxy
iptables -t nat -A PREROUTING -i $LAN_IN -p tcp --dport 80 -j DNAT --to $SQUID_SERVER:$SQUID_PORT
 # if it is same system
iptables -t nat -A PREROUTING -i $INTERNET -p tcp --dport 80 -j REDIRECT --to-port $SQUID_PORT

 # DROP everything and Log it
iptables -A INPUT -j LOG
iptables -A INPUT -j DROP

● ตรวจสอบว่าโดเมนไหนใช้ IP Address เดียวกันบ้าง

http://www.yougetsignal.com/tools/web-sites-on-web-server/

● DHCP Server

1. Configuration of eth1 interface

[root@Centos6 ~]# nano /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
NETWORK=192.169.0.0
NETMASK=255.255.0.0
IPADDR=192.169.0.1
USERCTL=no

2. Install DHCP deamon by yum

[root@Centos6 ~]# yum –y install dhcp

3. Configure DHCP subnet for our network

[root@Centos6 ~]# cat /etc/dhcp/dhcpd.conf
#
 # DHCP Server Configuration file.
 # see /usr/share/doc/dhcp/dhcpd.conf.sample*
 # see 'man 5 dhcpd.conf'
#

```
ddns-update-style none;
option domain-name-servers 8.8.8.8, 8.8.4.4;
option domain-name "centos.local";
default-lease-time 600;
max-lease-time 7200;
# option subnet-mask 255.255.0.0;
# option broadcast-address 192.169.255.255;
# option routers 192.169.0.1;
authoritative;
log-facility local7;
subnet 192.169.0.0 netmask 255.255.0.0 {
        option routers 192.169.0.1;
        range 192.169.0.10 192.169.255.250;
        # option broadcast-address 192.168.255.255;
}
```

4. Configure listening Interface to DHCP

```
[root@Centos6 ~]# nano /etc/sysconfig/dhcpd
# Add command line options here
DHCPDARGS=eth1
```

5. สร้างไฟล์เก็บข้อมูลให้ dhcp server เก็บค่าที่ได้ leases IP เครื่องลูกข่าย

```
[root@Centos6 ~]# touch /var/lib/dhcpd/dhcpd.leases
[root@Centos6 ~]# chmod 777 /var/lib/dhcpd/dhcpd.leases
```

6. Start DHCP Server on CentOS

```
[root@Centos6 ~]# /etc/init.d/dhcpd restart
Starting dhcpd: [ OK ]
```

7. Make the dhcp server start at boot time

```
[root@Centos6 ~]# chkconfig dhcpd on
```

8. Client gets IP Address from DHCP Server

```
[root@Centos6 ~]# ip addr
```

9. ตั้งค่า iptables สำหรับ DHCP อย่างง่ายไม่ได้ป้องกันอะไร เพียงบังคับให้ผ่าน Proxy เท่านั้น

```
iptables –F
iptables –P INPUT ACCEPT
iptables –P FORWARD ACCEPT
iptables –P OUTPUT ACCEPT
iptables –t nat –A POSTROUTING –s 192.169.0.0/16 –o eth0 –j MASQUERADE
iptables –A FORWARD –s 192.169.0.0/16 –j ACCEPT
iptables –t nat –A PREROUTING –i eth1 –p tcp --dport 80 –j DNAT –to 192.169.0.1:3128
iptables –t nat –A PREROUTING –i eth0 –p tcp --dport 80 –j REDIRECT --to-port 3128
```

iptables –A INPUT –m state --state NEW –m tcp –p tcp --dport 80 –j ACCEPT
iptables –A INPUT –m state --state NEW –m tcp –p tcp --dport 3128 –j ACCEPT
iptables –A FORWARD –j DROP
หรือใช้เพียง
iptables –F
iptables –t nat –F
iptables –t nat –A POSTROUTING –s 192.169.0.0/16 –o eth0 –j MASQUERADE
iptables –t nat –A PREROUTING –i eth1 –p tcp --dport 80 –j REDIRECT --to-port 8080
iptables –A INPUT –p tcp --dport 3128 –j ACCEPT

10. สร้างลิ้งค์ iptables ให้เปิดอ่านทุกครั้งเมื่อเปิดเครื่อง
เพิ่มลงในไฟล์ rc.local
sh /etc/firewall.iptables

● WEB Server on Centos

1. ปิดการทำงานของ SELINUX เสียก่อน
[root@Centos6 ~]# nano /etc/selinux/config
เปลี่ยนจาก SELINUX=enforcing เป็น SELINUX=disabled
สั่งปิด SELINUX โดยยังไม่ต้อง Restart ใหม่
[root@Centos6 ~]# setenforce 0

2. ติดตั้ง WEB Server
[root@Centos6 ~]# yum –y install httpd httpd-manual mod_ssl
[root@Centos6 ~]# yum –y install mysql mysql-server mysql-devel
[root@Centos6 ~]# yum –y install php php-mysql php-cli php-mbstring
หรือ
yum –y install php php-common php-cli php-devel php-mysql php-gd php-imap
php-mbstring php-mhash php-pear php-xml php-xmlrpc

3. แก้ไขให้รองรับภาษาไทย
[root@Centos6 ~]# nano /etc/httpd/conf/httpd.conf
DefaultLanguage th
AddLanguage th .th
LanguagePriority th en da nl ...
AddCharset TIS-620 .tis-620 .th

4. แก้ไข /etc/httpd/conf/httpd.conf ให้เป็นไปตามด้านล่างเพิ่มเติม
ServerTokens Prod
KeepAlive On
ServerName www.nakorn.ac.th:80
Options FollowSymLinks ExecCGI

AllowOverride All
DirectoryIndex index.html index.htm index.php index.cgi
ServerSignature off

5. แก้ไขไม่ให้แสดงรายชื่อ File ใน Directory

Options Indexes FollowSymLinks เอา Indexes ออกเป็น Options FollowSymLinks

6. ให้ User มีเว็บของตนเองได้

ค้นหาคำว่า #UserDir disable เปลี่ยนเป็น UserDir public_html และให้มีข้อความเหมือนข้างล่างนี้

```
<Directory /home/*/public_html>
        AllowOverride
        All
        Options ExecCGI
        <Limit GET POST OPTIONS>
                Order allow,deny
                Allow from all
        </Limit>
        <LimitExcept GET POST OPTIONS>
                Order deny,allow
                Deny from all
        </LimitExcept>
</Directory>
```

Directory ของ User ต้องมีโหมดเป็น 711 ด้วยคำสั่ง chmod 711 /home/userid สร้าง Directory ชื่อ public_html ใน home ของ User และเปลี่ยนโหมดเป็น 755

7. สร้าง Virtual host

[root@Centos6 ~]# nano /etc/httpd/conf/httpd.conf ไม่มีให้ต่อท้ายไฟล์

```
NameVirtualHost *:80
<VirtualHost *:80>
        DocumentRoot /var/www/html
        ServerName www.nakorn.ac.th                 # Host name ของ Server
        ServerAdmin webmaster@nakorn.ac.th          # E-Mail ของ root
        ErrorLog logs/virtual.host-error_log
        CustomLog logs/virtual.host-access_log combined
</VirtualHost>
```

8. แก้ไข php.ini

[root@Centos6 ~]# nano /etc/php.ini

upload_max_filesize = 2M เป็น 20M
max_execution_time = 30 เป็น 300
memory_limit = 32M เป็น 128M
post_max_size = 8M เป็น 20M

session.auto_start = 0 เป็น 1

register_globals off เป็น on

9. กำหนดให้ httpd ทำงานตอนเปิดเครื่องทุกครั้ง

[root@Centos6 ~]# chkconfig httpd on

10. firewall.iptables สำหรับ Web Server

```
iptables –F
iptables –P INPUT ACCEPT
iptables –P FORWARD ACCEPT
iptables –P OUTPUT ACCEPT
iptables –A INPUT –i eth0 –p tcp –m tcp --dport 80 --syn –j ACCEPT
iptables –A INPUT –i eth0 –p tcp –m tcp --dport 10000 --syn –j ACCEPT
iptables –A INPUT –i eth0 –p tcp –m tcp --dport 3306 --syn –j ACCEPT
iptables –A FORWARD –j DROP
```

• DNS Server [port 53]

1. Install BIND

[root@Centos6 ~]# yum –y install bind caching-nameserver

2. **Configure BIND** from example Global IP [202.143.143.18/255.255.255.240] Private IP [192.169.0.0/16] Domain name [nakorn.ac.th]

[root@Centos6 ~]# nano /etc/named.conf หรือ nano /var/named/chroot/var/named/named.conf

```
#Create new
options {
        directory “/var/named”;
        allow-query { localhost; 192.169.0.0/16; };
        allow-transfer { localhost; 192.169.0.0/16; };
        recursion yes;
};
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
}
view “internal” {
        match-clients {
                localhost;
                192.169.0.0/16;
        };
        zone “.” IN {
                type hint;
```

```
        file “named.ca”;
    };
    zone “nakorn.ac.th” IN {
        type master;
        file “nakorn.ac.th.lan”;
        allow-update { none; };
    };
    zone “0.169.192.in-addr.arpa” IN {
        type master;
        file “0.169.192.db”;
        allow-update { none; };
    };
    zone “localdomain” IN {
        type master;
        file “localdomain.zone”;
        allow-update { none; };
    };
    zone “localhost” IN {
        type master;
        file “localhost.zone”;
        allow-update { none; };
    };
    zone “0.0.127.in-addr.arpa” IN {
        type master;
        file “named.local”;
        allow-update { none; };
    };
    zone “255.in-addr.arpa” IN {
        type master;
        file “named.broadcast”;
        allow-update { none; };
    };
    zone “0.in-addr.arpa” IN {
        type master;
        file “named.zero”;
        allow-update { none; };
    };
};
```

```
view “external” {
        match-clients { any; };
        allow-query { any; };
        recursion no;
        zone “nakorn.ac.th” IN {
                type master;
                file “nakorn.ac.th.hosts”;
                allow-update { none; };
        };
        zone “18.143.143.202.in-addr.arpa” IN {
                type master;
                file “18.143.143.202.db”;
                allow-update { none; };
        };
};
Include “/etc/rndc.key”;
```

3. Create zone file

Internal zone for name to ip

```
[root@Centos6 ~]# nano /var/named/nakorn.ac.th.lan
$TTL 86400
@       IN      SOA     ns1.nakorn.ac.th.       root.nakorn.ac.th. (
        2013070201      ; Serial
        28800           ; Refresh
        14400           ; Retry
        604800          ; Expire
        86400           ; Minimum TTL
)
@       IN      NS      ns1.nakorn.ac.th.               # define name server
        IN      MX      10      ns1.nakorn.ac.th.       # define MAIL exchanger
        IN      A       192.169.0.1                     # define internal IP address of name server
ns1     IN      A       192.169.0.1                     # define IP address and hostname
```

External zone for name to ip

```
[root@Centos6 ~]# nano /var/named/nakorn.ac.th.hosts
$TTL 86400
@       IN      SOA     ns1.nakorn.ac.th.       root.nakorn.ac.th. (
        2013070201      ; Serial
        28800           ; Refresh
```

```
        14400       ; Retry
        604800      ; Expire
        86400       ; Minimum TTL
)
IN      NS      ns1.nakorn.ac.th.               # define name server
IN      A       202.143.143.18                  # define external IP address of name server
IN      MX      10      ns1.nakorn.ac.th.       # define MAIL exchanger
ns1     IN      A       202.143.143.18          # define IP address and hostname
```

Internal zone for ip to name

```
[root@Centos6 ~]# nano /var/named/0.169.192.db
$TTL 86400
@       IN      SOA     ns1.nakorn.ac.th.       root.nakorn.ac.th. (
        2013070201  ; Serial
        28800       ; Refresh
        14400       ; Retry
        604800      ; Expire
        86400       ; Minimum TTL
)
IN      NS      ns1.nakorn.ac.th                # define name server
IN      PTR     nakorn.ac.th.                   # define range that this domain name is in
IN      A       255.255.0.0
1       IN      PTR     ns1.nakorn.ac.th.       # define IP address and hostname
```

External zone for ip to name

```
[root@Centos6 ~]# nano /var/named/18.143.143.202.db
$TTL 86400
@       IN      SOA     ns1.nakorn.ac.th.       root.nakorn.ac.th. (
        2013070201  ; Serial
        28800       ; Refresh
        14400       ; Retry
        604800      ; Expire
        86400       ; Minimum TTL
)
IN      NS      ns1.nakorn.ac.th                # define name server
IN      PTR     nakorn.ac.th.                   # define range that this domain name is in
IN      A       255.255.255.240
18      IN      PTR     ns1.nakorn.ac.th.       # define IP address and hostname
```

4. สอบถาม hostname

[root@Centos6 ~]# uname –n

5. Make sure server can resolve domain names or IP address

[root@Centos6 ~]# dig ns1.nakorn.ac.th.

● Setup RADIUS Server และ Chilli Hotspot Server

1. Install radius

[root@Centos6 ~]# yum –y install freeradius freeradius-mysql

2. แก้ไข /etc/raddb/radius.conf

user = radiusd	เป็น	# user = radiusd	
group = radiusd	เป็น	# groupd = radiusd	
# $INCLUDE ${confdir}/sql.conf	เป็น	$INCLUDE ${confdir}/sql.conf	
# sql	เป็น	sql	*มี 2 ที่*

เพิ่มข้อความใน tag authorize { ... }

```
noresetcounter
dailycounter
monthlycounter
```

เพิ่มข้อความก่อนบรรทัด sqlcounter dailycounter { ... }

```
sqlcounter noresetcounter {
        counter-name = Max-All-Session-Time
        check-name = Max-All-Session
        key = User-Name
        reset = never
        query = “SELECT SUM(AcctSessionTime) FROM radacct WHERE UserName='%{%k}'”
}
```

3. แก้ไข /etc/raddb/sql.conf

```
login = “root”
password = “123456”          # password mysql
radius_db = “radius”
```

4. แก้ไข /etc/raddb/clients.conf

secret = testing123	เป็น	secret = mytestkey

5. แก้ไข /etc/sysctl.conf

net.ipv4.ip_forward = 0	เป็น	net.ipv4.ip_forward = 1

สั่งให้ทำงานทันทีด้วยคำสั่ง # echo “1” > /proc/sys/net/ipv4/ip_forward

6. แก้ไข LAN Card (eth1) /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=none
```

7. แก้ไข /etc/chilli.conf

net 192.168.182.0/24 เป็น net 10.0.1.0/24 *# IP วงที่ต้องการแจก*
radiusserver1 rad01.chillispot.org เป็น radiusserver1 127.0.0.1
radiusserver2 rad02.chillispot.org เป็น radiusserver2 127.0.0.1
radiussecret testing123 เป็น radiussecret mytestkey
#uamserver https://radius.chillisport.org /hotsportlogin
เป็น uamserver https://10.0.1.1/wifi/hotspotlogin.php
#uamhomepage http://192.168.182.1/welcome.html
เป็น uamhomepage http://10.0.1.1/wifi/index.php
#uamsecret ht2eb8ej6s4et3rg1ulp เป็น uamsecret ht2eb8ej6s4et3rg1ulp
#uamlisten 192.168.182.1 เป็น uamlisten 10.0.1.1

• การตั้งเวลาด้วย Crontab

1. แก้ไขไฟล์ /etc/crontab

รูปแบบของคำสั่ง crontab มีทั้งหมด 6 fields ดังนี้

minute	*, 0-59	กำหนดเวลาเป็นนาที
hour	*, 0-59	กำหนดเวลาเป็นชั่วโมง
day	*, 1-31	กำหนดเป็นวัน
month	*, 1-12	กำหนดเป็นเดือน
weekday	*, 0-6	กำหนดวันแต่ละสัปดาห์ 0=อาทิตย์, 1=จันทร์, ... 6=เสาร์
command	คำสั่งให้ทำงานตามเวลาที่กำหนด	

2. ตั้งเวลา restart server ตอน 2 นาฬิกา ทุกวัน

0 2 * * * root reboot

• MySQL Server [port 3306]

1. ติดตั้ง MySQL Server

[root@Centos6 ~]# yum –y install mysql mysql-server mysql-devel

2. เพิ่มข้อความต่อท้าย /etc/my.cnf

[client]
port = 3306
socket = /var/lib/mysql/mysql.sock

3. สั่งให้ทำงาน

[root@Centos6 ~]# /etc/init.d/mysqld start

4. สร้าง User และ Password สำหรับ root

[root@Centos6 ~]# /usr/bin/mysqladmin –u root password ‘liirpk’ *(ตั้งรหัสผ่านตามต้องการ)*

5. สร้าง Database ชื่อ radius

[root@Centos6 ~]# mysqladmin –uroot –pliirpk create radius

6. นำข้อมูล sql เข้า database

[root@Centos6 ~]# mysql –uroot –pliirpk radius < /tmp/radius.sql

7. ส่งข้อมูลออกเป็น sql

[root@Centos6 ~]# mysqldump –u root –p liirpk radius > /tmp/radius.sql

8. ตัวอย่างสร้าง user ชื่อ webusr รหัสผ่าน webpas ดาต้าเบส webdb

mysql> **CREATE DATABASE** webdb;

mysql> **CREATE USER** 'webusr'@'localhost' **IDENTIFIED BY** 'webpas';

mysql> **GRANT ALL ON** webdb.* **TO** 'webusr'@'localhost';

mysql> **FLUSH PRIVILEGES**;

9. เพิ่ม Rule ให้กับ iptables

iptables –A INPUT –m state --state NEW –m tcp –p tcp --dport 3306 –j ACCEPT

10. ทดสอบ remote ไปยัง MySQL Server

[root@Centos6 ~]# mysql –h 202.143.143.30 –u webusr –p webpas

• VSFTPD เป็น FTP Server [port 20, 21]

1. ติดตั้งโปรแกรม

[root@Centos6 ~]# yum –y install vsftpd

2. แก้ไขไฟล์คอนฟิก /etc/vsftpd มี 4 ไฟล์

[root@Centos6 ~]# nano /etc/vsftpd/vsftpd.conf

 # ปิดไม่ให้ anonymous ล็อคอินได้

anonymous_enable = YES เป็น anonymous_enable = NO

 # ให้ user อัพโหลด ล็อคอิน สร้างไฟล์ สร้างไดเร็คทอรี่ แก้ไข ลบได้เฉพาะ home directory ตนเอง

write_enable = YES

 # ให้ user ที่มีแอ๊คเค้าท์อยู่ในไฟล์ /etc/passwd ล๊อคอินได้

local_enable = YES

 # ไฟล์ที่ user อัพโหลดเข้าไดเร็คทรอรี่ถูกกำหนดให้เป็น755

local_umask = 022

 # เซ็ตแบนเนอร์

ftpd_banner = Welcome to Nakorn FTP Service

 # กำหนดให้ user ใน /etc/vsftpd/user_list ล็อคอินได้ แต่ต้องไม่อยู่ใน /etc/vsftpd/ftpusers

userlist_deny = NO

 # ให้ user อยู่ใน home directory ของตนเองเท่านั้น

chroot_local_user = YES

 # ให้ user ใน /etc/vsftp/chroot_list สามารถเปลี่ยนไดเร็คทรอรี่ไปยังคนอื่นได้

chroot_list_enable = YES

chroot_list_file = /etc/vsftpd/chroot_list

 # เก็บ log file ด้วย

xferlog_enable = YES

xferlog_file = /var/log/xferlog

xferlog_std_format = YES

 # สร้างไฟล์เก็บ log

[root@Centos6 ~]# touch /var/log/xferlog

ไฟล์ ftpusers เก็บรายชื่อ user ที่ไม่ให้ล็อคอินทาง FTP

ไฟล์ user_list เก็บรายชื่อที่จะยอมหรือไม่ยอมให้ล็อคอินขึ้นอยู่กับ userlist_deny = YES or NO

vsftpd_conf_migrate.sh ไฟล์สคริ๊ปต์สำหรับย้ายไดเร็คทรอรี่ของ user

ไฟล์ chroot_list เก็บรายชื่อ user ที่สามารถย้ายไปไดเร็คทรอรี่คนอื่นได้

ไดเร็คทรอรี่ /var/ftp/pub เตรียมไว้สำหรับ anonymous

3. กำหนด iptables อนุญาต port 20 และ 21

iptables –A INPUT –p tcp --dport 21 –j ACCEPT

iptables –A INPUT –p tcp --dport 20 –j ACCEPT

4. ตรวจสอบค่าเบื้องต้นว่าเป็นไปตามนี้หรือไม่

anonymous_enable=NO

local_enable=YES

write_enable=YES

local_umask=022

dirmessage_enable=YES

xferlog_enable=YES

connect_from_port_20=YES

xferlog_std_format=YES

listen=YES

pam_service_name=vsftpd

userlist_enable=YES

tcp_wrappers=YES

5. กำหนดเปิดเครื่องแล้วทำงานเลย

chkconfig vsftpd on

6. การทำ Chroot vsftpd with non-system users

ติดตั้งระบบ

[root@Centos6 ~]# yum –y install vsftpd db4-utils

เรียกสคิ๊ปเพื่อตั้งค่าบน Ftp Server

vsftpd_virtual_config.sh	ตั้งค่าเบื้องต้นกรณีไม่ใช้ TLS
vsftpd_virtual_config_withTLS.sh	ตั้งค่าเบื้องต้นกรณีใช้ TLS

ถ้าต้องการให้บริการทางอินเทอร์เน็ตต้องใช้ vsftpd_virtual_config_withTLS.sh

การจัดการสำหรับ User (การเรียกใช้ Script ใช้คำสั่ง /bin/sh <file sh>)

vsftpd_virtualuser_add.sh	เพิ่มผู้ใช้ ต้องมี vsftpd_virtualuser_config.tpl
vsftpd_virtualuser_update.sh	ปรับปรุงแก้ไขผู้ใช้
vsftpd_virtualuser_remove.sh	ลบผู้ใช้
vsftpd_virtualuser_info.sh	แสดงรายละเอียดผู้ใช้

การตั้งค่า Firewall

iptables –A INPUT –m state --state NEW –m tcp –p tcp --dport 21 –j ACCEPT

iptables –A INPUT –m state --state NEW –m tcp –p tcp --dport 64000:65535 –j ACCEPT

● PHPMyAdmin Manager of MySQL

1. ดาวน์โหลด

[root@Centos6 ~]# cd /tmp

[root@Centos6 tmp]# wget pkgs.repoforge.org/phpmyadmin/phpmyadmin-2.11.9.6-1.el5.rf.noarch.rpm

2. ติดตั้งโปรแกรม

[root@Centos6 tmp]# rpm –Uvh phpmyadmin-2.11.9.6-1.el5.rf.noarch.rpm

3. คัดลอกไฟล์ไปไว้ใน Home Page

[root@Centos6 /]# cp /usr/share/phpmyadmin /var/www/html/

4. แก้ไขไฟล์ /var/www/html/phpmyadmin/config.inc.php

เปลี่ยน $cfg[‘Servers’][$i][‘auth_type’] = ‘cookie’;

เป็น $cfg[‘Servers’][$i][‘auth_type’] = ‘http’;

5. แก้ไขไฟล์ /etc/httpd/conf.d/phpmyadmin.conf ให้เหมือนข้อความด้านล่างนี้

```
<Directory “/var/www/html/phpmyadmin”>
        # Order Deny,Allow
        Order Allow,Deny
        # Deny from all
        Allow from all
        Allow from 127.0.0.1
</Directory>
# Alias  /phpmyadmin  /usr/share/phpmyadmin
# Alias  /phpMyAdmin  /usr/share/phpmyadmin
# Alias  /mysqladmin  /usr/share/phpmyadmin

Alias  /phpmyadmin  /var/www/html/phpmyadmin
Alias  /phpMyAdmin  /var/www/html/phpmyadmin
Alias  /mysqladmin  /var/www/html/phpmyadmin
```

คำสั่งต่างใน Linux

- **useradd –u <uid> -g <group> -d <home dir> -s <shell> -m loginname**

ใช้เพิ่ม user เข้าไปในระบบ (หลังจากเพิ่ม user แล้วต้องกำหนดรหัสผ่านเสมอโดยคำสั่ง passwd) การเพิ่ม user เข้าไปในระบบจะถูกเก็บเข้าไปในไฟล์ /etc/passwd โดย 1 แถว คือ 1 user โดยมีรูปแบบ ดังนี้ username:en-password:uid:gid:comment:homedir:shell)

เช่น useradd –u 120 –g teacher –d /home/nutty –s /bin/sh –m nutty

-u <uid>	กำหนดหมายเลข user id ซึ่งแต่ละคนจะไม่ซ้ำกัน
-g <group>	กำหนด group ให้กับ user
-d <home dir>	กำหนด directory หลักให้กับ user
-s <shell>	กำหนด shell ให้กับ user
-m	บอกให้ทำการสร้าง directory บ้านขึ้นมาถ้ายังไม่มี
loginname	คือชื่อ login ของผู้ใช้ใหม่

- **passwd username**

ใช้ในการเปลี่ยนรหัสผ่านของ User

- **userdel loginname**

ใช้ลบ user ออกจากระบบ (หรือจะลบแถวออกจากไฟล์ /etc/passwd ก็ได้) การ disabled user สามารถทำได้ง่ายๆ เช่น เพิ่ม เครื่องหมาย “!” เข้าไปด้านหน้าสุดของ password เป็นต้น

- **ตรวจสอบ CPU**

more /proc/cpuinfo **หรือ** cat /proc/cpuinfo **หรือ** less /proc/cpuinfo