Proxy Server :: Squid Authen with FreeRadius Server

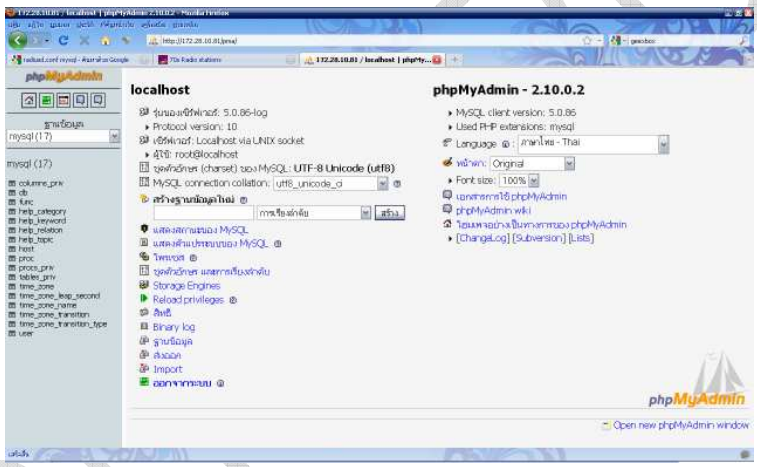
ข้อตกลง : ในเอกสารนี้ขอข้ามขั้นตอนการ Compile Kernel ของ FreeBSD เพื่อทำเป็น NAT ในการ share internet ให้เครื่องลูกข่าย สามารถใช้งานผ่านเครื่อง proxy นี้

เริ่มกันเลย...

สามารถดาวน์โหลดไฟล์ distfiles ได้จาก http://freebsd.aru.ac.th/FreeBSD80/f80distfiles.tar แล้วนำไปแตกไว้ที่ /usr/port/distfiles/

ให้ทำการติดตั้ง Apache2.2 , MySQL 5.0 , PHP5 ให้เรียบร้อยสามารถใช้งานได้ (ดูเอกสารอื่นที่ผู้เขียน เขียนไว้ประกอบ ในการติดตั้ง ได้ที่ http://freebsd.aru.ac.th)

ให้ติดตั้ง phpMyAdmin จนสามารถเข้าไปจัดการฐานข้อมูล MySQL ได้



ติดตั้ง FreeRadius

cd /usr/ports/net/freeradius

make ; make install clean

rehash

เพิ่มบรรทัด radiusd_enable="YES" ในไฟล์ /etc/rc.conf

สร้าง log files ให้กับ FreeRadius

cd /var/log

mkdir radacct

touch radius.log radutmp radwtmp

chmod 700 radacct

chmod 644 radius.log radwtmp

chmod 600 radutmp

chown radiusd:radiusd radacct radius.log radutmp radwtmp

ตรวจสอบว่า FreeBSD Service ตั้งค่า Radius ไว้ที่ port หมายเลขใด

cat services | grep radius

ผลลัพธ์จากคำสั่งด้านบน พบว่า เป็น port 1812

```
# IMPORTANT NOTE: Ports 1645/1646 are the traditional radius ports used by
#radius         1645/udp   #RADIUS authentication protocol (old)
radius          1812/udp   #RADIUS authentication protocol (IANA sanctioned)
```

สำรองไฟล์ .conf ทั้งหมดไว้ก่อน (กันพลาด)

cd /usr/local/etc/raddb/

foreach file (`ls -l | grep .conf | awk '{print $9}'`)

foreach? cp $file $file.sample

foreach? end

แก้ไขไฟล์ config อื่น ๆ

ee /usr/local/etc/raddb/sql.conf

แก้ไขข้อมูลในบรรทัดต่อไปนี้ เพื่อให้ radius สามารถเชื่อมต่อ MySQL ได้ แล้วบันทึก

```
        server = "localhost"
        login = "root"
        password = "rootpass"
```

ee /usr/local/etc/raddb/radiusd.conf

```
port = 1812
```

ที่บริเวณท้ายไฟล์ ในส่วนต่าง ๆ ต้องมีลักษณะดังนี้

```
authorize {
        preprocess
        chap
        mschap
        #counter
        #attr_filter
        #eap
```

```
        suffix
        sql
        #files
        #etc_smbpasswd
}

authenticate {
        authtype PAP {
                pap
        }
        authtype CHAP {
                chap
        }
        authtype MS-CHAP{
                mschap
        }
        #pam
        #unix
        #authtype LDAP {
        #       ldap
        #}
}

preacct {
        preprocess
        suffix
        #files
}

accounting {
        acct_unique
        detail
        #counter
        unix
        sql
        radutmp
        #sradutmp
}

session {
        radutmp
}
```


เตรียมฐานข้อมูล MySQL เพื่อรองรับ FreeRadius

mysql -u root –p

mysql> create database radius;

mysql> \q

สร้างตารางในฐานข้อมูล

mysql -u root -p radius < /usr/local/share/doc/freeradius/examples/mysql.sql

ทดลอง insert ข้อมูลเข้าระบบ

mysql -u root -p

mysql> connect radius;

mysql> insert into radcheck(username,attribute,value) values('test1','User-Password','test1');

mysql> select * from radcheck;

```
+----+----------+--------------+----+-------+
| id | UserName | Attribute    | op | Value |
+----+----------+--------------+----+-------+
|  1 | test1    | User-Password | == | test1 |
+----+----------+--------------+----+-------+
1 row in set (0.00 sec)
```

mysql> \q

TIP : เราสามารถกำหนด Attribute ได้หลายแบบดังตัวอย่าง

Cleartext-Password , User-Password , MD5-Password

```
+----+----------+-------------------+----+----------------------------------+
| id | UserName | Attribute         | op | Value                            |
+----+----------+-------------------+----+----------------------------------+
|  1 | test1    | User-Password     | == | test1                            |
|  2 | boy      | Cleartext-Password | := | 12345                            |
|  3 | girl     | MD5-Password      | := | 827ccb0eea8a706c4c34a16891f84e7b |
+----+----------+-------------------+----+----------------------------------+
3 rows in set (0.00 sec)
```

จากตัวอย่าง

user test1 จะมี password คือ test1

user boy จะมี password คือ 12345

user girl จะมี password คือ 12345 (เข้ารหัสแบบ md5) โดยใช้คำสั่งด้านล่างนี้

```
mysql>insert into radcheck(username,attribute,op,value)
      values('girl','MD5-Password',':=',md5('12345'));
```

สั่งให้ radius ทำงาน

/usr/local/etc/rc.d/radiusd start

ทดสอบ radius

radtest test1 test1 localhost 1812 testing123

```
Sending Access-Request of id 160 to 127.0.0.1 port 1812
        User-Name = "test1"
        User-Password = "test1"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=160, length=20
```

จากผลลัพธ์ มี Access-Accept แสดงว่า user authen ได้แล้ว

เราจะใช้ Squid Cache: Version 2.6.STABLE18 ซึ่งรองรับการ Authen ด้วย Radius

ผู้เขียนเก็บไฟล์ squid-2.6.STABLE18.tar.gz ไว้ใน f80distfiles.tar ด้วยดังนั้นให้ copy จาก /usr/ports/distfiles ไปไว้ที่ /tmp

cp /usr/ports/distfiles/squid-2.6.STABLE18.tar.gz /tmp/

เริ่มติดตั้ง Squid

cd /tmp

tar -zxvf squid-2.6.STABLE18.tar.gz

cd squid-2.6.STABLE18

./configure --prefix=/usr/local/squid --enable-removal-policies=heap --enable-delay-pools --enable-snmp --enable-arp-acl --enable-basic-auth-helpers=squid_radius_auth

make all

make install

#cd /usr/sbin/

#ln -s /usr/local/squid/sbin/squid squid

#rehash

cd /usr/local/squid/var/logs/

touch access.log store.log cache.log

chmod 777 *.log

cd /usr/local/squid/var/

mkdir cache

chmod -R 777 cache

cd /usr/local/squid/etc/

สร้างไฟล์ squid_radius_auth.conf เพื่อใช้เชื่อมต่อกับ radius server

#ee squid_radius_auth.conf

```
server localhost
secret testing123
```

แก้ไข config ของ squid แก้ไขเพิ่มเติมส่วนต่าง (หมายเลขบรรทัดโดยประมาณใกล้เคียงของเดิม)

ee squid.conf

```
280  auth_param basic program /usr/local/squid/libexec/squid_radius_auth -f
/usr/local/squid/etc/squid_radius_auth.conf
281  auth_param basic children 20
282  auth_param basic realm ITC Web Access Authen. More Info Tel.3201,3220
283  auth_param basic credentialsttl 2 hours
284  auth_param basic casesensitive off
```

```
598  acl radius-auth proxy_auth REQUIRED
599  acl itc src 172.28.10.0/255.255.255.0
```

```
639  http_access allow radius-auth
640  http_access allow itc
```

```
1654  memory_replacement_policy heap GDSF
```

```
1696  cache_replacement_policy heap GDSF
```

บันทึกไฟล์ แล้วกลับไปที่ root

cd

สร้าง cache

squid -z

สร้างไฟล์ script เพื่อไว้สั่ง start/stop squid

ee squid.sh

```
#!/bin/sh
case "$1" in
start)
if [ -f /usr/local/squid/bin/RunCache ]; then
echo -n 'starting Squid ...'
(/usr/local/squid/bin/RunCache &)
fi
;;
stop)
kill -9 `ps ax | grep RunCache | awk '{print $1}'`;
/usr/local/squid/sbin/squid -k shutdown;
;;
*)
echo "squid.sh stop|start"
;;
esac
exit 0
```

บันทึกไฟล์แล้วเปลี่ยน mode ให้ script ทำงานได้

chmod +x squid.sh

ในการเรียกใช้งาน ให้ทำดังนี้

cd /root/

#./squid.sh stop

เพื่อ stop squid process

#./squid.sh start

เพื่อ start squid process

หากมีการแก้ไขเพิ่มเติมในไฟล์ /usr/local/squid/etc/squid.conf ให้ใช้คำสั่งต่อไปนี้ เพื่อให้ squid ทำงานตามที่เรา config เพิ่มเติมไป

squid –k reconfig

การติดตั้ง ezRadius เพื่อเป็น Radius User Manager

ผู้เขียนได้ นำเอาไฟล์ ezradius-comm-0.2.1.tar.gz เก็บไว้ใน f80distfiles.tar แล้ว สามารถ copy ไปใช้งานได้เลย

cd /usr/local/www/apache22/data/

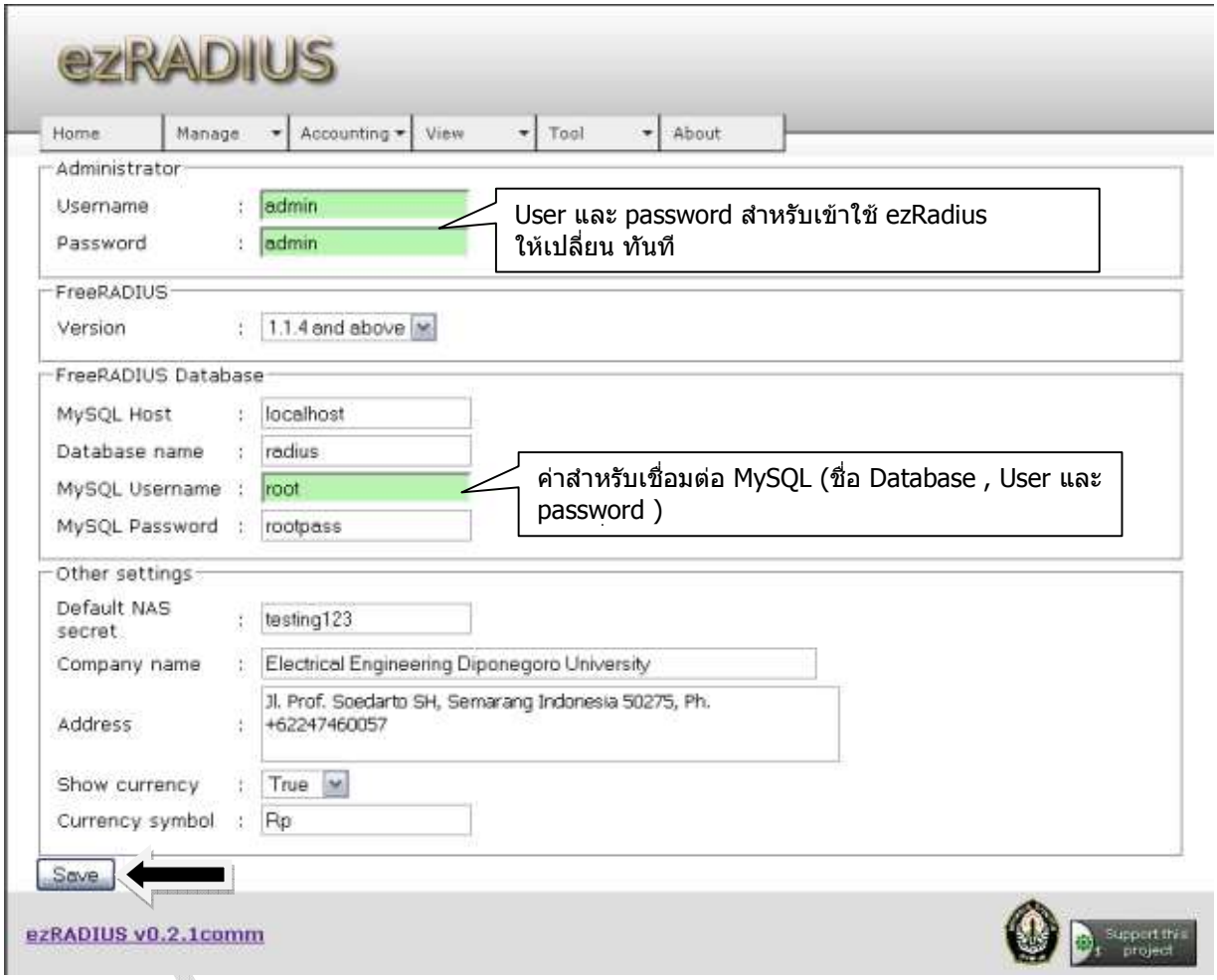
cp /usr/ports/distfiles/ezradius-comm-0.2.1.tar.gz ./

tar -zxvf ezradius-comm-0.2.1.tar.gz

mv ezradius-comm ezradius

chown -R www:www ezradius

ลองเปิด เวบไป http://proxy_ip_address/ezradius



ส่วนใหญ่จะใช้งานที่เมนู Manage อย่างเดียวในการจัดการกับ user นอกจากนั้นไม่จำเป็น