# POSTFIX - DEALING WITH LARGE MAILS

Large emails? Not exactly a security problem you might say. But the problem is that unless you have some sort of strategy then you could be the position where a email user inadvertently causes a denial of service attack on your email server, bandwidth or both. So one solution is to place large emails on hold until off-peak times so other emails can flow as normal. Now I like *postfix*, it can do a lot, but it does not have this functionality built in. I realize there are two sides to this but I wanted it, so here's how I got it..

*Finding them?*
Firstly you need a script that can find large emails and can place them on hold. The following script (which in a fit of imagination I called *postfix_delay*) does that..

```
AQ=/var/spool/postfix/active
SINGLEINST=5120
TOOBIG=10485760

for x in `find $AQ -size +"$SINGLEINST"c -type f`
 do
  NAME=`echo $x | cut -f 6 -d "/"`
  MSIZE=`ls -l $x | gawk '{ print $5 }'`
  NUMRECIP=`/usr/sbin/postcat $x | head -180 | grep -e "original_recipient:" | wc -l`
  TOTSIZE=`expr $NUMRECIP \* $MSIZE`
  logger "POSTFIX-DELAY = $NAME : $MSIZE : $NUMRECIP : $TOTSIZE"
  if [ `expr $TOTSIZE \> $TOOBIG` == 1 ]
   then
    /usr/sbin/postsuper -h $NAME
  fi
 done
```

The *SINGLEINST* variable is there to specify that if an email message is this size or smaller we do not bother with it. The *TOOBIG* variable is the limit for email, if a email message is this size or larger we place it on hold (both figures are in bytes). The for loop goes through each active email message, gets the number of recipients and then multiplies that by the message size. The result is a size that we use to compare against our size limit, and we make nice entries in *syslog* for checking. Lastly if the size is too big, we use *postsuper* to place it on hold. As always, this script works for me, feel free to use it if you want, tweak it, etc - just remember you use it, you are responsible for it.

*Running it?*
Simple. Use *crontab*..

```
*/10 7,8,9,10,11,12,13,14,15,16,17,18,19 * * * /admin/bin/postfix_delay
```

I run it every 10 minutes from 7AM to 19PM, so my off-peak is from 20PM to 7AM. So to release all held emails during off-peak times, we use *crontab* again..

```
10 20 * * * /usr/sbin/postsuper -H ALL
```

*Thats it?*
In a nutshell - yes.

*Final Words*
Humor aside, an unintentional dos attack is a very real and possible threat, and dealing with situations where it can occur is only prudent. So play around, learn and have fun.