**Danh sách các file được cấu hình**

1. **Clamav**
   1. /etc/clamav/clamd.conf

LocalSocket /var/run/clamav/clamd.ctl

Thêm dòng này vào cuối file:

VirusEvent mv $CLAM\_VIRUSEVENT\_FILENAME /home/khang/quarantine

* 1. /etc/clamav/freshclam.conf

thêm dòng này vào cuối file

# Check for new database 24 times a day

Checks 24

DatabaseMirror db.local.clamav.net

DatabaseMirror database.clamav.net

1. **Dansguardian**
   1. /etc/dansguardian/dansguardian.conf

đặt dấu ‘#’ vào dòng

#UNCONFIGURED - Please remove this line after configuration

…

…

# the port that DansGuardian listens to.

filterport = 8080

# the ip of the proxy (default is the loopback - i.e. this server)

proxyip = 127.0.0.1

# the port DansGuardian connects to proxy on

proxyport = 3128 # port của squid proxy

…

…

# Daemon runas user and group

# This is the user that DansGuardian runs as. Normally the user/group nobody.

# Uncomment to use. Defaults to the user set at compile time.

# Temp files created during virus scanning are given owner and group read

# permissions; to use content scanners based on external processes, such as

# clamdscan, the two processes must run with either the same group or user ID.

daemonuser = 'clamav' # dansguardian và clamav cùng chạy trên 1 user

daemongroup = 'clamav'

* 1. /etc/dansguardian/contentscanners/clamdscan.conf

giá trị clamdudsfile trong file /etc/dansguardian/contentscanners/clamdscan.conf

phải giống giá trị LocalSocket trong file /etc/clamav/clamd.conf

clamdudsfile = '/var/run/clamav/clamd.ctl'

1. **Squid proxy**
   1. etc/squid/squid.conf

cấu hình cache cho squid proxy là 3Gb

cache\_dir ufs /var/spool/squid 3000 16 256

#cache\_dir rock /hdd1 ... min-size=100000

#cache\_dir rock /ssd1 ... max-size=99999

#cache\_dir rock /hdd2 ... min-size=100000

#cache\_dir rock /ssd2 ... max-size=99999

#cache\_dir rock /hdd3 ... min-size=100000

#cache\_dir rock /ssd3 ... max-size=99999

1. **Shorewall**

Trong thư mục /etc/shorewall thêm các file sau:

* 1. action.SSHLIMIT
  2. action.SSH\_BLACKLIST
  3. actions
  4. getblacklist.sh
  5. interfaces
  6. masq
  7. policy
  8. rules
  9. shorewall.conf
  10. zones

thực hiện lệnh

$ sudo bash getblacklist.sh

để lấy danh sách blacklist ip và sinh ra file blrules

1. **Apache**
   1. /etc/apache2/sites-available/default-ssl.conf

ServerName demo.com:443

SSLEngine on

SSLCertificateFile /etc/apache2/ssl/apache.crt

SSLCertificateKeyFile /etc/apache2/ssl/apach

* 1. /etc/apache2/ssl/apache.crt
  2. /etc/apache2/ssl/apache.key