

Dansguardian Setup with ClamAV Content Filtering & Squid Transparent Proxy[20061017]

Dansguardian is true content filtering proxy that can be used either standalone or integrated with other antivirus and proxy solutions. With today's growing Internet threats, many enterprises faced the challenges of preventing their networks from viruses and worms infection. This setup is extremely useful for deployment within a network with multiple users connecting to the Internet and of high risk of virus threats. The method introduced by utilizing all the Open Source Tools are highly effective in controlling and enforcing security of your network. It is hard to find any comprehensive documentations on setting up dansguardian on FreeBSD platform thus it should be ideal for me to create one.

I've chosen FreeBSD as Operating System of my choice since it is one of most robust platforms and more importantly I am familiar with it. Another advantage of using FreeBSD is no other than its powerful, simple to use application ports/package system. All the applications that I needed for this setup are available.

Please do note that I have different kind of fonts for different context to ease the readers.

bold - configuration file name

italic - content of configuration files

shell> - command lines

I will try to explain the setup in details. However, I will not cover details on how to install FreeBSD since you can find it in FreeBSD Handbook. I will cover kernel recompiling and performance tweaking of the FreeBSD system as it directly relates to performance of this deployment.

Once you have already installed the FreeBSD system, you will find your kernel configuration file under /usr/src/sys/(hardware platform)/conf. The demonstration box is i386 Intel Hardware. It may be vary if you are installing on other hardware platform such as amd64 and so forth.

Important : Your kernel tuning limits may vary depending on resources your system has. Please refer to tuning(7) for guidance.

To recompile kernel

```
shell>cd /usr/src
```

```
shell>cd /usr/src/sys/i386/conf
```

```
shell>cp GENERIC MYKERNEL
```

Tune the MYKERNEL to enable all the necessary functions

```
options UFS_ACL
```

```
options MAC
```

```
options AUDIT
```

```
options DEVICE_POLLING
```

```
options HZ=1000
```

```
options MAXDSIZ="(1380*1024*1024)"
```

```
options DFLDSIZ="(1380*1024*1024)"
options MAXSSIZ="(1024*1024*1024)"
```

The below tweaking is to enable the firewalling and traffic shaping in kernel

```
options ALTQ
options ALTQ_CBQ
options ALTQ_RED
options ALTQ_RIO
options ALTQ_HFSC
options ALTQ_PRIQ
options ALTQ_NOPCC
```

```
device pf
device pflog
device pfsync
```

Compiling the new kernel,

```
shell>cd /usr/src && make buildkernel KERNCONF=MYKERNEL
```

Installing the new kernel,

```
shell>make installkernel KERNCONF=MYKERNEL
```

We have successfully compiled and installed the new kernel, we can now tune /etc/sysctl.conf for better performance,

```
net.inet.tcp.sendspace=65536
net.inet.tcp.recvspace=65536
net.inet.ip.redirect=0
net.inet.tcp.syncookies=1
net.inet.tcp.delayed_ack=0
kern.coredump=0
kern.maxfiles=65536
kern.maxfilesperproc=32768
kern.maxprocperuid=16384
kern.ipc.somaxconn=2048
kern.ipc.maxsockbuf=2097152
kern.ipc.nmbclusters=32768
net.inet.udp.maxdgram=57344
kern.threads.max_threads_per_proc=40000
kern.threads.max_groups_per_proc=40000
```

After we have done the Operating System tuning, it's time to play with the applications.

Installing Dansguardian Development Version

Before you install dansguardian development version, you will have to download its source and put it into /usr/src/distfiles directory,

```
shell>cd /usr/src/distfiles;
```

```
shell>fetch http://dansguardian.org/downloads/2/Alpha/dansguardian-2.9.7.0.tar.gz
```

```
shell>cd /usr/ports/www/dansguardian-devel
```

```
shell>make install clean
```

Installing Clamav stable version

```
shell>pkg_add -r clamav
```

Installing Squid stable version

```
shell>pkg_add -r squid
```

Edit **/usr/local/etc/dansguardian/dansguardian.conf**

```
daemonuser = 'clamav'  
daemongroup = 'clamav'
```

```
forwardedfor = on
```

```
contentscanner = '/usr/local/etc/dansguardian/contentscanners/clamdscan.conf'
```

Adding this to rc.conf for startup

```
squid_enable="YES"  
clamav_clamd_enable="YES"  
clamav_freshclam_enable="YES"  
dansguardian_enable="YES"
```

Change the startup script of dansguardian and squid so that the startup sequence is right -

/usr/local/etc/rc.d/dansguardian

From

```
# PROVIDE: dansguardian  
# REQUIRE: NETWORKING SERVERS squid  
# BEFORE: DAEMON  
# KEYWORD: shutdown
```

To

```
# PROVIDE: dansguardian
```

```
# REQUIRE: NETWORKING SERVERS squid
# BEFORE: LOGIN
# KEYWORD: shutdown
```

/usr/local/etc/rc.d/squid

From

```
# PROVIDE: squid
# REQUIRE: LOGIN
# KEYWORD: shutdown
```

To

```
# PROVIDE: squid
# REQUIRE: DAEMON
# KEYWORD: shutdown
```

/usr/local/etc/dansguardian/contentscanners/clamscan.conf

From

```
clamdudsfile = '/var/run/clamav/clamd.sock'
```

To

```
clamdudsfile = '/var/run/clamav/clamd'
```

Then we can run squid -z to create the cache before restarting our system

```
shell> squid -z
```

We can also create memory disk to host the ipc files -

```
shell> mkdir /usr/dsgn-md
```

```
shell> mdmfs -s 128m md /usr/dsgn-md
```

And you can add it permanently on boot at **/etc/fstab**

```
md          /usr/tmpdata  mfs   rw,-s128m   0    0
```

Change dansguardian configuration files to point the ipc files to the memory disk -

/usr/local/etc/dansguardian/dansguardian.conf

```
# IPC filename
#
# Defines IPC server directory and filename used to communicate with the log process.
ipcfilename = '/usr/tmpdata/.dguardianipc'

# URL list IPC filename
#
# Defines URL list IPC server directory and filename used to communicate with the URL
# cache process.
urlipcfilename = '/usr/tmpdata/.dguardianurlipc'

# IP list IPC filename
#
# Defines IP list IPC server directory and filename, for communicating with the client
# IP cache process.
ipipcfilename = '/usr/tmpdata/.dguardianipipc'
```

You will have to allow 127.0.0.1 since both dansguardian and squid are running in the same host.

```
/usr/local/etc/squid/squid.conf
```

```
acl localhost src 127.0.0.1/255.255.255.255
```

I think that's all and now you just need to restart your FreeBSD Operating System and everything should be operational. After the system is rebooted, you can just configure your Internet browser to point to the IP of the dansguardian+clamav+squid system and port 8080 and you are now saved from various kind of Internet threats.

Transparency Proxy Setup

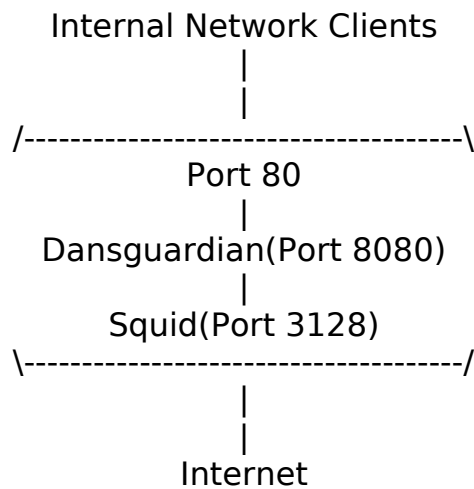
Why transparent proxy, that will be easy way and require zero configuration on desktop user side. Provided if you are setting up this on your router/gateway, you can actually make use of pf to provide true transparent proxy by redirecting the port 80 traffic to port 8080. Assuming your box with the IP of 192.168.0.1 and network interface bge0, you can add this one liner to the PF configuration file - **/etc/pf-transproxy.conf**

```
rdr on bge0 proto tcp from any to 192.168.0.1 port 80 -> 127.0.0.1 port 8080
```

If you want this kind of setup to handle big networks especially in enterprise environment, I suggest you have another router that doing traffic forwarding from port 80 to port 8080 of this box instead.

I will improve the documentation over time when possible, any suggestions and ideas to improve this documentation are welcomed by the way, till then.

The current setup is illustrated as



Written by geek00L (;)]

Improved by chflags(Credit to this awesome guy)