Dari internet banyak bibit penyakit semacam virus, trojan maupun lainnya. Kita inginkan bagaimana caranya gateway kita bisa memfilter bibit2 penyakit ini. Jadi semua paket data dari internet entah dari port mana aja akan di scan habis oleh program tersebut, nama program tersebut adalah HAVP yang merupakan repository dari http://www.server-side.de/ .

HAVP ini tidak bekerja sendiri, dia hanya memeriksa data masuk aja dan anti virus-nya sebagai acuhan bisa ClamAV atau AVG, disini sy menggunkan ClamAV. Dan disini sy sengaja memadukan dgn Squid agar yang di cache bener2 bersih dari penyakit.

Step by Step:

1. update dan upgrade linux.
edit /etc/apt/sources.list dan aktifkan, buang tanda "#"
lakukan update :

```
# apt-get update
```

kemudian upgrade :

```
# apt-get upgrade
```

2. Install ClamAV
install sangat mudah:

```
# apt-get install clamav
```

kemudian update database anti virusnya:

```
# freshclam
```

3. Install HAVP
install:

```
# apt-get install havp
```

tambahkan aturan Nat iptables, tujuannya khusus port 80 dipastikan di scan :

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3128
```

lakukan reboot :

```
# reboot
```

4. untuk memadukan dgn squid:
edit file /etc/squid/squid.conf:
tambahkan baris:

```
##############################
# HAVP + Clamav
cache_peer 127.0.0.1 parent 8080 0 no-query no-digest no-netdb-exchange default
```

nah, semua dari luar sudah di scan ama HAVP dan ClamAV, bagi server yg bermemory kecil, sy rekomendasikan untuk menambah memory.

ada yg kurang.... HAVP juga bisa nge-block situs2 yg gak kita inginkan, kita bisa menambah list:
edit aja file "/etc/havp/blacklist" untuk memblock situs misalnya dan "/etc/havp/whitelist" untuk situs masuk dalam daftar whitelist.

untuk test udah jalan ato belum kunjungi >>>> http://www.eicar.org/anti_virus_test_file.htm

dl untuk http port >>>
http://www.eicar.org/download/eicarcom2.zip

dl untuk https port >>>
https://secure.eicar.org/eicarcom2.zip

klo memang dah jalan, akan muncul **"Access to the page has been denied because the following virus was detected. ClamAV: Eicar-Test-Signature"** dgn background merah.

HAVP ini berjalan karena port 8080 di loading oleh squid, skemanya:

Port 80 ===> HAVP (8080) ===> Squid (3128) ===> Client
||
CLAMAV+LIBCLAMAV

By:
th@opikdesign.com
08123003336