HAVP - Проверка web-трафика антивирусом с помощью HTTP AntiVirus proxy

Опубликовано muff в Втр, 2010-08-31 09:52



Настроив работу пользователей через Squid, задумался о том, что было бы совсем неплохо дополнительно проверять этот трафик антивирусным софтом. Информации на эту тему довольно много. Я же остановил свой выбор на связке Squid+Clamav+HAVP. Реализовывать будем такую схему: Client->Squid->HAVP->Internet. Неоспоримым плюсом такого метода есть то, что вирусы не попадают в кеш, и файлы, которые отдаются пользователям из кеша прокси, не сканируются по несколько раз.

Отталкиваться будем от того, что $\underline{\text{Squid}}$ [1] и $\underline{\text{Clamav}}$ [2] уже установлены и настроены. Займемся установкой HAVP:

cd /usr/ports/www/havp/ && make install clean && rehash

Опции сборки оставил по дефолту.

После установки приступаем к редактированию конфигурационного файла, благо о дефолтном конфиге позаботились разработчики. Не забудьте удалить (или закомментировать) эту строку- REMOVETHISLINE deleteme. Разработчики позаботились о том, чтобы вы все-таки посмотрели конфигурационный файл;) Кстати, он довольно хорошо прокомментирован, так что с большинством опций разобраться можно без проблем.

В результате получился вот такой конфигурационный файл:

cat /usr/local/etc/havp/havp.config

SERVERNUMBER 25

MAXSERVERS 100

LOG OKS false

PORT 3127

BIND ADDRESS 127.0.0.1

TEMPLATEPATH /usr/local/etc/havp/ru

FAILSCANERROR falce

SCANNERTIMEOUT 5

STREAMUSERAGENT Player Winamp iTunes QuickTime Audio RMA/ MAD/ Foobar2000 XMMS

STREAMSCANSIZE 0

ENABLECLAMLIB true

CLAMDBDIR /var/db/clamav

ENABLECLAMD false

ENABLEFPROT false

ENABLEAVG false

ENABLEAVESERVER false

ENABLESOPHIE false

ENABLETROPHIE false

ENABLENOD32 false

ENABLEAVAST false

ENABLEARCAVIR false

ENABLEDRWEB false

Советую потратить немного времени и разобраться более детально с конфигурационным файлом HAVP.

Следующим шагом копируем файлы шаблонов:

cp -R /usr/local/share/examples/havp/templates/ru /usr/local/etc/havp/

Создаем файлы черных и белых списков HAVP:

touch /usr/local/etc/havp/whitelist /usr/local/etc/havp/blacklist

Запускаем HAVP, предварительно добавив опции запуска в /etc/rc.conf:

echo '# HTTP AntiVirus proxy' >> /etc/rc.conf
echo 'havp_enable="YES"' >> /etc/rc.conf
sh /usr/local/etc/rc.d/havp start

Starting havp.

Starting HAVP Version: 0.91

Mandatory locking disabled! KEEPBACK settings not used!

Вроде запустилось и все гуд... Следующим шагом будет "заворачивание" трафика из Squid в HAVP. Для этого в секцию "TAG: external_acl_type" добавляем такой блок:

cache_peer 127.0.0.1 parent 3127 0 default no-query never direct allow all

Первой строкой заворачиваются все потенциально кешируемые запросы, которых нет в кеше, на родительский прокси, которым выступает HAVP. Особенностью будет то, что в родительский кеш не будут попадать запросы описанные опцией сквида hierarchy_stoplist - запросы, которые содержат "cgi-bin" или "?", тоесть запросы к веб-скриптам. Конечно, вероятность того, что скрипты будут возвращать вирус есть, но при определенных обстоятельствах это можно проигнорировать. Таким образом проверятся будут только файлы на которые можно попасть прямой ссылкой. Позитивным моментом есть тот факт, что когда родительский кеш «упал» - то для пользователей это никак не проявляется, сквид работает как обычно.

После внесения изменений необходимо перезапустить Squid:

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

Проверяем "полет"... Заходим на <u>страницу теста</u> [3] и пробуем скачать предложенные файлы. Если все настроили правильно, то при попытке перейти по предложенным ссылкам, получим следующее окошко сообщения:



[4]

При этом, в лог-файлах можно наблюдать следующие записи:

tf /var/log/havp/access.log

31/08/2010 16:41:00 127.0.0.1 GET 200 http://www.rexswain.com/eicar.zip [5] 254+186 VIRUS

ClamAV: Eicar-Test-Signature

31/08/2010 16:41:05 127.0.0.1 GET 200 http://www.rexswain.com/eicar.com [6] 262+70 VIRUS

ClamAV: Eicar-Test-Signature

31/08/2010 16:41:27 127.0.0.1 GET 200 http://www.eicar.org/download/eicar_com.zip [7] 287+184

VIRUS ClamAV: Eicar-Test-Signature

31/08/2010 16:41:31 127.0.0.1 GET 200 http://www.eicar.org/download/eicarcom2.zip [8] 288+308

VIRUS ClamAV: Eicar-Test-Signature

31/08/2010 16:41:35 127.0.0.1 GET 200 http://www.eicar.org/download/eicar.com.txt [9] 328+88

VIRUS ClamAV: Eicar-Test-Signature

31/08/2010 16:41:38 127.0.0.1 GET 200 http://www.eicar.org/download/eicar.com [10] 298+68

VIRUS ClamAV: Eicar-Test-Signature

Источник (получено 2025-12-13 07:13):

 $\frac{\text{http://muff.kiev.ua/content/havp-proverka-web-trafika-antivirusom-s-pomoshchyu-http-antivirus-prox}{Y}$

Ссылки:

- [1] http://muff.kiev.ua/content/squid-sams-gibkost-v-upravlenii-dostupom
- [2] http://muff.kiev.ua/content/clamav-antivirusnaya-zashchita-servera
- [3] http://www.rexswain.com/eicar.html
- [4] http://muff.kiev.ua/files/imagepicker/1/havp.png
- [5] http://www.rexswain.com/eicar.zip
- [6] http://www.rexswain.com/eicar.com
- [7] http://www.eicar.org/download/eicar_com.zip
- [8] http://www.eicar.org/download/eicarcom2.zip
- [9] http://www.eicar.org/download/eicar.com.txt
- [10] http://www.eicar.org/download/eicar.com