Прокси сервер Squid с E2guardian и Clamav

Тема достаточно избитая, но у E2Guardian - форка Dansguardian, появились новые возможности, и теперь эту связку можно настроить несколько красивее. Сразу скажу что в плане SSL трафика все стало намного лучше.

Теория.

Прокси сервер Squid хорошо работает в режиме SSL bump, раскрывая SSL соединение и получая доступ к его содержимому. Далее он может это содержимое отдать на проверку ICAP серверу по протоколу icap://. Еще раз поясним, что в этот момент контент уже не шифрован, а plain.

Раньше использовали сервер C-icap с бэкендами (как правило с одним только Clamav или другим AV) для дальнейшего сканирования. Для сканирования контента на фразы по icap:// не было бесплатной реализации, а Dansguardian использовался как каскадный Proxy, и не имел доступа к SSL содержимому (или я ошибаюсь, поправьте меня).
Dansguardian заброшен с 2012 года, но нашлись люди, который сделали форк под наименованием E2guardian. В него добавили функциональность работы в режиме ICAP сервера.

То есть теперь на текущий момент Squid может отдавать раскрытый SSL трафик прямо в E2guardian по протоколу icap://. E2guardian в свою очередь может сканировать трафик по фразам, а также он унаследовал возможность отдавать его на проверку в Clamav на вирусы. Получается достаточно красивая связка Squid =icap://=> E2guardian => Clamav.

Сборка.

Я собираю все в Slackware64-current (просто у меня дома сейчас так). Сборка не интересна, слакваристы сами умеют это делать, и отнимает много времени. Кому все таки надо, вот мой build.

Итак мы получили 3 пакета:

```
squid-4.6-x86_64-2.txz
clamav-0.101.2-x86_64-2.txz
e2guardian-5.3-x86_64-2
```

Я установил их в chroot /opt/SEC-server и установил туда окружение с нужными зависимостями.

Настройку описывать не буду, потому что это совет, а не инструкция.

Предлагаю скачать готовый 64-битный chroot, он не замусорит систему.
Необходимо сгенерить и установить ключ с сертификатом и установить в etc/squid, а также поправить etc/resolv.conf и etc/hosts. Сертификат устанавливается также на каждую рабочую станцию в корневые центры сертификации.

Тесты.

Тесты на вирусы: https://www.eicar.org/?page_id=3950. Проверяем и SSL и Plain ссылки.
Тест на большой файл с вирусом: bigfile
Тест на фразы Google: анонимные прокси