

Оригинал: <http://zeroshell.net/eng/proxy-antivirus/>

Цель данной статьи – описать процесс создания web-прокси с антивирусной проверкой веб-страниц и добавлением сайтов в черный/белый список.

Содержание:

- **Зачем использовать прокси с антивирусной проверкой?**
- **«Прозрачный» режим прокси**
- **Конфигурация и активация сервиса**
- **Логи доступа и приватность**
- **Антивирусная проверка картинок**
- **Автообновление баз ClamAV**
- **Черный/белый список сайтов**
- **Проверка функций прокси и антивируса**

Зачем использовать веб прокси с антивирусом?

Веб-страницы становятся наиболее распространенным методом распространения всякой нечисти в виде вирусов и червей по сети Интернет. Веб-сайты умышленно, или же (вследствие незащищенности) после взлома, могут содержать ссылки на исполняемый код, который может заразить компьютер пользователя. Более того, ситуация ухудшилась с появлением уязвимостей в системе отображения картинок, вследствие чего появилась возможность распространять JPEG файлы, содержащие вирусы. Растущее, в последнее время, количество java-апплетов лишь способствует развитию мультиплатформенных вирусов, распространяющихся по HTTP и функционирующих вне зависимости от платформы (PC, смартфон, КПК) и установленной ОС.

Наилучшее решение для такой проблемы – обеспечение каждого устройства, имеющего доступ в интернет, хорошим антивирусным ПО с real-time защитой и проверкой каждого входящего файла. Однако, этого не будет достаточно по двум причинам: во-первых, не существует антивирусного ПО, способного отловить 100% вирусов и прочей нечисти, даже если оно обновляется ежеминутно; во-вторых, real-time проверка требует определенных вычислительных мощностей, а на устройствах, и без того не шибко мощных, антивирусное ПО может настолько замедлять их работу, что пользователи предпочитают просто отключить real-time защиту.

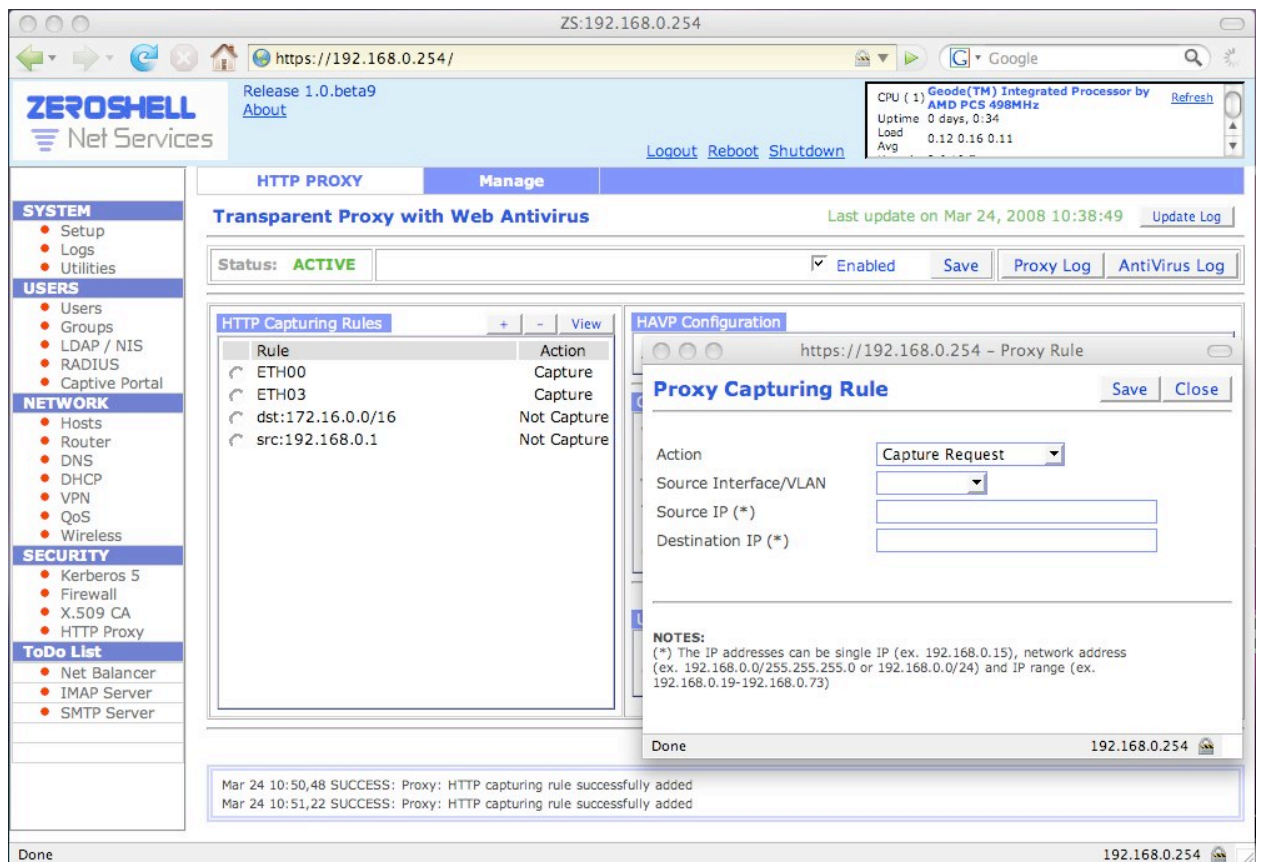
По этим причинам, проверка на вирусы поднимается на новый уровень – на уровень, когда файл проверяется на вирусы еще до того как попадает к пользователю. Другими словами, на серверах устанавливаются централизованные антивирусные системы, предлагая особый сервис. Наиболее распространенный пример данного сервиса – сервера электронной почты, которые имеют системы, анализирующие исходящие письма по SMTP протоколу и сканирующие приложения в письмах на вирусы. В таком случае, приложения антивирусной очень удачно расположены, т.к. электронные письма в любом случае пройдут через эти сервера перед тем как попасть во «входящие» письма пользователя.

«Прозрачный» режим прокси-сервера

Одной из наибольших проблем с использованием прокси сервера – это конфигурация всех браузеров для его использования. Для этого также необходимо выделить отдельный IP-адрес или имя хоста, порт на котором прокси будет проживать. Это может быть достаточно обременительно в случае, когда в локальной сети много пользователей, к тому же, она не может на 100% гарантировать, что пользователь не удалит конфигурацию работы с прокси-сервером и каким-либо способом получит прямой доступ к интернетом, тем самым избегая антивирусной проверки, логов и фильтрации по черным/белым спискам.

Для решения данной проблемы в ZeroShell используется «прозрачный» прокси, который включает в себя автоматический перехват клиентских запросов по 80 порту. Разумеется, для того, чтобы ZeroShell перехватывал такие запросы, он должен быть сконфигурирован

как сетевой шлюз, чтобы клиентский трафик проходил через него. ZeroShell будет автоматически перехватывать HTTP запросы, будучи и вторым уровнем шлюза (мост между Ethernet, WiFi, VPN-соединением) или третьим (роутер). И, тем не менее, важно выбрать на каком сетевом интерфейсе или в каких IP подсетях эти запросы будут переадресовываться. Это производится путем добавления правил «HTTP Capturing Rules» (правила перехвата HTTP):



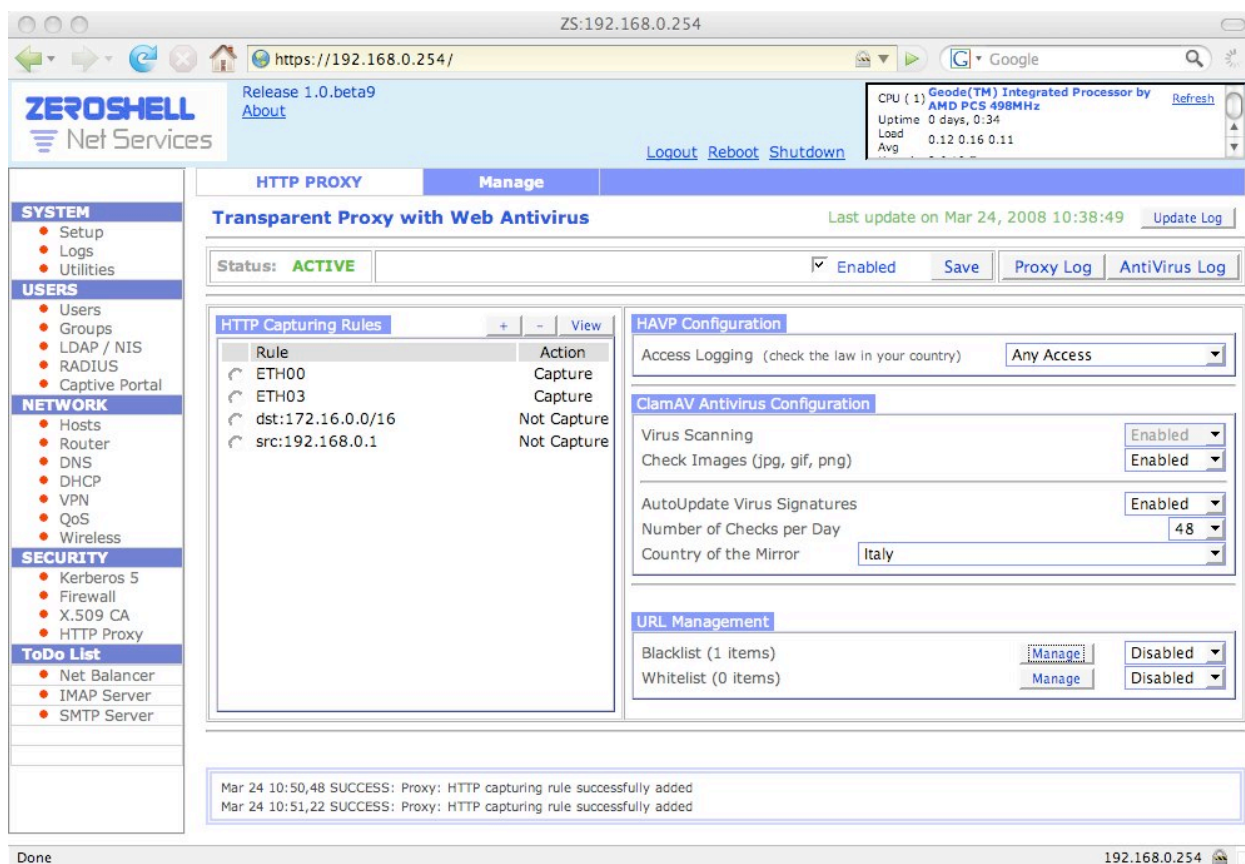
В данном примере, HTTP запросы с ETH00 и ETH03 сетевых интерфейсов будут перехватываться. Исключаются из этих запросов те, что направлены на веб-адреса, принадлежащие IP 172.16.0.0/16 подсети и те, что исходят от клиента с IP 192.168.0.1. Есть несколько причин, по которым необходимо настроить исключение вмешательства прозрачного прокси на некоторых клиентах и веб-серверах. Например, один веб-сервер может запрещать доступ только клиентам с определенным IP по своему черному списку. В таком случае, если прокси будет перехватывать такой запрос, то даже нежелательный клиент получит доступ на сервер, т.к. фактически, запрос будет идти не с его IP а с IP ZeroShell'a. С другой стороны, если на сервере, наоборот, есть доступ только для определенных IP, то залогиниться на сервер у клиента не выйдет, т.к. опять же, фактически запрос будет происходить с IP адреса сервера прокси. Так что очевидно, что единственным выходом из ситуации является просто избегание перехватывания запросов прозрачным прокси.

Напоследок, учтите, что в iptables правила перенаправления на прокси (8080 TCP) расположены ниже правил перехвата «Captive Portal», так что, благодаря этому, «Captive Portal» и «Transparent Проху» могут быть включены одновременно на одном и том же сетевом интерфейсе.

Настройка и активация прокси сервиса.

Как показано на скриншоте внизу, настройка прокси сервиса с антивирусной проверкой довольно проста. После настройки коробки с ZeroShell внутри в роли роутера, и после настройки его в качестве основного шлюза для клиентов, или настройка его мостом в точке где трафик проходит в/из интернета, просто поставьте флажок «Enabled» для

запуска прокси. Как упоминалось в предыдущем параграфе, перехватываться и перенаправляться на прокси будут запросы, для которых были настроены правила в «HTTP Capturing Rules».



Заметьте, что запуск прокси сервиса происходит очень медленно по сравнению с другими сервисами, и на не очень мощном железе может занять до 30-40 секунд. Это происходит в связи с необходимостью подключения антивирусных библиотек ClamAV - необходимо подгрузить и расшифровать большое количество вирусных сигнатур в памяти. Для предотвращения того, чтобы данный процесс блокировал веб-интерфейс и загрузочные скрипты на неопределенное время, этот сервис стартует асинхронно. Следовательно, когда прокси включается или перенастраивается, статусная индикация не отображается сразу как ACTIVE (зеленого цвета), а, для начала, оранжевет и покрывается надписью «STARTING», что означает, что подгружаются сигнатуры. Для того чтобы понять, когда же, действительно, прокси заработает – перейдите в «Proxy Log» для просмотра сообщений, или просто нажмите на «Manage» для обновления странички настроек. Во время запуска HAVP демона, правила в iptables относительно перехвата HTTP запросов временно удаляются для того, чтобы позволить трафику спокойно проходить, но, разумеется, в такой момент антивирусная проверка не проводится. Некоторые дополнительные настройки будут детальней проанализированы детальнее в следующем параграфе.

Лог доступа и приватность

Будучи программным шлюзом, способным интерпретировать HTTP-запросы, в целях корректной работы, веб-прокси расшифровывает ссылки, посещенные пользователями. По умолчанию, ZeroShell не отправляет такую информацию в лог, т.к., будучи проассоциированной с определенным IP адресом, можно проследить какое содержимое запрашивал пользователь.

Тем не менее, ведение логов с подобной информацией, может быть включено изменением параметра «Access Logging» с «Only URL Containing Virus» (лишь ссылки, содержащие вирусы) на «Any Access» (любой доступ). Сделав так, каждая ссылка, посещенная

пользователем, записывается в лог, ассоциированный с клиентским IP-адресом. Перед включением подобной опции лучше узнать у адвоката – разрешается ли местным законодательством сбор и хранение подобной информации и не нарушаются ли таким образом права на приватность.

Более того, необходимо учитывать, что после включения NAT, любой запрос, произведенный клиентами, фактически производится непосредственно сервером под управлением ZeroShell, также как и все запросы, производимые через прокси, осуществляются от имени IP адреса прокси. Это может повлечь за собой сложности в отслеживании личности пользователя, скажем, совершившего акт насилия над удаленным сервером. Метод решения данной проблемы, который, к тому же, не так сильно вмешивается в личную жизнь пользователей, существует – можно активировать ведение логов по отслеживанию соединений (в веб-интерфейсе ZeroShell в разделе «Firewall» пункт «Connection Tracking»). В таком режиме, любое TCP/UDP соединение записывается в лог информацией об исходном IP и порте и запрашиваемом IP и порте. Таким образом, невозможно отследить непосредственно контент, просмотренный пользователем, однако останется след о созданном подключении. Но, опять же, рекомендуется консультация у юриста перед включением такого отслеживания.

Антивирусная проверка изображений

На протяжении длительного времени казалось, что файл типа JPEG или GIF не может содержать в себе вирус, потому как он просто состоит из информации, сформированной в установленном формате, и интерпретируемой системой просмотра изображений операционной системы. Тем не менее, в последнее время, некоторые компоненты рендеринга картинок показали, что они уязвимы, если не обновляются патчами. Будучи сконструированным определенным методом, изображение может вызвать переполнение буфера и выполнение произвольного кода в системе. Легко понять всю серьезность данной проблемы, учитывая, что большая часть гипертекстового содержимого сети находится в форме изображений.

В ZeroShell NAMP прокси по умолчанию сконфигурирован для проверки изображений при помощи антивирусной программы ClamAV. Тем не менее, на медленном железе, процесс сканирования изображений может вызвать задержку в открытии веб-страниц с большим количеством изображений. В таком случае, можно отключить проверку файлов, содержащих изображения, переключив опцию «Check Images (jpg, gif, png)» из «Enabled» в «Disabled».

Автообновление сигнатур в ClamAV

Скорость, с которой новые вирусы добавляются в интернет и идентифицируются, означает, что антивирусные сигнатуры увеличиваются и изменяются довольно часто. Базы ClamAV также не являются исключением, так что, благодаря демону freshclam, они обновляются автоматически с определенным интервалом.

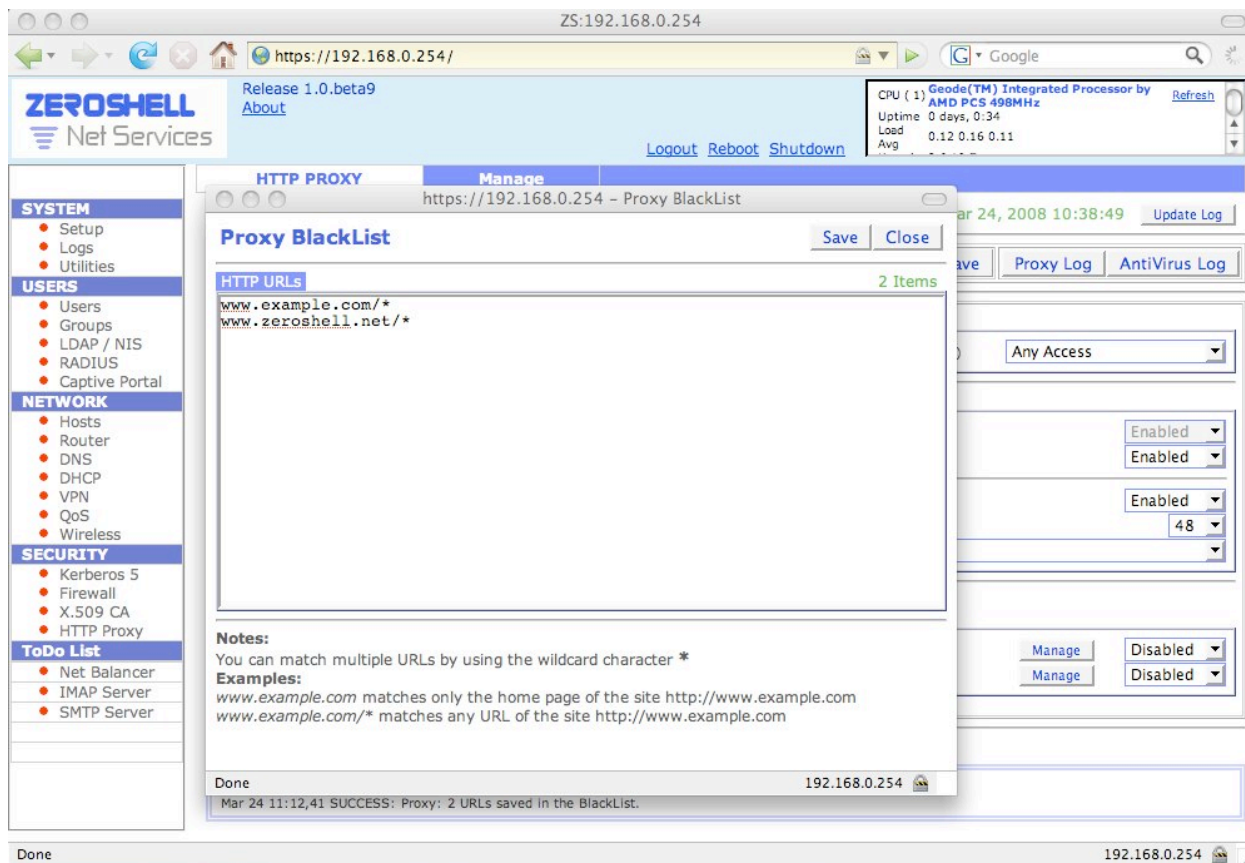
По умолчанию ZeroShell настраивает freshclam для обновления базы антивирусных сигнатур 12 раз в день. Данный интервал может быть установлен параметром «Number Of Checks Per Day» с минимального 1 до максимального 48 раз в день. Также достаточно важно установить зеркало для обновлений в параметре «Country Of Mirror» корректно, через которое freshclam выбирает ближайший источник для обновления сигнатур.

Заметьте, что процесс регулярного обновления – быстрая операция, которая не генерирует большого трафика, так как используется дифференциальная система обновления.

Создание черного/белого списка веб-сайтов.

Частенько есть необходимость блокировать отображение определенных сайтов в виду их «неудобного» содержания – будь то «вконтакт», «одноклассники» или иные порно-сайты. В таком случае очень эффективно решение принудительного использования прокси с софтом для фильтрации контента, например – DansGuardian, который анализирует

содержимое веб-страниц, блокируя все, что подпадает под нежелательную категорию. Механизмы данной фильтрации могут быть сравнены с системами антиспама. К сожалению, не совсем ясно, будет ли позволять окончательная лицензия на DansGuardian его использование в ZeroShell, так что данный программный продукт в ZeroShell не используется, дабы не нарушать условия лицензии, так что в данный момент единственный способ фильтрации нежелательного контента – формирование черных и белых списков как показано на скриншоте внизу.



Черный/белый список состоит из набора ссылок, расположенных с новой строки. Каждая строка может относиться к нескольким страницам, если используется знак '*'. Для блокирования сайта www.example.com нужно просто добавить строку 'www.example.com/*' в черный список, где запись вида 'www.example.com' будет означать лишь блокировку заглавной страницы сайта.

Белый список имеет приоритет над черным. В других словах, если сайт одновременно внесен и в белый список и в черный, то он будет доступен. Более того, белый список используется для создания списка «безопасных» сайтов, трафик с которых не будет проходить антивирусную проверку, так что учтите это. Если сетевой администратор хочет дать доступ лишь к определенным сайтам, он может добавить в черный список запись '*/*' и прописать исключения в белом списке.

Тестирование функций прокси и антивируса

В основном, есть две причины, почему прокси может не работать корректно. Во-первых, необходимо удостовериться, что ваш ящик с ZeroShell на борту, сконфигурирован как роутер или мост, и что трафик из интернета действительно проходит через него. Во-вторых, удостоверьтесь в правильной конфигурации «HTTP Capturing Rules», которые определяют, какие HTTP запросы будут перенаправлены через прокси (NATV прослушивает адрес 127.0.0.1:8080). В частности, если захват HTTP запроса происходит на сетевом интерфейсе, являющимся частью моста, надо быть уверенным, что хотя бы один из IP адресов был определен как конец моста.

Самый простой способ проверить работоспособность прокси – временно включить лог параметра «All Access» и посмотреть лог прокси после произведения серии запросов к нескольким сайтам со стороны клиента.

Будучи уверенным в том, что прокси перехватывает веб-запросы как запланировано, проверьте, что ClamAV также работает корректно. Для этого, во-первых, проверьте лог freshclam, чтобы удостовериться, что сигнатуры успешно обновляются, и делают это регулярно. Затем, посетите страничку http://www.eicar.org/anti_virus_test_file.htm для проверки того, что тестовый вирус EICAR-AV-Test (авторы заверяют в его безвредности) будет перехвачен и заблокирован.

Ну и, наконец, заметьте, что прокси не может обслуживать HTTPS (HTTP, зашифрованный по SSL/TLS) запросы, так как, не имея приватного ключа веб сервера, он не может расшифровывать содержимое, и как следствие, не перехватывает запросы, производимые по защищенному туннелю.