

netshe_doc_chap8

Original file



NETSHe Lab

**Универсальное
программное обеспечение
NETSHe
для сетевых устройств.**

Часть 8. HTTP проксирование.

NETSHe Lab длительное время занимается разработками программного обеспечения для сетевых устройств, провайдеров услуг и операторов связи. Среди программного обеспечения центральное место занимает операционная система NETSHe, которая может быть использована в широком спектре сетевых устройств и сервисов.

Версия 2
Май, 2020

Станислав Корсаков, ООО «Нетше лаб»
(с) 2009-2020 Ярославль

Оглавление

Использование HTTP прокси обусловлено рядом задач, которые предусматривают необходимость посредника (прокси) при передаче веб-трафика. Самая популярная из этих задач – ограничение Интернет доступа пользователям локальной сети. Более сложные задачи, такие как кэширование трафика и ускорение доступа к ресурсам Интернет, тоже реализуемы в NETSHe, но с использованием дополнительного оборудования под прокси-сервер верхнего уровня, т.к. аппаратные ресурсы устройств с NETSHe закономерно не позволяют организовать хранение кэшированного контента.

HTTP/HTTPS прокси в NETSHe

В NETSHe реализована функция HTTP/HTTPS прокси-сервера с возможностью перенаправления запросов на вышестоящий прокси-сервер, либо с обработкой «на месте». Настройка прокси производится в разделе меню WebUI «Службы→Прокси и UPnP» на закладке «HTTP/HTTPS прокси».

При включении прокси-сервера все запросы из локальной сети на порты 80 и 443 будут автоматически перенаправляться на его порт.

Для настройки Вы должны указать:

1. внешний интерфейс для прокси (интерфейс, по которому осуществляется доступ в Интернет и через который будут отправляться HTTP-запросы во внешний мир);
2. интерфейс локальной сети (на котором прокси будет получать HTTP-запросы от локальных пользователей);

3. Порт для прокси-сервера (по-умолчанию 3128);
4. Максимальное количество одновременных пользователей прокси-сервера (0 означает неограниченное количество. Значение отличное от нуля может быть использовано на устройствах с ограниченным объемом памяти для предотвращения перегрузки устройства).

Реализованный в NETSHe прокси-сервер имеет возможность контроля доступности ресурсов сети Интернет для локальных пользователей. Контроль доступа реализован через переключатель «Политика доступа прокси «запрещено»». По умолчанию применяется политика «Все разрешено» (галочка не установлена).

Пример политики HTTP прокси «все разрешено»

Для политики «Все разрешено» встроенный прокси-сервер будет запрещать запросы к Интернет-ресурсам (сайтам), в названии которых имеется соответствие со словами, введенными в списке регулярных выражений. Слова (регулярные выражения) следует разделять пробелами. Следует отметить, что символ маски * не применяется, но неявно присутствует с обеих сторон от каждой подстроки в списке регулярных выражений. Например, при указании регулярного выражения «ok.ru», кроме сайта «Одноклассники» будет отфильтрован и известный туристический сайт «pososhok.ru».

Данная политика проиллюстрирована следующей картинкой. Будет запрещен доступ к сайтам «Одноклассники».

Настройте HTTP/HTTPS прокси и службу UPnP



Служба UPnP HTTP/HTTPS прокси



Укажите внешний интерфейс, интерфейс на котором доступна служба, порт и количество клиентов



Разрешить HTTP/HTTPS прокси? :



Внешний интерфейс (для исходящих соединений)

eth0.2



Интерфейс, на котором доступна служба

br0:



Прокси порт:

3128



Максимальное количество одновременных пользователей (0 для неограниченного количества):

500



Максимальное количество работающих серверов:

20



Минимальное количество работающих серверов. Система автоматически запустит новый сервер, когда количество работающих станет меньше этого значения:

5



Использовать прокси верхнего уровня? :



Политка доступа в прокси 'Запрещено':



Вы можете задать регулярные выражения, чтобы блокировать/разрешить доступ к некоторым URL. Если политика 'Запрещено', то доступ будет разрешен только к URL, соответствующим списку. В противном случае доступ будет разрешен к URL не соответствующим списку. Пожалуйста, используйте пробел, чтобы разделять регулярные выражения:

odnoklassniki \ok. ok.

Удалять retracker.local из транзитных torrent файлов? :

URL Bittorrent retracker, который будет добавлен в транзитные torrent файлы:

Перезапустить сервис(ы) после сохранения? : Сохранить

* Заполнение выделенных полей обязательно!

Пример политики HTTP прокси «все запрещено»

Для политики «Все запрещено» встроенный прокси-сервер будет запрещать запросы к Интернет-ресурсам (сайтам), в названии которых отсутствует соответствие со словами, введенными в списке регулярных выражений. Слова (регулярные выражения) следует разделять пробелами.

Данная политика проиллюстрирована картинкой на следующей странице, в ней запрещен доступ к любым сайтам, кроме «Госуслуг», сайтов правительства и ФНС.

Следует принимать во внимание разницу фильтрации средствами прокси и средствами межсетевого экрана. В главе 5 «Межсетевой экран и средства фильтрации», казалось бы, описан уже аналогичный механизм фильтрации контента для локальных пользователей. Однако, если на межсетевом экране произвести настройки, аналогичные показанным на следующей картинке, то сайт налоговой службы скорее всего у пользователей открываться не будет. И дело даже не в возможных проблемах разрешения доменных имен (DNS). Дело в том, что любой сайт содержит ресурсы не только своего веб-сервера, а еще и ссылки на прочие сайты, часто динамически формируемый контент. А значит, путь на многие из этих ссылок будет проходить через межсетевой экран, который будет все подряд блокировать. В результате даже стартовая страничка любого современного сайта вряд ли сможет отрисоваться в браузере пользователя.

Иное дело - механизм фильтрации HTTP прокси, фильтрующий только непосредственно запросы, исходящие от пользователя, в данном примере URL <https://www.nalog.ru>. В списке разрешенных сайтов он есть, а запросы на дополнительный контент прокси сервером проверяться не будут.

Система | Сеть | Маршрутизация | Услуги | Утилиты | Диагностика

Настройте HTTP/HTTPS прокси и службу UPnP

Служба UPnP | HTTP/HTTPS прокси

Укажите внешний интерфейс, интерфейс на котором доступна служба, порт и количество клиентов

Разрешить HTTP/HTTPS прокси? :

Внешний интерфейс (для исходящих соединений) : eth0.2

Интерфейс, на котором доступна служба : br0

Прокси порт: 3128

Максимальное количество одновременных пользователей (0 для неограниченного количества): 500

Максимальное количество работающих серверов: 20

Минимальное количество работающих серверов. Система автоматически запустит новый сервер, когда количество работающих станет меньше этого значения: 5

Использовать прокси верхнего уровня? :

Политка доступа в прокси 'Запрещено':

Вы можете задать регулярные выражения, чтобы блокировать/разрешать доступ к некоторым URL. Если политика 'Запрещено', то доступ будет разрешен только к URL, соответствующим списку. В противном случае доступ будет разрешен к URL не соответствующим списку. Пожалуйста, используйте пробел, чтобы разделять регулярные выражения:

gosuslugi.ru gov.ru nalog.ru

Удалять retracker.local из транзитных torrent файлов? :

URL Bittorrent retracker, который будет добавлен в транзитные torrent файлы:

Перезапустить сервис(ы) после сохранения? : Сохранить

* Заполнение выделенных полей обязательно!

\\ Настройка прокси верхнего уровня

Использование прокси-сервера верхнего уровня позволяет строить сложные системы сокращения объемов Интернет-трафика / фильтрации контента. Параметры прокси-сервера верхнего уровня устанавливаются в меню «Система → Базовые установки системы» на закладке «Прокси верхнего уровня».



HTTP/HTTPS прокси верхнего уровня (имя хоста или адрес)	<input type="text" value="upstream.stasoft.ru"/>
Порт прокси-сервера	<input type="text" value="3128"/>
Вход/Имя пользователя/Ключ	<input type="text"/>
Пароль	<input type="text"/>

Перезапустить сервис(ы) после сохранения ? :

*** Заполнение выделенных полей обязательно!**

From:
<http://docs.netshe-lab.ru/> - Документация по NETSHe
Permanent link:
http://docs.netshe-lab.ru/doku.php?id=%D0%B3%D0%BB%D0%B0%D0%B2%D0%B0_8_&_http_%D0%BF%D1%80%D0%BE%D0%BA%D1%81%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5
Last update: 2020/07/20 10:20

