

Как срать на Роскомнадзор и смотреть закрытые им сайты

Роскомнадзор разминается на сайтах с «пропагандой» самоубийств и наркотиков для того, чтобы закрывать любые сайты и иметь централизованный контроль над рунетом. Под раздачу порой попадают полезные ресурсы. Если сайт, который вам нравится, будь то любимая сетевая библиотека, статья про вещества или бложек Миши Вербицкого, заблокировали — это не повод, печально пожав плечами, о нем забыть. Напротив — это отличный шанс без труда расширить свои возможности и научиться обходить любые неправомерные запреты, если вы этого еще не умеете. Лениться нельзя: Роскомнадзор имеет тенденцию блокировать целые домены из-за одной страницы, страдают невинные, а сейчас дело дошло до сайтов с кинопродукцией. Даже если владельцы сайтов удалили подозрительный контент и Роскомнадзор изъял их из списка, это вовсе не значит, что ваш провайдер немедленно сделает то же самое. В общем, сегодня закроют бложек Вербицкого, завтра заблокируют книги Хаксли и Хантера Томпсона, послезавтра — Космополитен, Экранку.ру и сайт Эрмитажа. А что дальше? Не нужно задаваться этим вопросом. Нужно делать так, чтобы «запрет» совершенно ничего не изменял ни в функционировании ресурса, ни в вашей жизни. Это по силам любому.

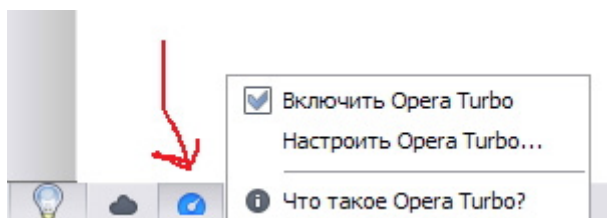
Думаю, что среди наших читателей много людей, которые не подкованы в IT, но хотят знать, как по-простому обойти запреты. Вот вам простой гайд с картинками. В качестве примера запрещенных сайтов будем брать любые сайты с самоубийствами или дудкой из списка здесь: <http://antizapret.info/>. Если не прибегать к ухищрениям, то при попытке открыть страницы провайдер демонстрирует примерно следующее:



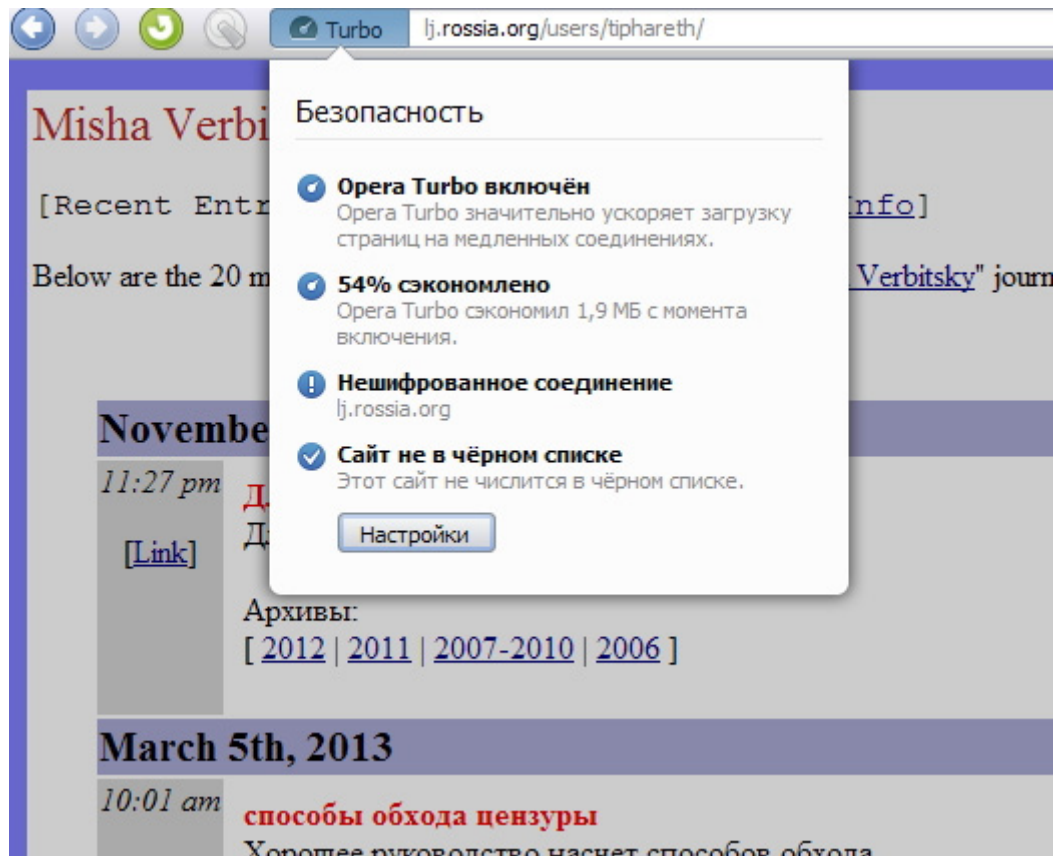
Если вы видите на экране своего экрана что-либо подобное, подчиняться не нужно. Список должен защищать детей, но мы давно уже не дети.

0. Opera Turbo

У пользователей Оперы есть отличная функция, решающая проблему с цензурой с помощью одного клика мышки, — это опция «Турбо». Ее идея заключается в том, что страница передается вам не напрямую, а через зарубежный сервер, где она оптимизируется для выдачи. Для зарубежного сервера заблокированная страница видна, а значит ее видите и вы. Включить ее можно с помощью небольшого значка в нижнем левом углу браузера:



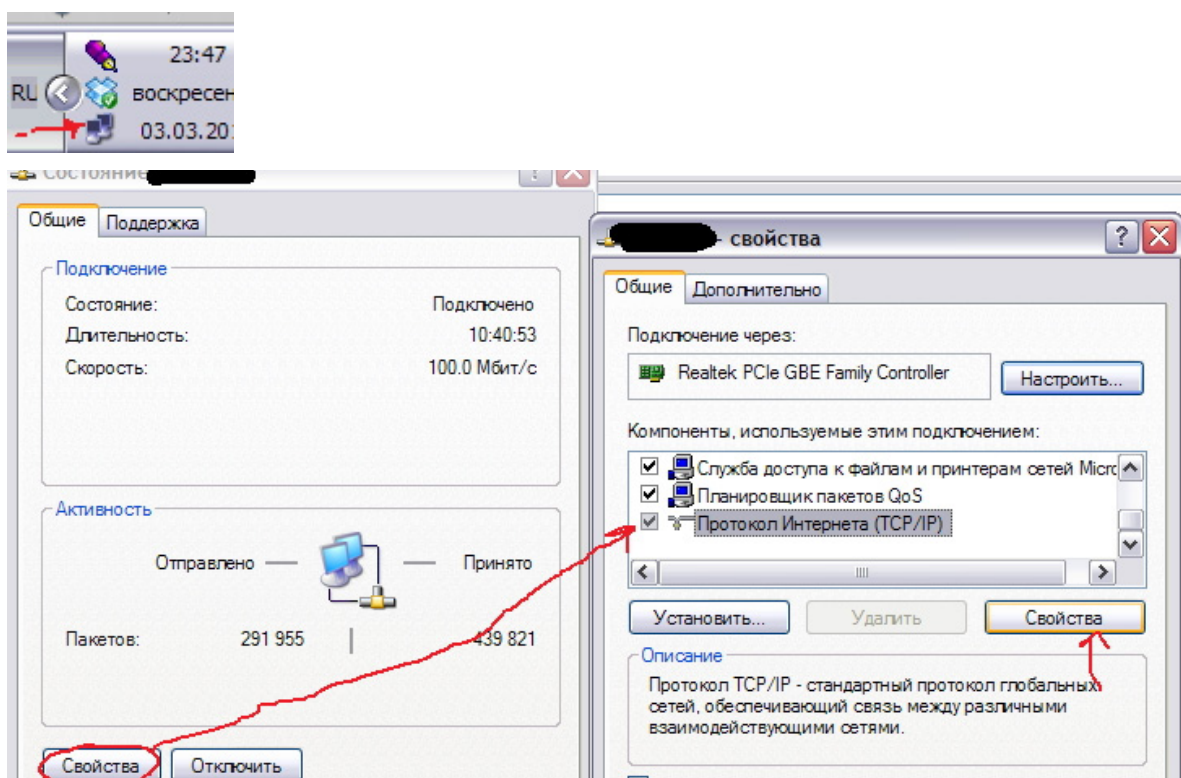
Все, страница в вашем распоряжении:

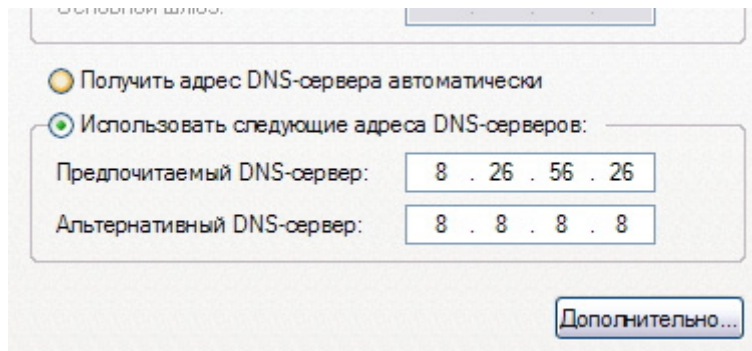


К сожалению, функция работает не всегда, но на сегодняшний день это определенно один из самых простых способов обхода блокировок.

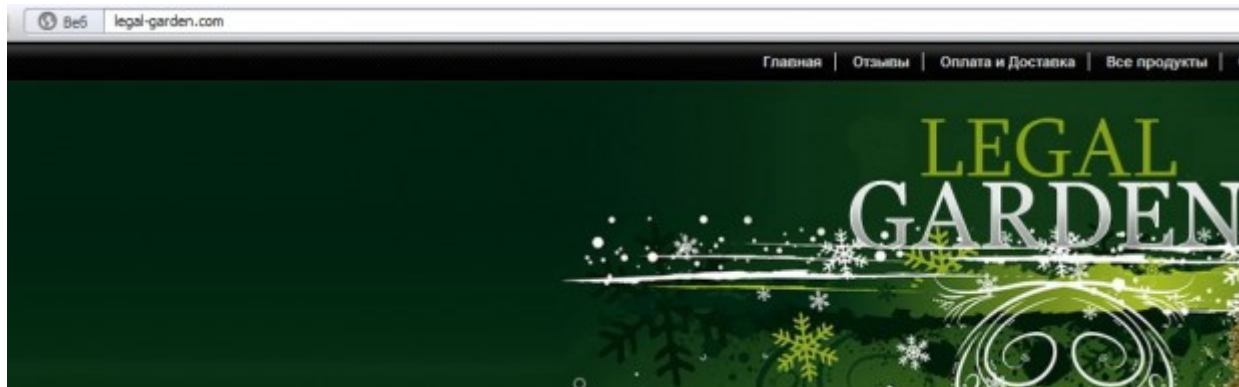
1. Смена DNS-сервера

Некоторые провайдеры не блокируют IP внесенных в список сайтов, поэтому достаточно изменить настройки своего сетевого соединения, поставив вместо DNS-сервера провайдера какой-нибудь публичный DNS-сервер. Для тех, кому предыдущая строка показалась бредом, я просто покажу, что нужно делать. Открываете настройки своего TCP/IP соединения и вписываете цифры 8.26.56.26 и 8.8.8.8 в поля DNS (см скриншоты):





Опа, теперь все сайты с «дудкой» мои:



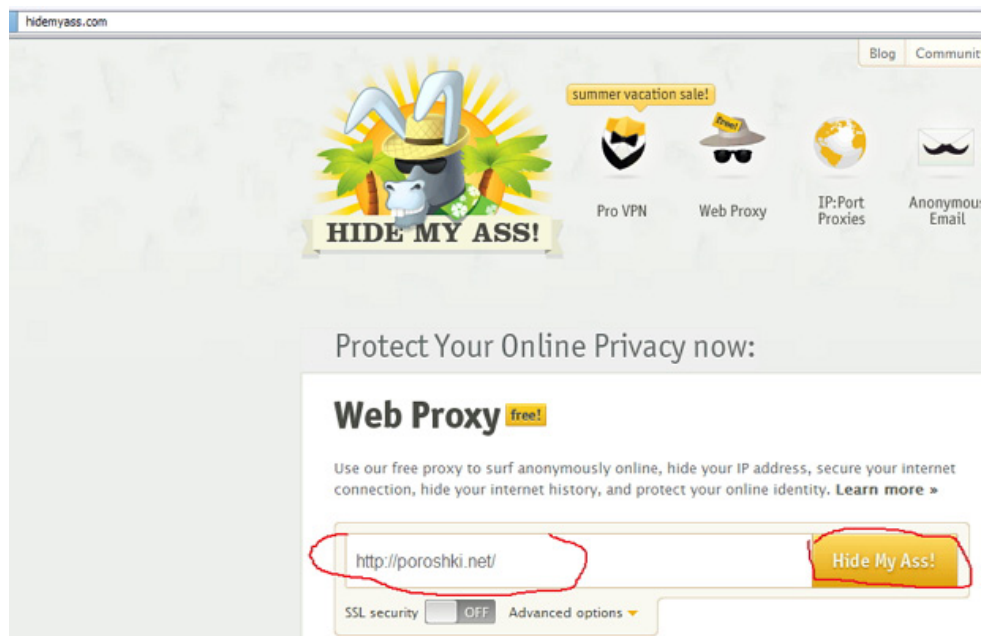
Можно использовать другие DNS из списка – <http://www.bestfreedns.net/>. Способ не подходит для компьютеров «с работы» из-за настроек локальных сетей. **Прежде чем экспериментировать, сохраните предыдущие настройки, чтобы безболезненно вернуться.**

2. Анонимайзеры

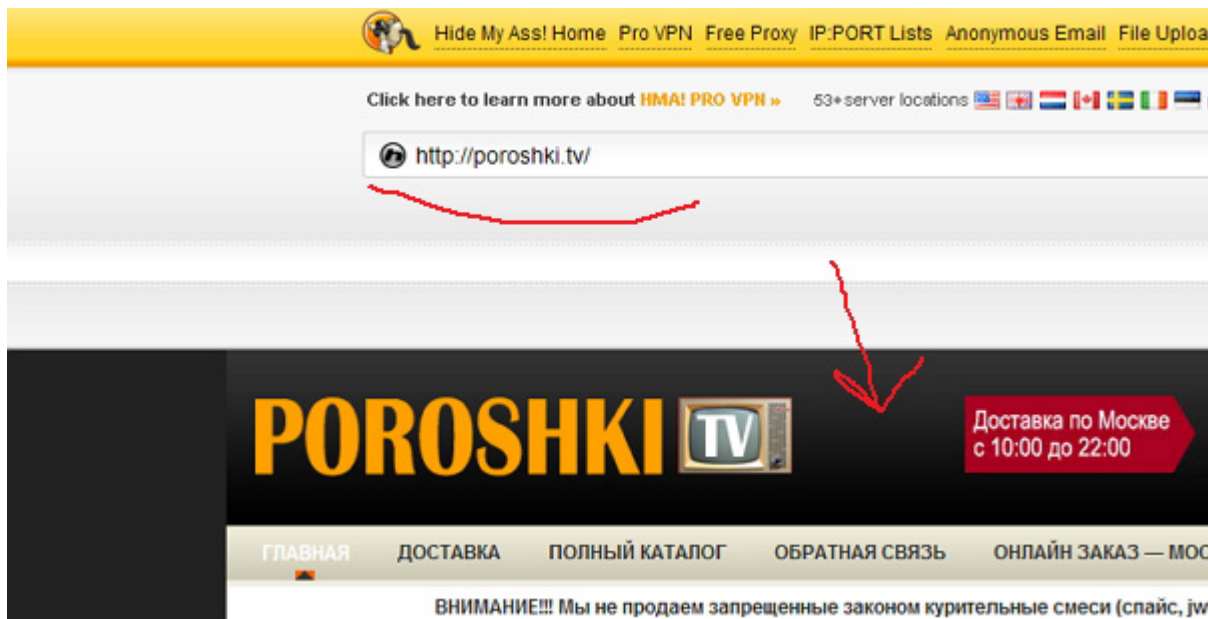
Если простейший способ не сработал, идем дальше. Идея работы анонимайзеров в следующем: вы подключаетесь к сайту вроде hidemyass.com, располагающемуся не в России, вводите нужный адрес в его окно, а анонимайзер транслирует вам в ответ запрещенную страницу, которая в других странах не запрещена.

<http://hidemyass.com/>

Это классика для тех, кто не желает разбираться в тонкостях. Просто заходите на сайт, вводите в окно запретный адрес – и, слегка подождав, получаете его на экране:



Ниже «шапки» анонимайзера виден контент сайта:



Чтобы автоматизировать процесс, можно поставить плагин для браузера (Firefox, Chrome). Но, конечно, это не единственный анонимайзер в мире и даже не самый удобный.

Вот несколько дополнительных примеров:

<http://goforproxy.appspot.com/>

<http://www.proxyweb.net/>

<http://webwarper.net/>

<http://kproxy.com/>

<http://www.pagewash.com/>

http://www.freeproxy.ru/ru/free_proxy/cgi-proxy.htm

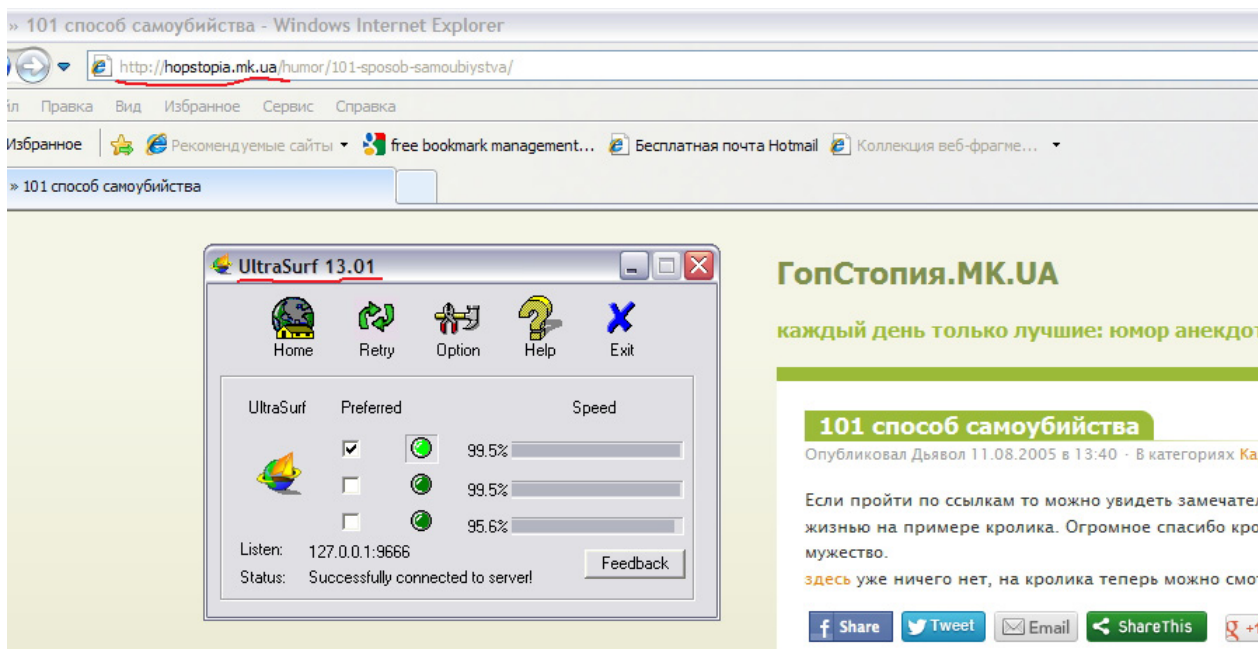
Этот текст рано или поздно устареет, какие-то из перечисленных страниц могут пропасть, но вы всегда можете получить актуальную информацию, поискав по слову «анонимайзер». Многие русские анонимайзеры требуют регистрации, платы или показывают тонны всплывающих окон и рекламы. Такие «анонимайзеры» сразу закрывайте и ищите аскетичные.

Тем, кто не разбирается в сетях и ничего знать об этом не хочет, этого более, чем достаточно, — быстро, просто и легко.

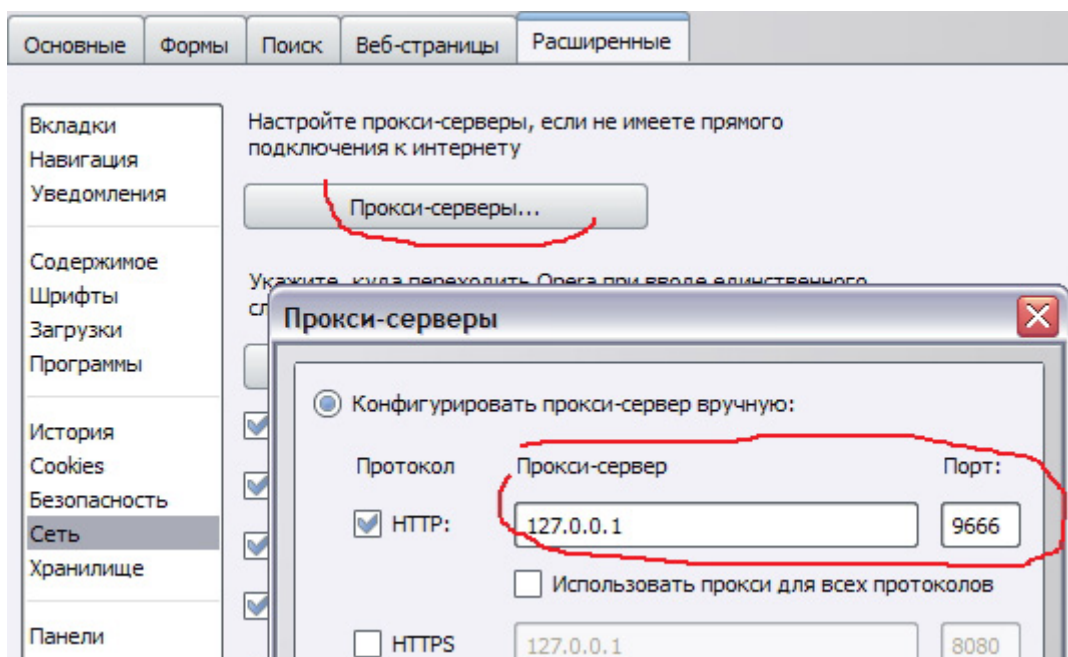
Любой человек, разбирающийся в IT, может развернуть свой публичный анонимайзер.

3. Ultrasurf

Программа была разработана китайцами для защиты от Великого Китайского Фаервола, не дающего получать информацию, отличающуюся от линии партии. Теперь она может послужить и вам. Скачиваете программу здесь — <http://ultrasurf.us/>, устанавливаете. При запуске она автоматически открывает настроенный на работу Internet Explorer, куда можно вводить нужный адрес и получать результат:



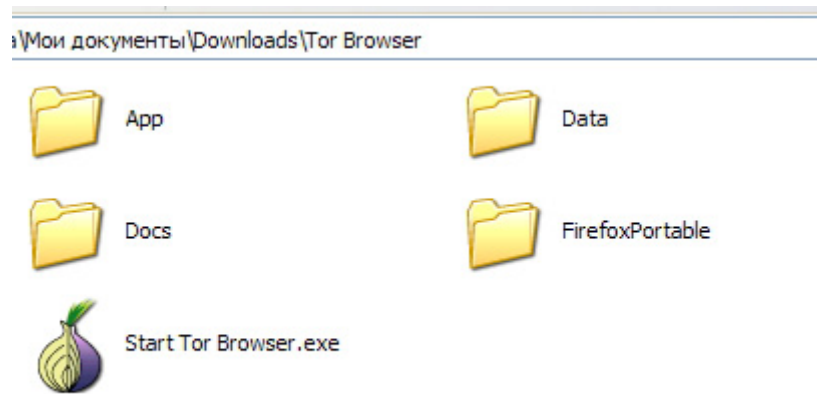
Те, кто работать с IE не способен из-за отвращения, могут настроить свой браузер на работу с ultrasurf. Для этого откройте настройки браузера и в качестве прокси-сервера укажите следующее:



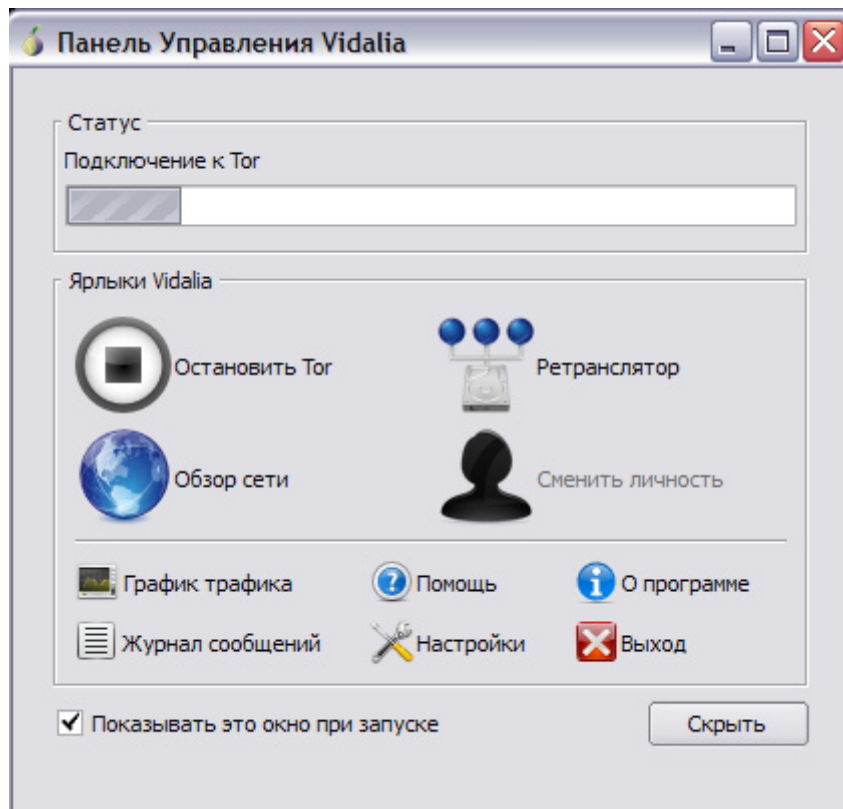
4. Tor

Возможности сети Тор велики, и хорошо то, что «почувствовать себя хакером» может любой. Я просто покажу, как можно использовать Тор для открытия запрещенных сайтов. Для простоты я буду полагать, что вы используете Windows. Люди, использующие Linux, в таких инструкциях не нуждаются. Подчеркиваю, что для установки не требуется никаких спецзнаний. Можно быть девочкой в розовом, которая при слове «IP» зеленеет, — это совершенно не мешает открывать запрещенные Роскомнадзором сайты!

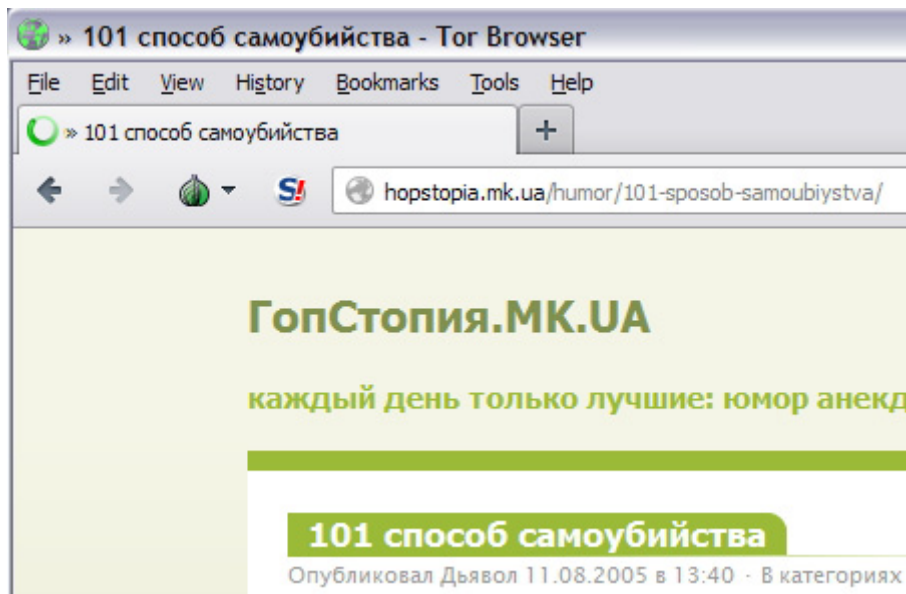
Скачиваете пак Tor Browser Bundle отсюда — <http://www.torproject.org>. Конечная ссылка может со временем меняться, но зайдя на torproject.org вы найдете, откуда скачать. Запускаете и распаковываете в папку, где затем сможете его найти. Например, так:



Запускаете «луковицу». Через некоторое время видите вот такое окно:



Следом открывается специально настроенный браузер Firefox и поздравляет вас. Ура, можно открывать запрещенные сайты с котиками в дополнительном браузере и наслаждаться:



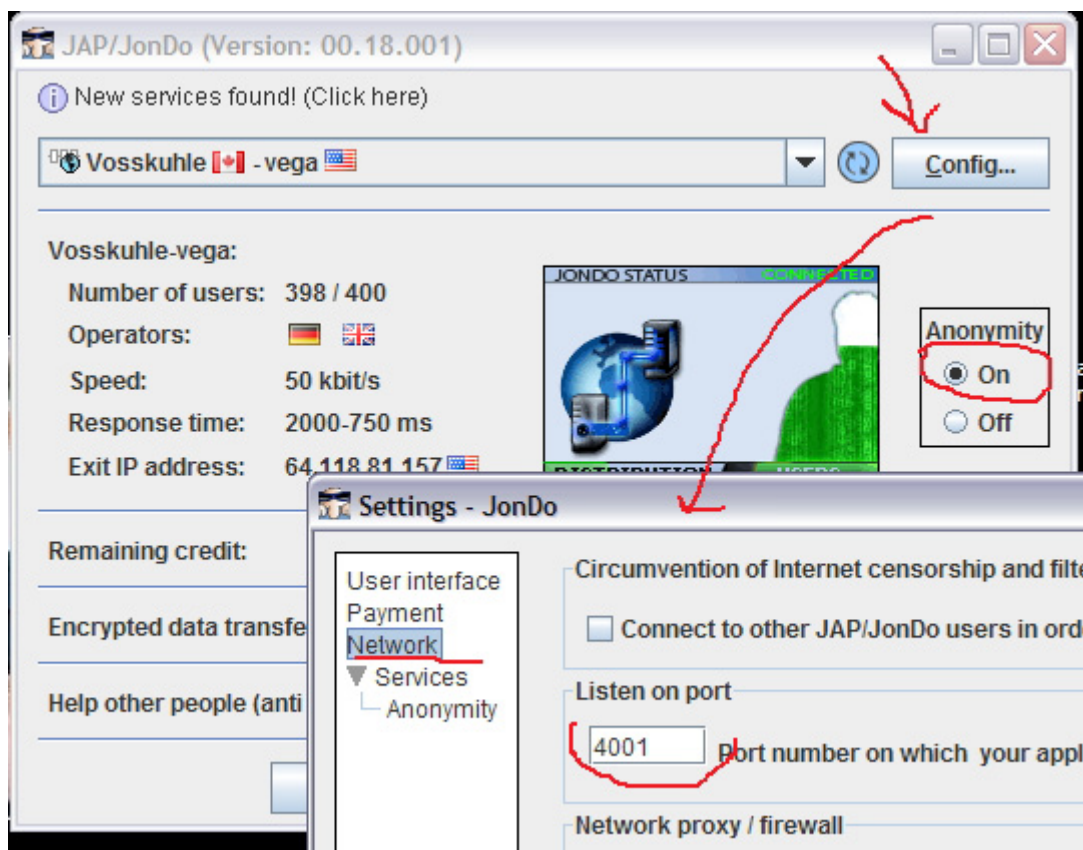
5. JAP

Я фанат JAP'a со старых времен по многим причинам, даже использую его платную версию. Он дает возможность подключаться к сети через каскад зарубежных прокси-серверов, поэтому годится больше для анонимизации (у вас будет IP адрес европейской страны), но его вполне можно использовать и для того, чтобы срать в рот Роскомнадзору. Почему нет – очевидно же, что на простых мерах они не остановятся. Единственная проблема в том, что бесплатные каскады работают медленно. Также я рекомендую этот способ для продвинутых пользователей, новичкам он может показаться слишком сложным.

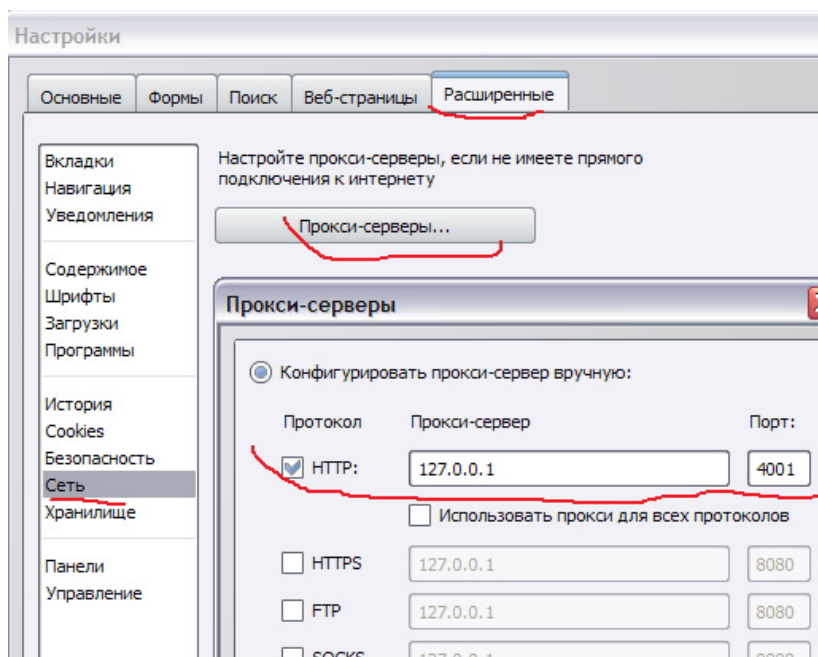
Скачать программу можно отсюда: http://anon.inf.tu-dresden.de/win/download_en.html



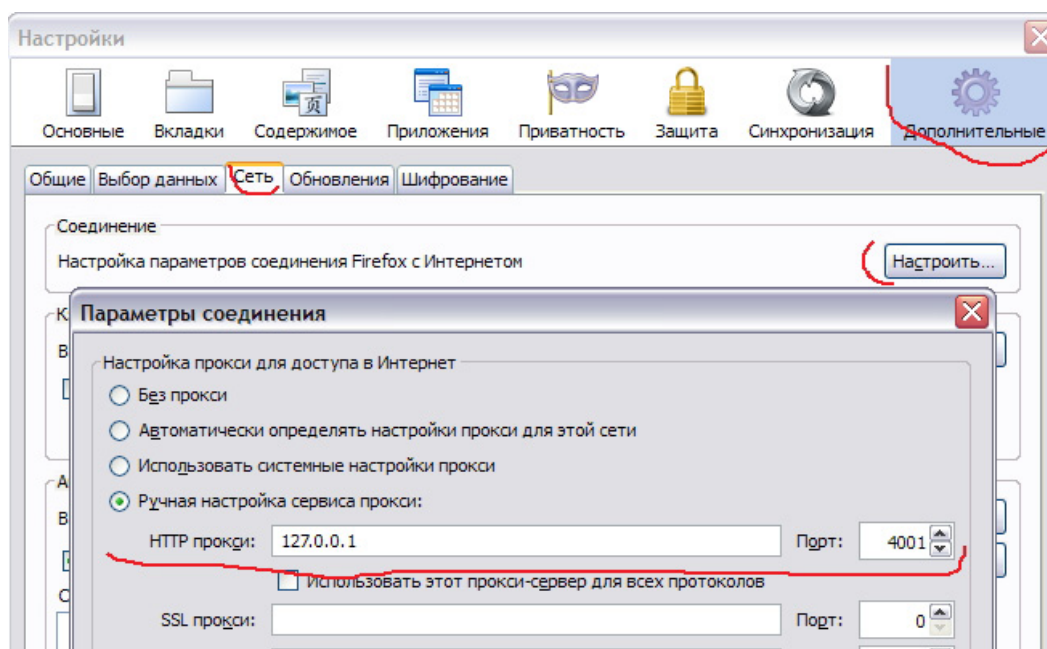
Для настройки придется немного поднапрячься, но осилить нехитрую цепь действий может каждый. После запуска программы проверьте опции и включите «Анонимность»:



Ваш интернет-браузер должен перенаправлять свои запросы на этот порт. Для этого откройте настройки соединения своего браузера (здесь для примера используется Опера):

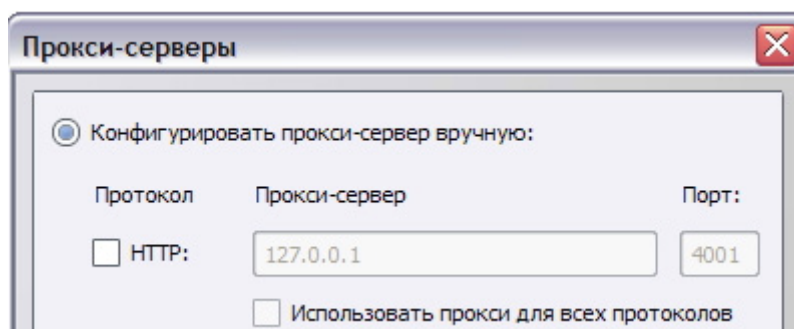


То же самое для Firefox:



После этого все соединения из вашего браузера будут перенаправляться в JAR. Наберите адрес в строке браузера, как обычно. Все запрещенные страницы со скриптом, но откроются.

Бесплатная версия работает медленно, однако дает доступ туда, куда вам с российским IP вход запрещен, а также демонстрирует закрытые Роскомнадзором сайты. Когда вам надоест, уберите прокси в настройках браузера:



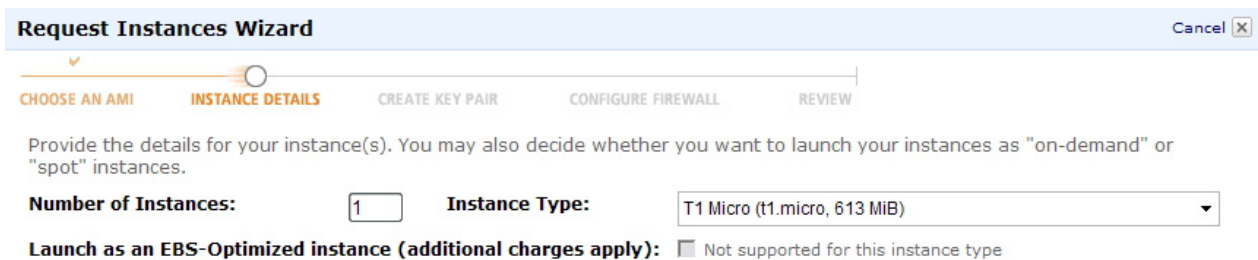
6. Хардкор

SSH-туннель к амазоновскому серверу или VPN на его базе.

Этот способ, конечно, для рядовых пользователей не подходит, но было бы неверно о нем не рассказать для остальных. Существует просто масса различных статей и видео на этот счет, потому что идея пришла в голову не только мне. Результат стоит небольших денег. Привожу этот пример потому, что он дико прост и этим очень остроумен. Лично мне он кажется крайне смешным. Amazon EC2 позволяет создавать сервера с различными операционными системами и мощностями и гонять их за умеренную почасовую оплату. Цена нужного нам инста (small, linux) – 0.03 (!) \$ / час. Вряд ли вы будете зачитываться запрещенными ресурсами дольше, но даже при условии работы по несколько часов в день – это весьма гуманно. Сервера располагаются в Америке и Ирландии, что идеально подходит для туннелирования.

Я буду исходить из того, что о создании машин в Amazon EC2 вы знаете и у вас уже есть аккаунт. Логиньтесь в консоль: <https://console.aws.amazon.com/ec2/home?region=us-east-1#s=Instances>, выберите EC2 -> Instances.

Создаете инст по вкусу: Launch instance -> выбор операционки (я для примера беру Red Hat или Ubuntu, тип – Micro):



Request Instances Wizard Cancel X

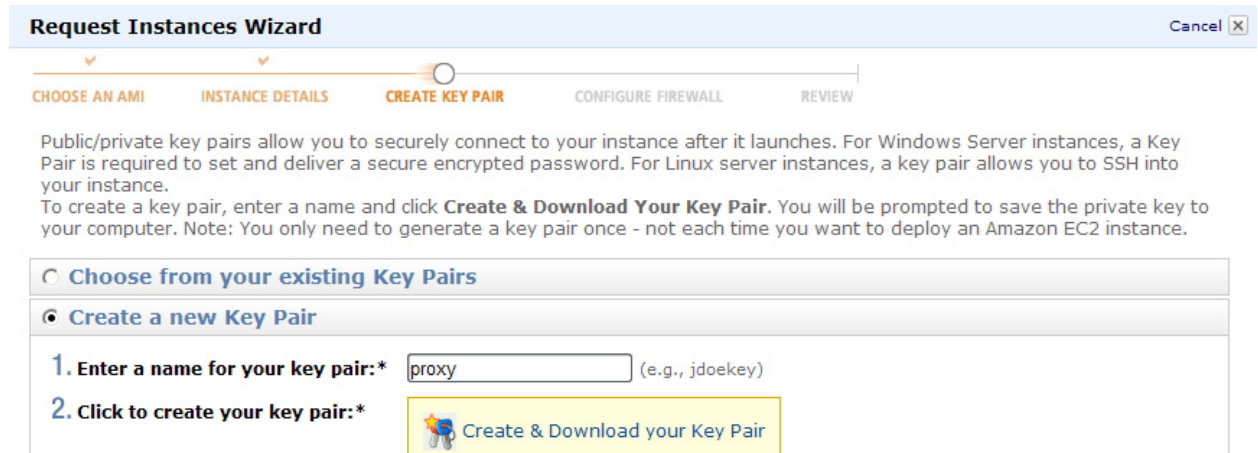
CHOOSE AN AMI | **INSTANCE DETAILS** | CREATE KEY PAIR | CONFIGURE FIREWALL | REVIEW

Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: **Instance Type:**

Launch as an EBS-Optimized instance (additional charges apply): Not supported for this instance type

Дальше все оставляете, как есть, -> создаете ключ и загружаете его:



Request Instances Wizard Cancel X

CHOOSE AN AMI | INSTANCE DETAILS | **CREATE KEY PAIR** | CONFIGURE FIREWALL | REVIEW

Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux server instances, a key pair allows you to SSH into your instance. To create a key pair, enter a name and click **Create & Download Your Key Pair**. You will be prompted to save the private key to your computer. Note: You only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

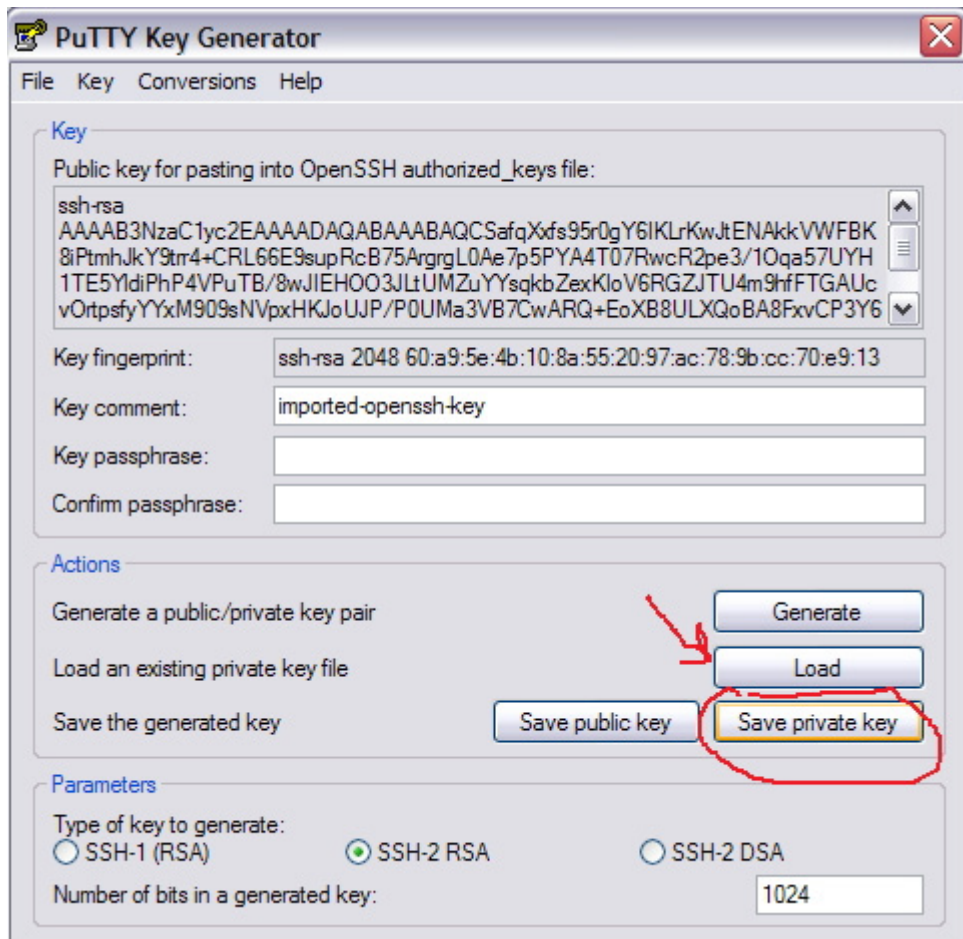
Choose from your existing Key Pairs

Create a new Key Pair

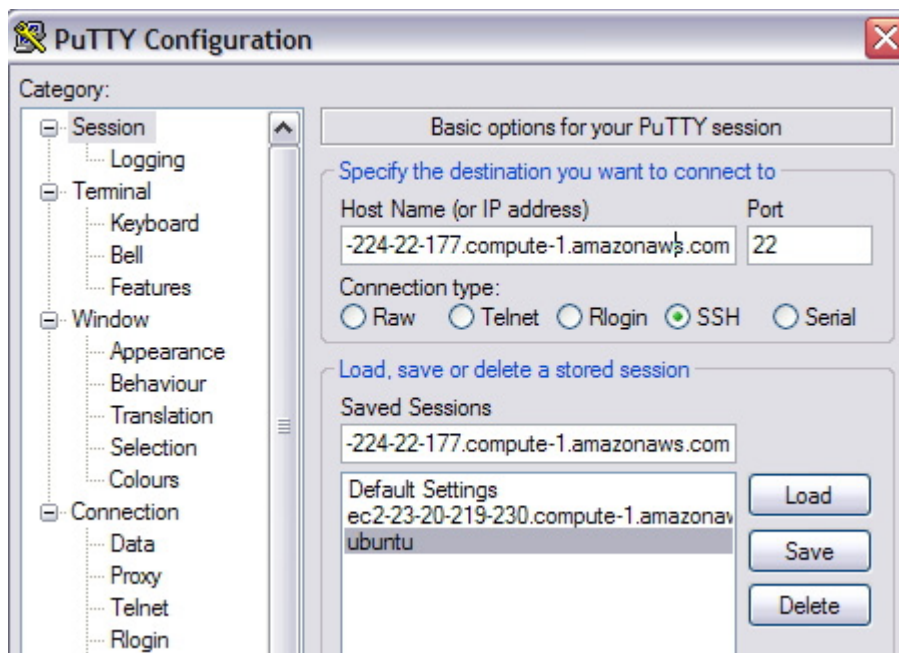
1. Enter a name for your key pair:* (e.g., jdoekey)

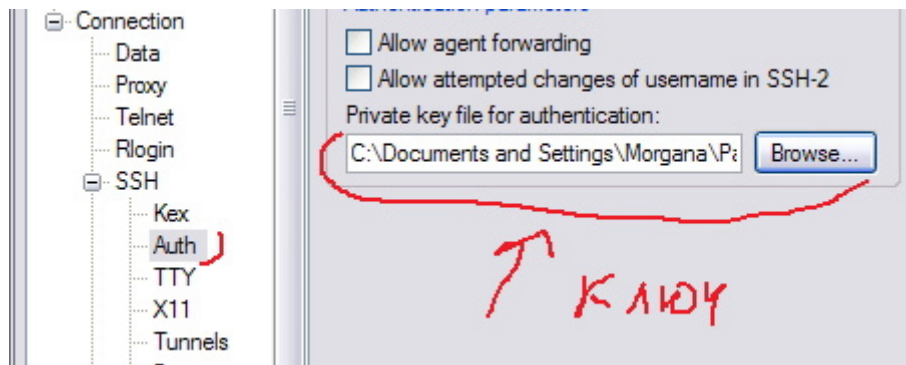
2. Click to create your key pair:*

Включаете в секьюрители-группу, где открыт SSH-порт (22), запускаете машину. После того, как инст запустился, к нему нужно подключиться. Для более разящего эффекта сделаем это через putty. Для этого загружаете ключ в Putty Key Generator (Load) и сохраняете private key:

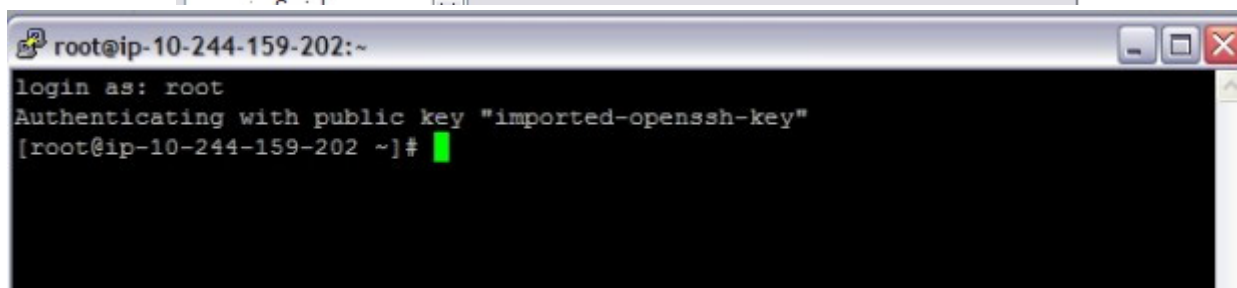
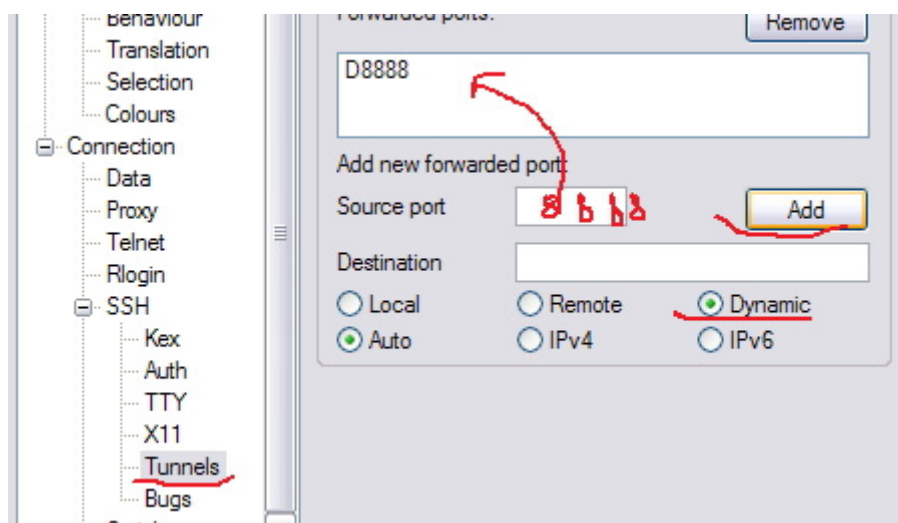


Дальше нужно настроить соединение к серверу. Смотрите public DNS в консоли и настраиваете подключение в putty:

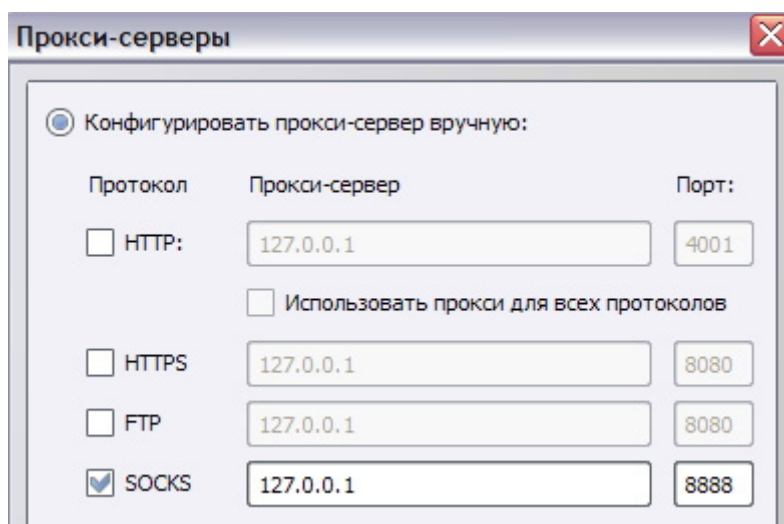




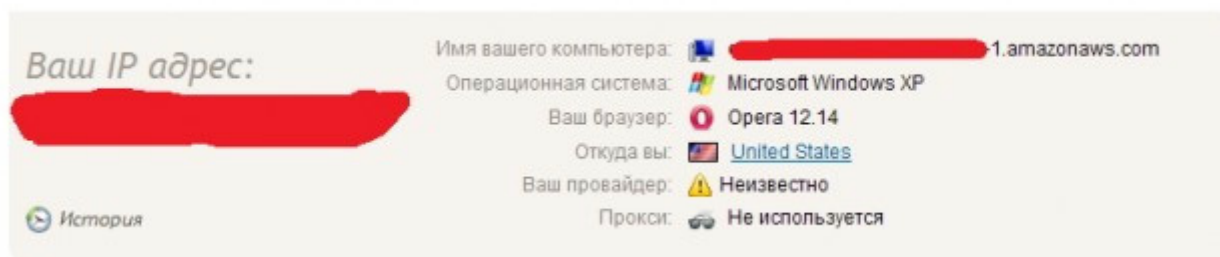
Порт выбираете любой свободный. Браузер будет обращаться на него, putty отправит запрос амазоновскому серваку, а затем примет ответ и перенаправит браузеру:



Отлично. Теперь настраиваете в браузере SOCKS-проху. Проху в данном случае выступает Putty:



Опа, у меня американский IP, высокая скорость и открыты абсолютно все сайты, нелюбимые Роскомнадзором.



Способ очень забавный, потому что прямолинейный. Можно развернуть свой VPN, но об этом есть масса материалов. Не забывайте выключать инсты, чтобы не тратить зря деньги. Если вы планируете качать что-либо или раздавать, имейте в виду, что исходящий трафик стоит небольшие суммы (детали). Кроме того вы не обеспечите себе анонимность, что хоть и не являлось целью моего текста, но все же важно помнить.

Я перечислила далеко не все возможные способы, друзья. Не подчиняйтесь неправомерным запретам.

