КАК ИЗБЕЖАТЬ ЦЕНЗУРЫ: ТЕХНИЧЕСКИЕ СОВЕТЫ

Нарт Вилленёв (Nart Villeneuve)

СОДЕРЖАНИЕ

- **ФИЛЬТРАЦИЯ КОНТЕНТА**
- **ТЕХНОЛОГИИ ОБХОДА (CIRCUMVENTION)**
- **ОЦЕНКА ПОТРЕБНОСТЕЙ И ВОЗМОЖНОСТЕЙ**
- **WEB-ТЕХНОЛОГИИ ОБХОДА ИНТЕРНЕТ-ФИЛЬТРОВ**
  - Общедоступные онлайновые системы
  - Программное обеспечение
  - Обеспечение безопасности
- **PROXY-СЕРВЕРЫ**
  - Программное обеспечение
  - Общедоступные proxy-серверы
    - Местонахождение открытых серверов
    - Открытые серверы
  - Proxy- серверы: безопасность
- **ТУННЕЛИРОВАНИЕ**
- **АНОНИМНЫЕ СИСТЕМЫ КОММУНИКАЦИИ**
- **ЗАКЛЮЧЕНИЕ**

ФИЛЬТРАЦИЯ КОНТЕНТА

Технологии фильтрации позволяют контролировать доступ к интернет-контенту. Разработанные первоначально для индивидуальных нужд – чтобы родители могли ограничивать доступ детей к нежелательному контенту – технологии фильтрации в настоящее время широко используются различными организациями и государственными структурами. Контроль доступа к интернет-контенту становится приоритетом для целого ряда организаций и учреждений, в том числе для школ, библиотек и корпораций. Технологии фильтрации все шире используются на государственном уровне. Все население страны могут лишать доступа к определенным сайтам, при этом правительства практически не отчитываются в своих действиях.

Технологии фильтрации основываются на блокировании определенных сайтов, входящих в список запрещенных, и на контроле определенных ключевых слов, что позволяет осуществлять динамичное блокирование контента. Составляются списки доменных имен и URL, затем они систематизируются и сообщаются специальным прог-

раммам, которые блокируют определенные категории сайтов. Когда пользователи пытаются открыть страницу, программа фильтрации обращается к базе данных и блокирует доступ к страницам, включенным в список. Если блокируется поиск по определенным ключевым словам, программа проверяет каждую страницу (домен, URL и/или тело контента (body content) запрашиваемой страницы) и динамически блокирует доступ к web-странице, если обнаруживается какое-либо из запрещенных ключевых слов.

Системы фильтрации могут допускать две основных ошибки: избыточное и недостаточное блокирование. Они часто блокируют доступ к неправильно классифицированному контенту или, наоборот, не блокируют контент, доступ к которому запрещен. Однако главное – это покров тайны, окружающий создание списков сайтов, которые блокируются при помощи технологий фильтрации. Существуют, конечно, открытые списки (они касаются, в основном, порнографии), но списки коммерческих фильтров и списки фильтрации, осуществляемой государственными структурами, сохраняются в тайне. Списки категорий доменов и URL, входящих в коммерческие фильтры, являются интеллектуальной собственностью производителей и не сообщаются широкой публике. Хотя некоторые производители программного обеспечения для фильтрации открывают доступ к онлайновым программам контроля URL, списки блокируемых сайтов остаются секретными и недоступными для независимого наблюдения и анализа.

Очень часто правительства расширяют списки сайтов коммерческих технологий фильтрации. Эти списки часто включают сайты оппозиционных политических партий и газет, правозащитных организаций, международных агентств новостей, сайты, критикующие правительство. В большинстве стран фильтруется, прежде всего, контент на национальном языке, важной мишенью являются также сайты, где возможны дискуссии, в частности, блоги и интернет-форумы.

WEB-ТЕХНОЛОГИИ ОБХОДА ИНТЕРНЕТ-ФИЛЬТРОВ

В ответ на фильтрацию и мониторинг интернета государством, разрабатываются различные технологии, позволяющие пользователям обойти ограничения фильтрации. Существует ряд технологий, которые позволяют гражданам и общественным организациям защитить себя и обходить интернет-цензуру. Эти инструменты получили название «технологий обхода» (circumvention). Суть этих технологий заключается в том, что запрос из страны, где осуществляется фильтрация перенаправляется на машину -посредник, которую фильтр не может блокировать. Этот компьютер затем находит информацию по запросу и передает ее пользователю. Иногда такие технологии разрабатываются с учетом специфической ситуации в стране. Во многих случаях пользователи могут адаптировать для обхода (circumvention) технологии, которые изначально разрабатывались для других целей.

Одни технологии были разработаны частными компаниями, другие – группами хакеров и активистов. Программы могут представлять собой как простые скрипты, так и сложные сетевые протоколы. Принимая во внимание это разнообразие,

потенциальные пользователи должны научиться анализировать достоинства и недостатки определенных техник и технологий, чтобы выбрать способы обхода (circumvention), соответствующие их потребностям.

В реализации технологии обхода (circumvention) участвуют провайдер обхода (circumvention provider) и пользователь. Провайдер обхода устанавливает программу на ссвоем компьютере, находящемся вне зоны фильтрации и делает сервис доступным онлайн для пользователей в зоне контроля. Таким образом, успех технологии зависит от того, насколько она соответствует специфическим потребностям обеих сторон.

Цель данной статьи – проинформировать пользователей, решивших обратиться к технологиям обхода, о существующих возможностях и о критериях выбора подходящей технологии. При этом я учитывал потребности и возможности обоих сторон, пользователей и провайдеров технологий обхода, что необходимо для соблюдения баланса между требуемым уровнем безопасности и удобством технологии для конечного пользователя. Эффективный, безопасный и надежный обход зависит от выбора правильной технологии, нужной пользователю.

ЦЕНКА ПОТРЕБНОСТЕЙ И ВОЗМОЖНОСТЕЙ

Технологии обхода часто предназначены для различных типов пользователей с разными возможностями и опытом. То, что хорошо работает в одной ситуации, может быть не самым лучшим решением для другой. При выборе технологии обхода потенциальный провайдер должен задать себе следующие вопросы:

Сколько будет пользователей и какова пропускная способность каналов? (провайдера и пользователя).
Где находится пункт первичного интернет-доступа предполагаемых пользователей и цель использования?
Каков технический уровень? (провайдера и пользователя).
Доступны ли конечному пользователю надежные внешние контакты?
Какие меры наказания грозят провайдеру и пользователю за использование технологии обхода?
• Понимает ли конечный пользователь угрозы, связанные с использованием специфических технологий обхода?

КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ И ДОСТУПНАЯ ПРОПУСКНАЯ СПОСОБНОСТЬ

Провайдер обхода должен оценить количество пользователей и соотнести это с возможной пропускной способностью канала. Конечный пользователь также должен принимать во внимание пропускную способность интернет-канала, поскольку использование обходных технологий замедлит скорость интернет-доступа.
Те, кто предполагает создать общественно доступный proxy-сервер, должны учитывать, что сервер могут использовать люди, не находящиеся там, где осуществляется фильтрация. Например, сервер может использоваться для загрузки фильмов, что может поглощать большой объем трафика. Поэтому вы, возможно, будете ограничивать либо

доступ к серверу, либо трафик. Различные технологии предоставляют различные возможности для разрешения подобных проблем.

ПЕРВИЧНЫЙ ПУНКТ ДОСТУПА И ИСПОЛЬЗОВАНИЕ

В зависимости от места доступа конечного пользователя, выбираются различные технологии обхода и услуги сервера. Например, пользователи, подключающиеся к интернет через общественно-доступные компьютеры и в интернет-кафе, скорее всего, не смогут устанавливать программное обеспечение, их доступ к онлайновым решениям также может быть ограничен. Некоторые будут стремиться использовать не только решения, основанные на технологии WWW (http), но и электронную почту (SMTP) и программы передачи файлов (FTP), поэтому им необходимо будет устанавливать новое программное обеспечение и изменять установки. Конечно, это требует определенных технических навыков.

УРОВЕНЬ ТЕХНИЧЕСКИХ ЗНАНИЙ

Чем выше уровень технических знаний (и меньше число пользователей), тем большее число решений становится доступным. Основными проблемами для простых пользователей являются инсталляция и запуск процесса, изменения конфигурации и другие действия, которые необходимо предпринять для реализации технологии обхода. Это касается как провайдера обхода, так и конечного пользователя. Некорректное использование технологий обхода подвергает пользователей неизбежному риску.

НАДЕЖНЫЕ КОНТАКТЫ

Большое значение для конечных пользователей имеет наличие людей, которым они доверяют, за пределами страны. Если у пользователя нет контактов, его возможности ограничены общедоступными системами. Но если пользователь может найти эти системы, то же могут сделать и те, кто осуществляет фильтрацию и блокирование. Имея надежные контакты, конечный пользователь может консультироваться с провайдером для того, чтобы выбрать решение, соответствующее его специфическим потребностям, сохраняя при этом конфиденциальность. Успешное и длительно использование технологий обхода в значительной степени зависит от надежных контактов с людьми, живущими там, где фильтрация не осуществляется.

ВОЗМОЖНЫЕ НАКАЗАНИЯ

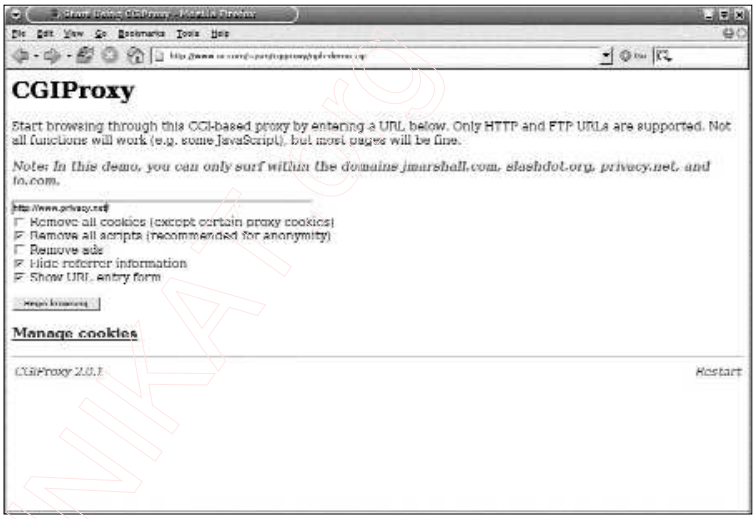
Чрезвычайно важно знать о наказаниях за использование технологий обхода. Выбор решения зависит от суровости наказания. Если законодательство достаточно мягкое и наказание не слишком сурово, пользователи могут выбрать эффективное решение, которое не требует чрезвычайной секретности. Но если законодательство сурово, необходимо выбирать технологии, которые обеспечивают максимальный уровень безопасности. Возможно даже придется придумывать легальное прикрытие для обходных технологий или другие меры предосторожности.

РИСКИ БЕЗОПАСНОСТИ

Очень часто пользователям предлагают обходные технологии, не предупреждая их о возможных рисках, которые могут быть минимизированы при использовании нужной технологии в нужном месте и при правильном поведении конечного пользователя.

WEB-ТЕХНОЛОГИИ ОБХОДА ИНЕТРНЕТ-ФИЛЬТРОВ

Web-технологии обхода – это специальные вебстраницы, содержащие форму, которая позволяет пользователю просто ввести URL, после чего онлайновая система обхода (web-based circumventor) осуществляет поиск страницы и показывает ее пользователю. Между пользователем и запрашиваемым сайтом не устанавливается связь, сервер передает запрос, что позволяет пользователю, оставаясь незамеченным, просматривать блокированные сайты. Онлайновые серверы также переписывают ссылки в запрашиваемой странице, так что пользователь может продолжать интернет-поиск. При использовании онлайновых систем обхода, конечному пользователю не нужно устанавливать никаких дополнительных программ. Все, что нужно сделать – это придти на соответствующий сайт, ввести URL сайта, который они хотят посетить и щелкнуть на кнопку (Внешний вид онлайновых систем обхода может быть разным, но их базовые функции одинаковы). Таким образом, не требуется никаких специальных технических знаний. Кроме того, эту технологию можно использовать независимо от типа доступа.



Proxy-серверы / изменение установок

Преимущества:

Онлайновые системы обхода просты в использовании и не требуют от конечного пользователя установки специальных программ.

Общедоступными онлайновыми услугами обхода могут пользоваться те, кто не имеет

надежных контактов там, где не осуществляется фильтрация.
Частные онлайновые системы обхода могут адаптироваться к специфическим нуждам пользователей, такие системы сложнее отследить органам, осуществляющим фильтрацию.

Недостатки:
Онлайновые системы обхода чаще всего ограничены web-трафиком (HTTP) и закрыты для шифрованного доступа (SSL). Так что web-сервисы (например, web-почта), которые требуют аутентификации, могут плохо функционировать. Общедоступные онлайновые услуги обхода обычно хорошо известны и могут быть заблокированы. Большинство таких серверов блокируется коммерческими фильтрующими программами.
Для того, чтобы пользоваться частными онлайновыми системами обхода, необходимо иметь связи с людьми в тех странах, где контент не фильтруется. В идеале, стороны должны иметь возможность общаться, не подвергаясь угрозе слежки.

ОБЩЕДОСТУПНЫЕ ОНЛАЙНОВЫЕ СИСТЕМЫ ОБХОДА

Существует как общедоступное программное обеспечение для обхода фильтров, так и общедоступные услуги. Большинство из них - бесплатные, хотя системы, предоставляющие дополнительные услуги (шифрованный доступ) могут требовать платную подписку. Вот несколько примеров:

http://www.anonymizer.com/	http://www.guardster.com/
http://www.unipeak.com/	http://www.webwarper.net/
http://www.anonymouse.ws/	http://www.proximal.com/
http://www.proxyweb.net/	http://www.the-cloak.com/

Поскольку эти адреса широко известны, они уже включены в большинство списков интернет - фильтров. Ясно, что если эти сайты блокированы, то пользоваться услугами невозможно. Кроме того, большинство общедоступных систем обхода не шифруют трафик между системой обхода и конечным пользователем. Любая информация, отправленная пользователем, может быть перехвачена оператором программы обхода.

Общедоступные системы обхода наиболее удобны для пользователей, которые подвергаются минимальному риску, не имеют личных контактов в странах, где не осуществляется интернет-фильтрация, обращаются к услугам от случая к случаю и не нуждаются в передаче важной информации.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Установка программного обеспечения для обхода фильтрации может требовать определенных технических знаний и ресурсов (сервер и пропускная

способность). Местонахождение частного сервера известно только тем, кто имеет к нему доступ, в то время как адреса общедоступных систем обхода и анонимных серверов известны как пользователям, так и тем, кто осуществляет фильтрацию (эти адреса также входят в списки блокировки всех коммерческих фильтров). Частную систему обхода гораздо сложнее найти и блокировать, чем общедоступную.

Частные системы обхода можно приспособить к специфическим нуждам конечного пользователя. Так, например, обычно изменяют номер порта на сервере и выполняют шифрование. Протокол защищенных сокетов (Secure Sockets Layer, SSL) - это протокол, гарантирующий безопасную передачу данных по сети. Этот протокол обычно используется сайтами для того, чтобы обеспечить защиту передаваемой информации, например номера кредитных карточек. Доступ к сайтам, защищенным SSL, обеспечивается посредством протокола HTTPS, вместо обычного HTTP.

Кроме того, SSL позволяет создать в корне сервера безвредную страницу и скрыть систему обхода при помощи случайного пароля и имени файла. Несмотря на то, что третья сторона может определить сервер, с которым связывается пользователь, она не сможет проследить путь запроса, поскольку часть запроса шифруется. Например, если пользователь запрашивает адрес https://example.com/sectretcircumventor/, третья сторона увидит только часть https://example.com/, и не узнает, что пользователь обращался к системе обхода. Если оператор размещает безвредную страницу на example.com, то система обхода вообще не будет обнаружен.

- CGIProxy: A CGI-скрипт, работает как HTTP или FTP proxy.
  http://www.jmarshall.com/tools/cgiproxy
- Peacefire's Circumventor: автоматический инсталлятор программ, который облегчает установку и настройку CGIProxy для неопытных пользователей.
  http://www.peacefire.org/circumventor/simple-circumventor-instructions.html
- pHproxy: экспериментальная, имеющая гибкие настройки онлайновая система обхода.
  http://ice.citizenlab.org/projects/phproxy
- Psiphon: SSL- вебсервер с свтроенной онлайновой системой обхода (будет запущен в ближайшее время).
  http://soon to be released

Частные онлайновые системы обхода, обеспечивающие шифрование, удобны для пользователей, которым необходимо постоянно обращаться к технологиям обхода и которые имеют надежные контакты в странах, где не осуществляется фильтрация интернет, с людьми, обладающими достаточными техническими навыками и ресурсами и способными поддерживать онлайновую систему обхода. Это наиболее гибкое решение для обычного интернет-трафика. Оно достаточно надежно и защищено от блокирования.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Системы обхода не всегда обеспечивают анонимность. Личность конечного пользователя скрыта от операторов посещаемых сайтов. Если же сеанс связи между пользователем и онлайновой системой обхода осуществляется в режиме простого текстового протокола (HTTP), на котором основано большинство бесплатных услуг, контент может быть легко перехвачен и проанализирован третьей стороной, в частности, провайдером услуг интернет (ISP). Поэтому даже при успешном обходе фильтрации, власти могут установить факт посещения пользователем онлайновой системы обхода. Более того, они могут определить контент, включая список сайтов, которые посещал пользователь онлайновой системы обхода.

Онлайновые системы обхода, которые работают в режиме простого текста (нешифрованного) часто используют замену знаков в URL, чтобы сбить с толку системы, предназначенные для фильтрации контента по ключевым словам в URL. Например, простая технология ROT-13 основана на том, что буквы заменяются одним из 13 символов, предшествующими им в алфавите: URL http://ice.citizenlab.org принимает вид uggc://vpr.pvgvmrayno.bet/ . Другими словами, текст URL кодируется таким образом, что ключевые слова, по которым осуществляется фильтрация, исчезают из URL. Тем не менее, контент сайта остается доступным для прослеживания даже в случае удачного обхода.

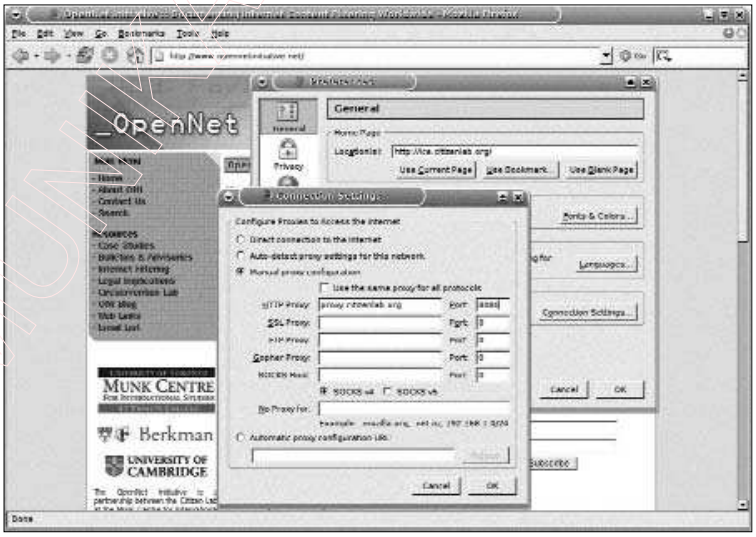
Существуют также риски, связанные с использованием скриптов и фрагментов данных о предыдущих обращениях пользователей (cookies). Многие онлайновые системы обхода удаляют такие фрагменты и скрипты. Однако при этом должны соблюдаться определенные предосторожности. С этим связан и риск использования паролей при входе в систему, основанную не передаче простого текста и использования системы для запроса информации с шифрованного сервера (encrypted server). В этой ситуации, системы обхода получают информацию от SSL-сервера посредством передачи шифрованных данных, но затем посылают контент пользователю в виде простого открытого текста. Таким образом, создается возможность для перехвата информации.
Некоторые из перечисленных выше проблем могут быть решены посредством использования шифрованной связи с онлайновыми агентами доступа (proxies). Доступ к некоторым онлайновым программам (proxies) возможен на основе SSL (HTTPS) протоколов, которые шифруют связь между конечным пользователем и онлайновой системой обхода. В этом случае третья сторона может видеть связь пользователя с онлайновой системой обхода, но не получит доступа к контенту. Если использование технологий обхода фильтрации опасно, пользователи обязательно должны удостовериться, что они используют SSL протокол.

Несмотря на то, что связь пользователя с онлайновой системой обхода

онлайновым может быть надежно защищена, любая информация проходящая через систему, может быть перехвачена его владельцем. Таким образом, необходимо предпринять меры для того, чтобы владелец системы обхода не раскрывал информацию. В зависмости от места расположения системы или сервера, у властей может появиться возможность доступа к регистрационным записям (log files).

Пользователи должны понимать, что и при использовании SSL-протоколов, существуют определенные опасности. Например, пользователи могут привлечь внимание властей из-за использования криптографии, что считается незаконным в некоторых странах. Кроме того, власти могут определить, какие сайты пользователь посещает при помощи обходного модуля, используя такие технологии как атаки HTTP fingeprinting и Man-in the Middle (MITM) attacks. Тем не менее, страницы с динамическим контентом и ситемами обхода, которые добавляют ложный текст или изображение к запрашиваемому контенту могут свести риск от подобных атак до минимума. Если у пользователей есть "отпечатки пальцев", или цифровая подпись SSL-сертификата, они могут вручную проверить аутентичность сертификата, избежав риска MITM атаки (1).

PROXY-СЕРВЕРЫ



Proxy -сервер - это сервер, расположенный между клиентом (web-браузером) и web-сервером. Proxy-сервер действует как буфер между клиентом и сервером и может поддерживать различные запросы, включая web-трафик (HTTP), протокол передачи файлов (FTP) и зашифрованный трафик (SSL). Proxy-серверы используются отдельными людьми, учреждениями и государствами для разных целей, в том числе для обеспечения безопасности, анонимности, кэширования и фильтрации. Для того, чтобы использовать proxy-сервер, конечный пользователь должен произвести настройку конфигурации своего web-браузера в соответствии с IP-адресом или именем хоста proxy-сервера, а также номером порта, который использует proxy-сервер. Несмотря на простоту решения, иногда бывает невозможно настроить браузер в пунктах общественного интернет-доступа - библиотеках или интернет-кафе, на работе.

1. Подробнее о возможных атках на модули обхода - в статье Беннетта Хейзелтона (Bennett Haselton) List of possible weaknesses in systems to circumvent Internet censorship (http://peacefire.org/circumventor/list-of-possible-weaknesses.html)." и в ответе Поля Барановски (Paul Baranowski) http://www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

Преимущества:
Существует большой выбор программных пакетов, которые попозволяют прозрачно использовать различные типы трафика, а не только web-трафик (HTTP), и которые можно настроить для работы на нестандартных портах. Существует множество общедоступных proxy-серверов.
Недостатки:
Многие proxy-серверы не настроены на шифрование по умолчанию, поэтому трафик между пользователем и сервером не защищен.
Пользователь должен получить разрешение изменить необходимые настройки браузера, и если провайдер услуг интернет требует, чтобы трафик шел через его proxy-сервер, общедоступными серверами нельзя будет воспользоваться.
Использование общедоступных proxy-серверов может быть незаконным, поэтому такие серверы могут быть не всегда доступными для пользователя.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ PROXY-СЕРВЕРОВ

Программное обеспечение для proxy-серверов может быть установлено надежными людьми в странах, где интернет-контент не фильтруется. Эти люди должны обладать некоторыми техническими знаниями. Программное обеспечение proxy-серверов должно устанавливаться там, где возможна большая пропускная способность интернет-канала. Кроме того, должны использоваться технологии криптографии. Это особенно удобно в ситуациях, когда небольшая организация нуждается в технологиях обхода фильтрации интернет. После того как пользователи настроили свой браузер для работы через proxy-сервер, они могут осуществлять поиск информации в интернет. Не являясь самыми незаметными технологиями обхода, proxy-серверы все же более надежны, чем онлайновые proxy-системы. Они более удобны для доступа к сайтам, которые требуют аутентификации и паролей, например, к web-почте.
Proxy-сервреры также легко адаптировать к специфическим потребностям конечного пользования с учетом применяемых механизмов фильтрации.

• Squid - бесплатное программное обеспечение для proxy -серверов, может быть защищено при помощи сервера Stunnel.
http://www.squid-cache.org, http://www.stunnel.org
http://ice.citizenlab.org/projects/aardvark
• Privoxy имеет дополнительные возможности фильтрации для защиты конфиденциальности. http://www.privoxy.org
• Secure Shell (SSH) встроенный socks proxy ($ ssh -D port secure.host.com)
http://www.openssh.com
• HTTPport/HTTP хост позволяет обойти HTTP proxy, который блокирует интернет-доступ.

Частные proxy-серверы с опциями шифрования - лучшее решение для пользователей в офисах, когда необходим постоянный доступ к модулям обхода фильтрации. Такой сервер должен находиться за пределами страны, обеспечивать необходимую пропускную способность и поддерживаться надежными людьми, обладающими необходимыми техническими навыками.

ОБЩЕДОСТУПНЫЕ PROXY -СЕРВЕРЫ

Открытые proxy-серверы - это серверы, которые поддерживают контакты с удаленными компьютерами. Часто трудно определить создан ли такой сервер намеренно или просто неправильная конфигурация сервера позволяет осуществлять такую связь.

ПРЕДУПРЕЖДЕНИЕ: В соответствии с законодательством некоторых стран использование proxy-серверов может трактоваться как "несанкционированный доступ", а пользователи могут понести за это наказание. Мы рекомендуем не использовать открытые proxy-серверы.

Местонахождение открытых proxy-серверов

На многих вебсайтах можно увидеть списки открытых proxy -серверов, однако это не гарантирует, что перечисленные в них серверы функционируют. Нет также гарантий того, что эти списки точны, в особенности это касается уровня анонимности и географического расположения серверов. Помните, что вы пользуетесь этими серверами на свой страх и риск.

Список сайтов с открытыми proxy:

http://www.samair.ru/proxy/
http://www.antiproxy.com/
http://tools.rosinstrument.com/proxy/
http://www.multiproxy.org/
http://www.publicproxyservers.com/

Программное обеспечение: ProxyTools/LocalProxy

http://proxytools.sourceforge.net

Открытые proxy: нестандартные порты

Во многих странах, где осуществляется фильтрация интернет, блокируется доступ к стандартным портам proxy. "Порт" - это абстракция, используемая транспортным протоколом интернет для обозначения соединения. Различные интрнет-сервисы передают данные через определенные порты. Номера портов распределяются организацией Internet Assigned Numbers Authority (Центральный координатор по присвоению уникальных параметров протоколов интернет). Например, порт 80 зарезервирован для HTTP трафика. Когда браузер получает доступ к определенному сайту, вы на самом деле устанавливаете связь с портом 80. Proxy-серверы также имеют порты, приписанные им по умолчанию. Программы фильтрации могут блокировать доступ к этим портам. Поэтому для успешного обхода фильтрации необходим proxy, который настроен на работу через нестандартный порт.

http://www.web.freerk.com/proxylist.htm

PROXY-СЕРВЕРЫ: БЕЗОПАСНОСТЬ

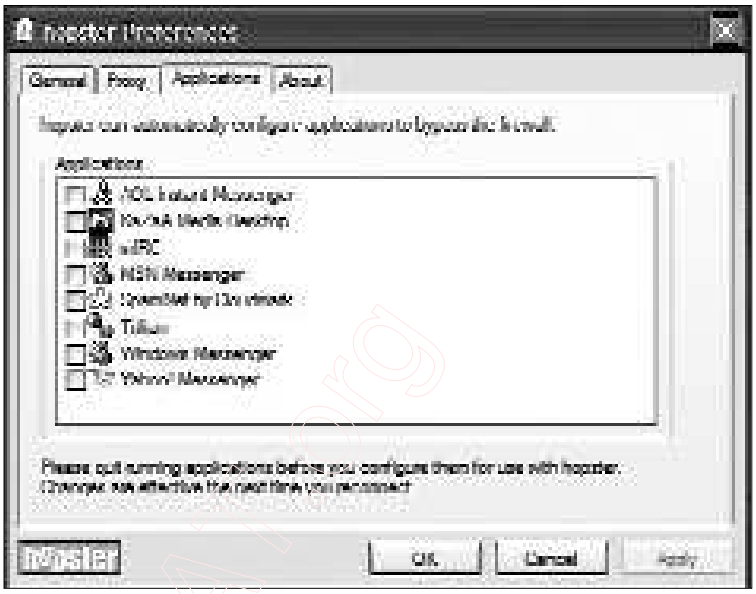
От конфигурации proxy-сервера зависит уровень анонимности соединения. Кроме того, что proxy-серверы не обеспечивают шифрование данных, они могут передавать информацию о конечном пользователе серверу, на который поступил запрос, что дает возможность установить IP -адрес компьютера, с которого поступил запрос. А поскольку связь между вами и proxy-сервером осуществляется в режиме открытого текста, контент легко перехватить. Информация же, проходящая через proxy-сервер, всегда может быть перехвачена его владельцем. Поэтому мы не рекомендуем использование общедоступных proxy-серверов. Открытые proxy-серверы часто используются из-за простоты доступа, однако они не обеспечивают необходимый уровень защиты, хотя и позволяют успешно обойти фильтрацию.

Как и онлайновые proxy, proxy-серверы не обеспечивают безопасность. Конечный пользователь может получать нежелательные скрипты и "cookies" . Кроме того, даже при использовании инструментов шифрования, proxy-серверы могут подвергнуться атакам MITM и HTTP fingertips. Необходимо также отметить, что при использовании некоторых браузеров возможна утечка информации при соединении с proxy-серверами, обеспечивающими не только web-трафик, но и другие типы трафика. При запросе какого-либо вебсайта, доменное имя переводится в IP-адрес. Некоторые браузеры выполняют эту операцию сами, т.е процесс не осуществляется через proxy. В этом случае запрос сайта с блокированным доменным именем выполняется серверами Системы доменных имен (Domain Name System, DNS) в стране, которая осуществляет фильтрацию (2).

2. Смотри сайт: http://tor.eff.org/cvs/tor/doc/CLIENTS

Мы не рекомендуем пользоваться открытыми общедоступными proxy-серверами. Такие серверы пригодны для периодического использования в странах, где это не влечет за собой серьезных последствий. Открытые proxy-серверы не следует использовать для передачи важной информации.

ТУННЕЛИРОВАНИЕ



Программное обеспечение для туннелирования

Туннелирование, или переадресация портов, позволяет инкапсулировать открытый, нешифрованный трафик при помощи протоколов шифрования. Пользователь, подвергаемый цензуре, должен загрузить клиентскую программу, которая создает тоннель к компьютеру, находящемуся вне пределов фильтрации. Пользователю доступны все обычные сервисы, однако он получает доступ к ним через шифрованный туннель, ведущий к безопасному компьютеру, который, в свою очередь, перенаправляет запросы и ответы на них. Существуют различные программы для туннелирования. Те, у кого есть связи с людьми в странах, не осуществляющих фильтрацию, могут использовать частные услуги. Те же, у кого таких контактов нет, могут подписаться на платные коммерческие услуги.

Бесплатные сервисы, как правило, используют рекламу. Рекламные запросы передаются открытым текстом (HTTP). Эти запросы могут быть перехвачены и третья сторона может узнать об использовании услуг переадресации. Кроме того, многие услуги туннелирования используют socks proxy, что может привести к утечке информации о запрашиваемых доменных именах.

http://www.http-tunnel.com/
http://www.hopster.com/
http://www.htthost.com/

Преимущества:

Переадресация портов обеспечивает шифрованную передачу данных.

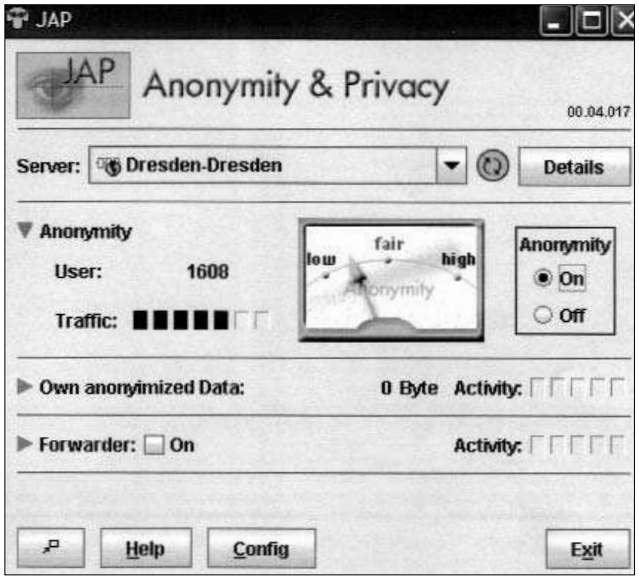
Приложения обычно могут использовать различные протоколы, а не только web-трафик.

Существуют коммерческие услуги, которыми можно пользоваться даже в странах, осуществляющих фильтрацию интернет.

Недостатки:
Коммерческие услуги переадресации портов могут быть известны, а потому также подвергаться фильтрации. Приложениями туннелирования невозможно пользоваться в пунктах общественного интернет-доступа (библиотеках, интернет-кафе и т.п.), где нельзя устанавливать свои программы. Использование таких приложений может требовать более глубоких технических знаний, чем другие методы обхода фильтрации.
Технологии переадресации портов наиболее удобны для пользователей, обладающих определенными техническими знаниями, которым нужны безопасные (но не анонимные) услуги обхода фильтрации, причем не только web-трафика. Услуги туннелирования, предоставляемые на коммерческой основе, могут быть отличным решением для пользователей, которые не имеют контактов в странах, где не осуществляется фильтрация.

АНОНИМНЫЕ КОММУНИКАЦИОННЫЕ СИСТЕМЫ

Технологии обхода и анонимные коммуникационные системы похожи и часто взаимодействуют, хотя предназначены для разных целей. Анонимные коммуникационные системы, прежде всего, обеспечивают конфиденциальность запрашивающего пользователя от провайдера контента. Кроме того, некоторые усовершенствованные системы используют разнообразные техники маршрутизации, чтобы обеспечить защиту от самой системы анонимных коммуникаций. Системы обхода интернет-фильтрации не всегда гарантируют анонимность пользователя. Они обеспечивают безопасные коммуникации для преодоления специфических запретов на отправку и получение сообщений. Для выполнения этой задачи требуются безопасные технологии связи, иногда некоторая "маскировка", но не обязательно анонимность.
Анонимные коммуникационные системы часто используют для обхода интернет-фильтров. Преимущество таких систем заключается в том, что имеется несколько сетей, войдя в одну из которых, можно обойти запреты на доступ к определенному контенту, сохраняя анонимность.



Использование анонимных коммуникационных систем для обхода фильтров требует установки соответствующего программного обеспечения. Те, кто имеет доступ в интернет через публичные терминалы, библиотеки или интернет-кафе, вероятнее всего, не смогут использовать такие системы. Кроме того, анонимные коммуникационные системы также могут замедлить скорость интернет-подключения.

Пользователи, стремящиеся обойти интернет-фильтрацию на национальном уровне или на уровне провайдера интернет-услуг, могут узнать, что власти принимают меры для блокировки анонимных коммуникационных систем. Если используемая система оперирует через статический порт, фильтрующие программы легко могут быть настроены на блокирование доступа к ней. Чем более известна анонимная коммуникационная система, тем больше риск того, что ее блокируют. Кроме того, для борьбы с системами, использующими одноранговые или общедоступные узлы, власти могут просто закрыть доступ к этим хостам. Власти могут также запустить собственный узел, чтобы проследить пользователей, пытающихся подключиться к нему.В некоторых странах, где установлены серьезные ограничения, трафик к известным системам прослеживается, и их использование таких систем может привлечь внимание к пользователю (3).

Преимущества:

Они обеспечивают как безопасность, так и анонимность.

Они могут обеспечивать безопасный доступ с использованием различных протоколов, не ограничиваясь web-трафиком.

Часто их поддерживают сообщества пользователей и разработчиков, которые могут обеспечить техническую помощь.

Недостатки:

Они не создаются исключительно для обхода, широко известны и могут подвергнуться фильтрации.

Их нельзя использовать в местах публичного доступа, где пользователи не могут устанавливать программное обеспечение, например, в интернет-кафе или в библиотеках.

• Tor - это сеть виртуальных туннелей, позволяющих повышать безопасность и более надежно обеспечивать конфиденциальность при использовании интернет. Tor также позволяет разработчикам программного обеспечения создавать новые инструменты коммуникаций со встроенными функциями безопасности. Tor обеспечивает основу для ряда приложений, позволяющих организациям и индивидуумам обмениваться информацией через общественные сети, не нарушая конфиденциальность. http://tor.eff.org

• JAP позволяет осуществлять интернет-поиск анонимно. Вместо подключения напрямую к web-серверу, пользователь осуществляет обход, используя шифрованное соединение через нескольких посредников, так называемых "mixes".
http://anon.inf.tu-dresden.de/index_en.html

• Freenet - бесплатное программное обеспечение, которое позволяет сообщать и получать информацию в интернет без боязни цензуры. оно полностью децентрализовано, так что и публикаторы, и потребители информации полностью анонимны.
http://freenet.sourceforge.net

3. Дополнительную информацию о системах обхода можно получить из статьи Беннетта Хейзелтона (Bennet Hazelton) "List of possible weaknesses in systems to circumvent Internet censorship"(http://peacefire.org/circumventor/list-of-possible-weaknesses.html) и ответ на нее Поля Барановски (Paul Baranowski): http://peacefire.org/circumventor/list-of-possible-weaknesses.html

Использование таких систем может потребовать довольно высокого уровня технической квалификации.
Анонимные коммуникации предназначены для технически грамотных пользователям, которым необходимы как технологии обхода фильтрации, так и анонимность при использовании различных протоколов, а не только web-трафика. Такие системы также невозможно использовать в общественных пунктах интернет-доступа.

ЗАКЛЮЧЕНИЕ

К выбору технологий обхода фильтров интернет необходимо отнестись со всей серьезностью, тщательно проанализировав специфические потребности, доступные ресурсы и требования безопасности конечного пользователя. Существует широкий спектр технологий, доступных пользователям, которые хотят избежать интернет-фильтрации. Однако, их успешное и стабильное использование зависит от ряда факторов, включая уровень технических умений пользователя, потенциальный риск безопасности и контакты за пределами страны. Правительства также могут принять ответные меры и блокировать сервисы и возможности обхода интернет-фильтрации.

Ключ к успешному и стабильному использованию систем обхода фильтрации - доверие и эффективность. Системы обхода должны учитывать конкретные обстоятельства и обеспечивать возможность адаптации для нужд конечного пользователя. Они должны быть безопасными, реконфигурируемыми и "замаскированными". Между провайдером услуг и конечным пользователем должны быть установлены отношения доверия. Необходимо также осознавать как специфику юридических и политических условий, в которых вынужден работать пользователь, так и ограничений технологий обхода.

Нарт Вилленёв - директор программы технических исследований Citizen Lab (Гражданская Лаборатория), центра междисциплинарных исследований Центре международных исследований (the Munk Centre for International Studies) Университета Торонто. В качестве разработчика программ и исследователя, сотрудничает с OpenNet Initiative (ONI), осуществляя мониторинг и документируя фильтрацию интернет в различных странах. Нарт Вилленёв также занимался сбором, анализом и разработкой технологий обхода интернет-фильтров. Кроме цензуры интернет, Нарт исследует такие феномены, как хактивизм, кибертерроризм и интернет-безопасность. Нарт Вилленёв недавно закончил обучение в рамках программы исследований мира и конфликта в Университете Торонто.

Нарт Вилленёв выражает особую благодарность Мишелю Левеск (Michelle Levesque), Дереку Бамбауэру (Derek Bambauer) и Беннетту Хэйзелтону (Bennett Haselton.