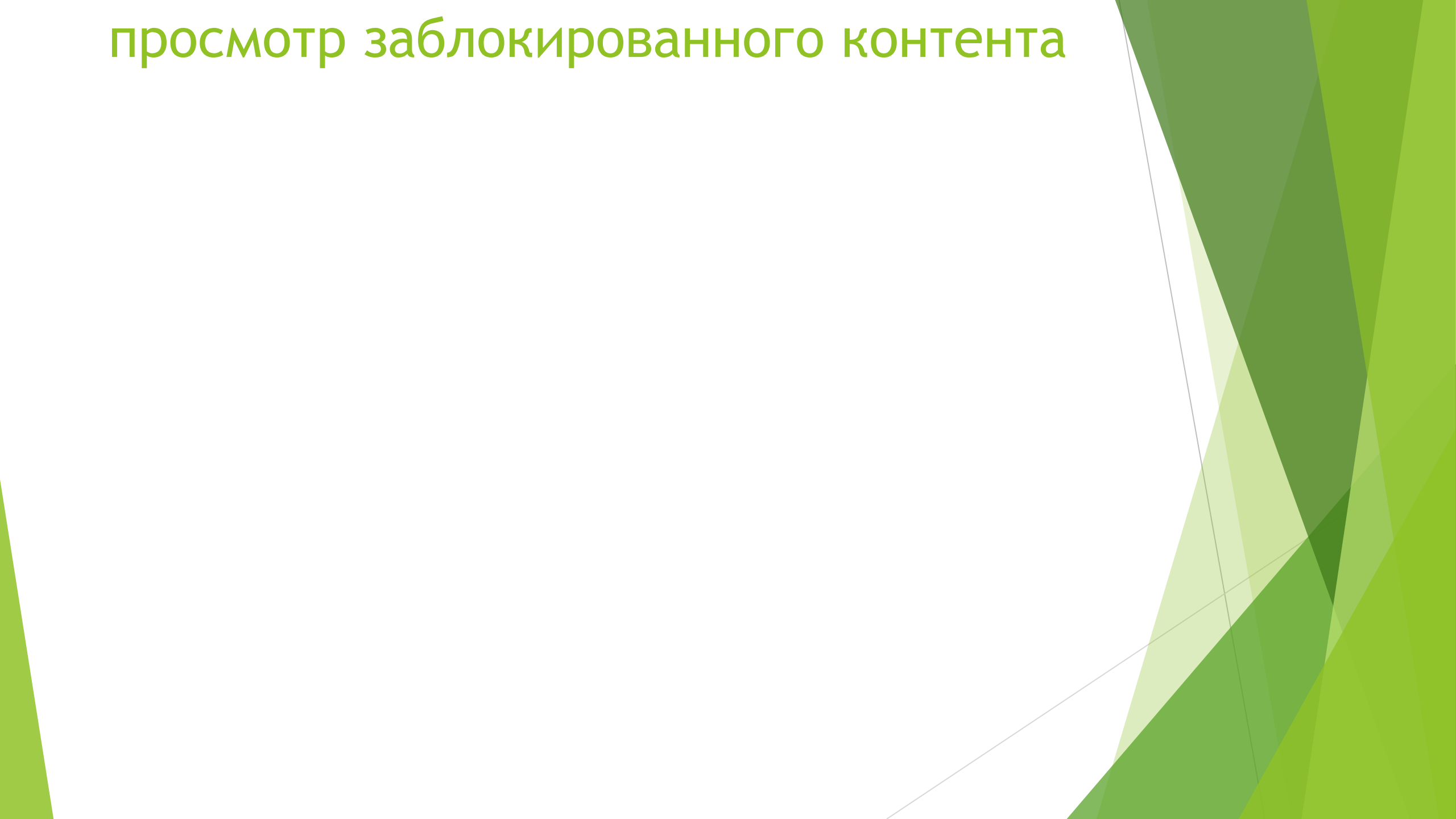


анонимность в сети интернет

- При существующем темпе развития информационных технологий и внедрения их в нашу жизнь особое место необходимо уделять вопросам безопасности. Безопасность использования технологий - это проблема, которую решают корпорации, использующие их. Однако личная безопасность - это персональный вопрос, каждый начинающий и опытный пользователь сможет выбрать для себя один или несколько из предложенных вариантов защиты, изучив их достоинства и недостатки, описанные в данной статье.



просмотр заблокированного контента



Средства обеспечения анонимности

Прокси -сервер

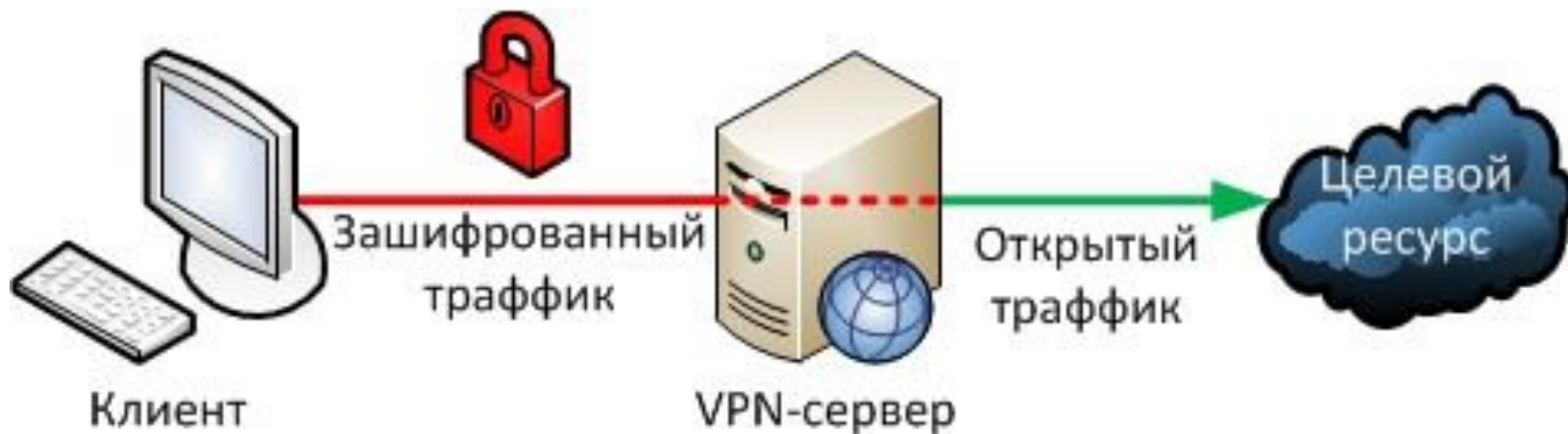
Прокси-сервер по своей сути это посредник между пользователем интернета (клиентом) и конечным адресом, к которому он (клиент) обращается. Прокси используются как для защиты локальной сети от внешнего доступа, а также выхода компьютеров из локальной сети в интернет, так и для анонимности в сети при доступе к определенным ресурсам. Прокси можно настроить так, чтобы локальный компьютер выходил в сеть только через прокси сервер. В таком случае внешние компьютеры будут видеть только прокси сервер.

Вот схема работы прокси-серверов.



VPN

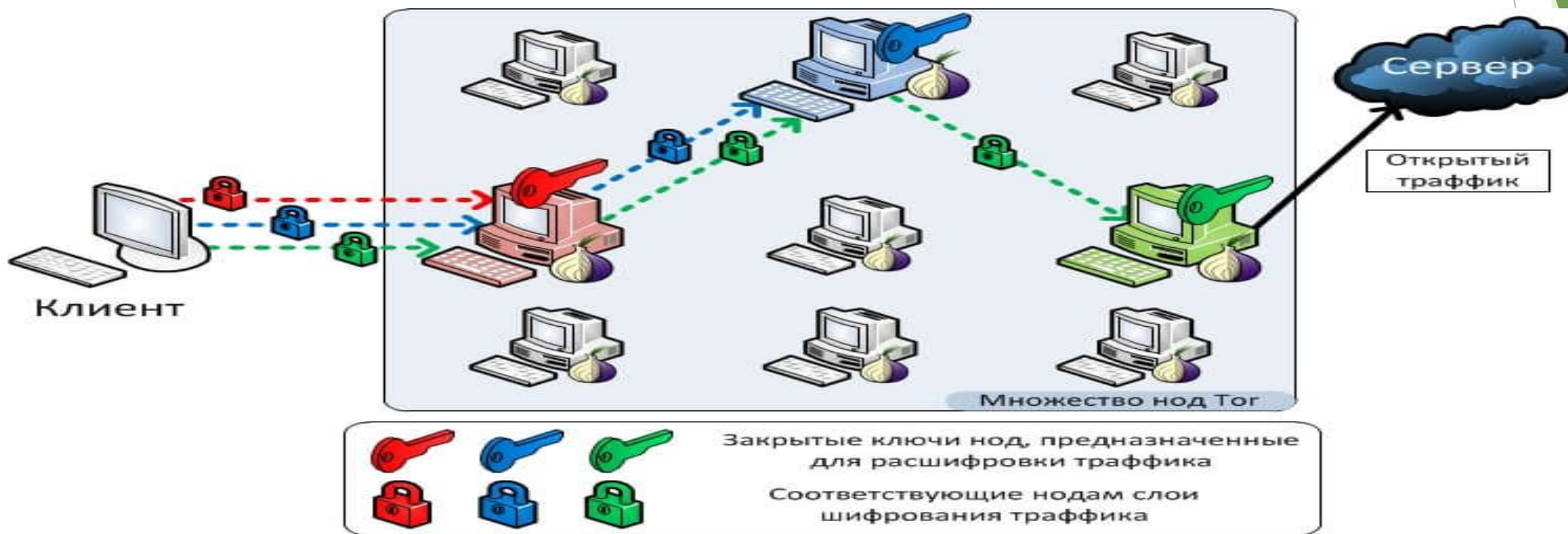
VPN в переводе с англ. Virtual Private Network — виртуальная частная сеть. VPN состоит из 2-х частей: внутренней (которая может состоять из нескольких сетей) и внешней, по которой происходит соединение. Схема работы VPN ниже.



На схеме видно, что трафик от клиента до VPN-сервера зашифрован, что является несомненным плюсом. Также плюс такого способа обеспечения анонимности в сети в простоте и удобстве, т.е. не нужно отдельно настраивать программы.

Анонимность в интернете. TOR

Tor — это система маршрутизаторов, устанавливающая анонимное соединение, которое защищено от прослушивания. Данная технология называется луковой. Ниже упрощенная схема работы TOR.



При соединении через TOR, клиент соединяется с интернетом по цепочке узлов. Обычно цепочка состоит из трех узлов. При этом ни один узел не знает про клиента и про конечный ресурс, к которому обращается клиент. При этом шифруется трафик отдельно для каждого узла.

Плюсы данной технологии:
высокая степень анонимности

Tails

Для обеспечения анонимности при исходящем соединении, соединение будет происходить через сеть TOR, при этом, все не анонимные соединения, которые проходят напрямую, будут заблокированы. При использовании Tails вы можете анонимно пользоваться интернетом, обходя цензуру или другие ограничения, обеспечивается приватность личных данных. Операционную систему Tails, в частности, использовал Эдвард Сноуден.

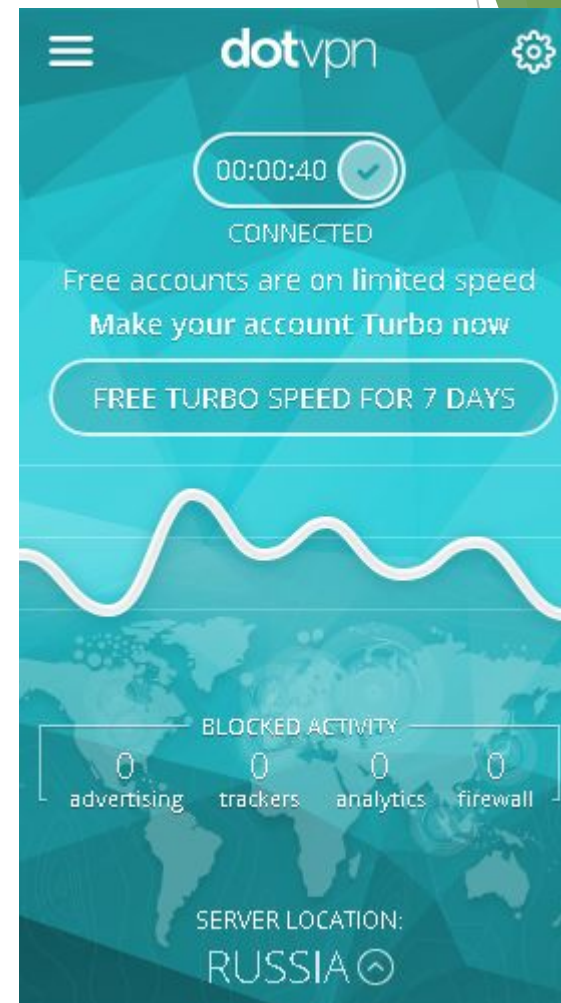
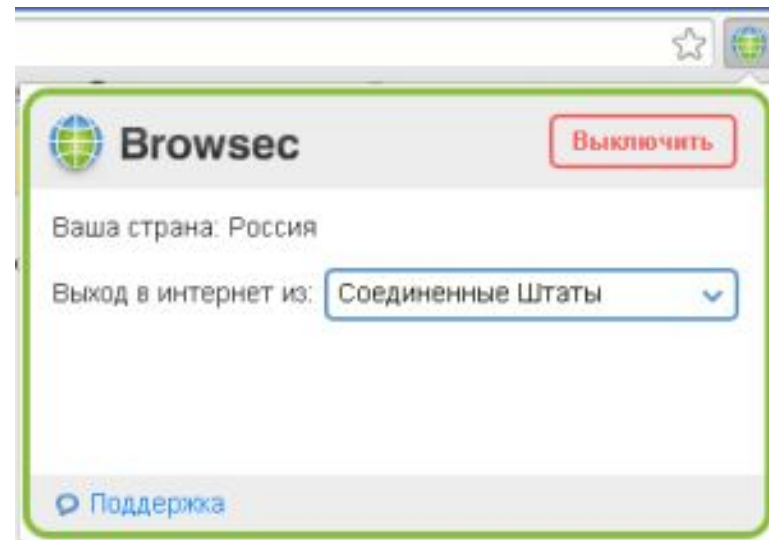
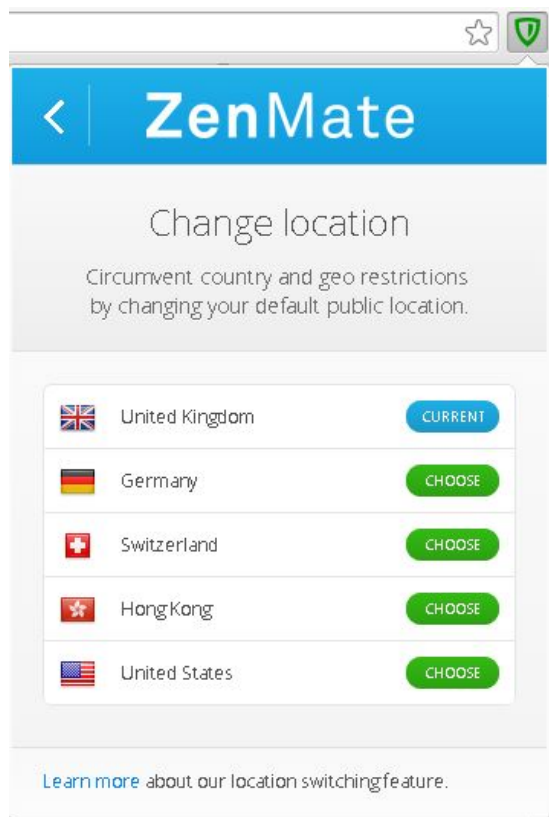


2IP

- ▶ I2P это сеть внутри сети, анонимная оверлейная сеть. Она предназначена для защиты передачи данных от внешнего наблюдения и надзора, например, от слежки провайдера.



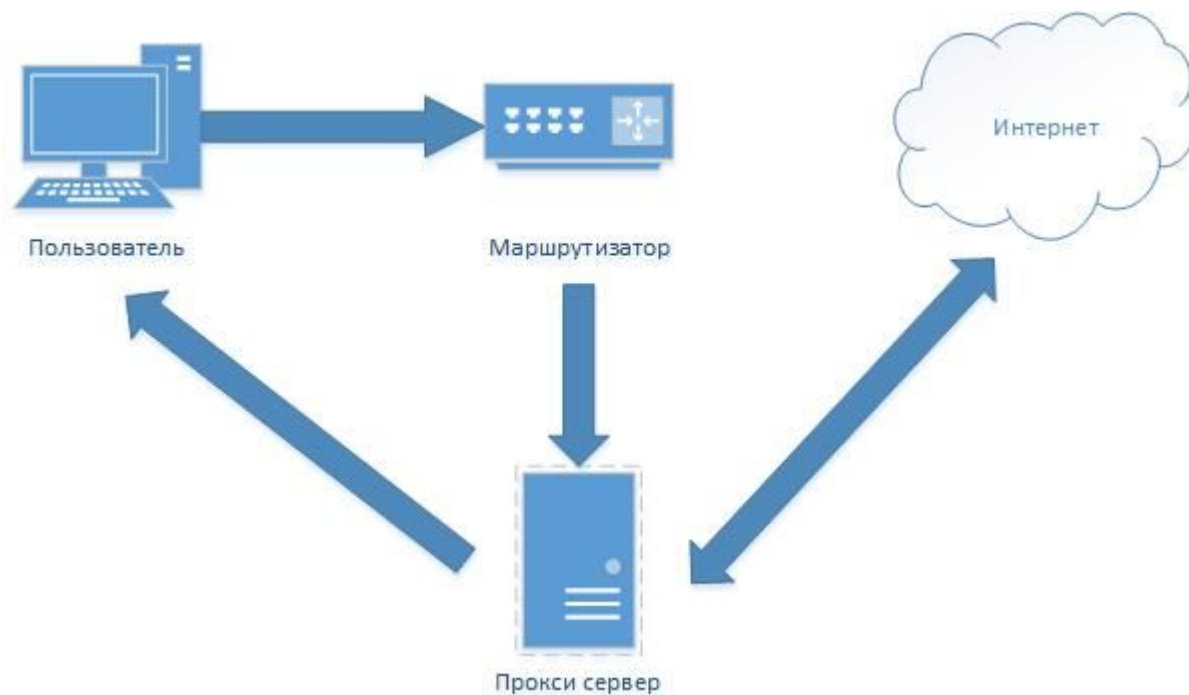
дополнения браузеров для обеспечения анонимности



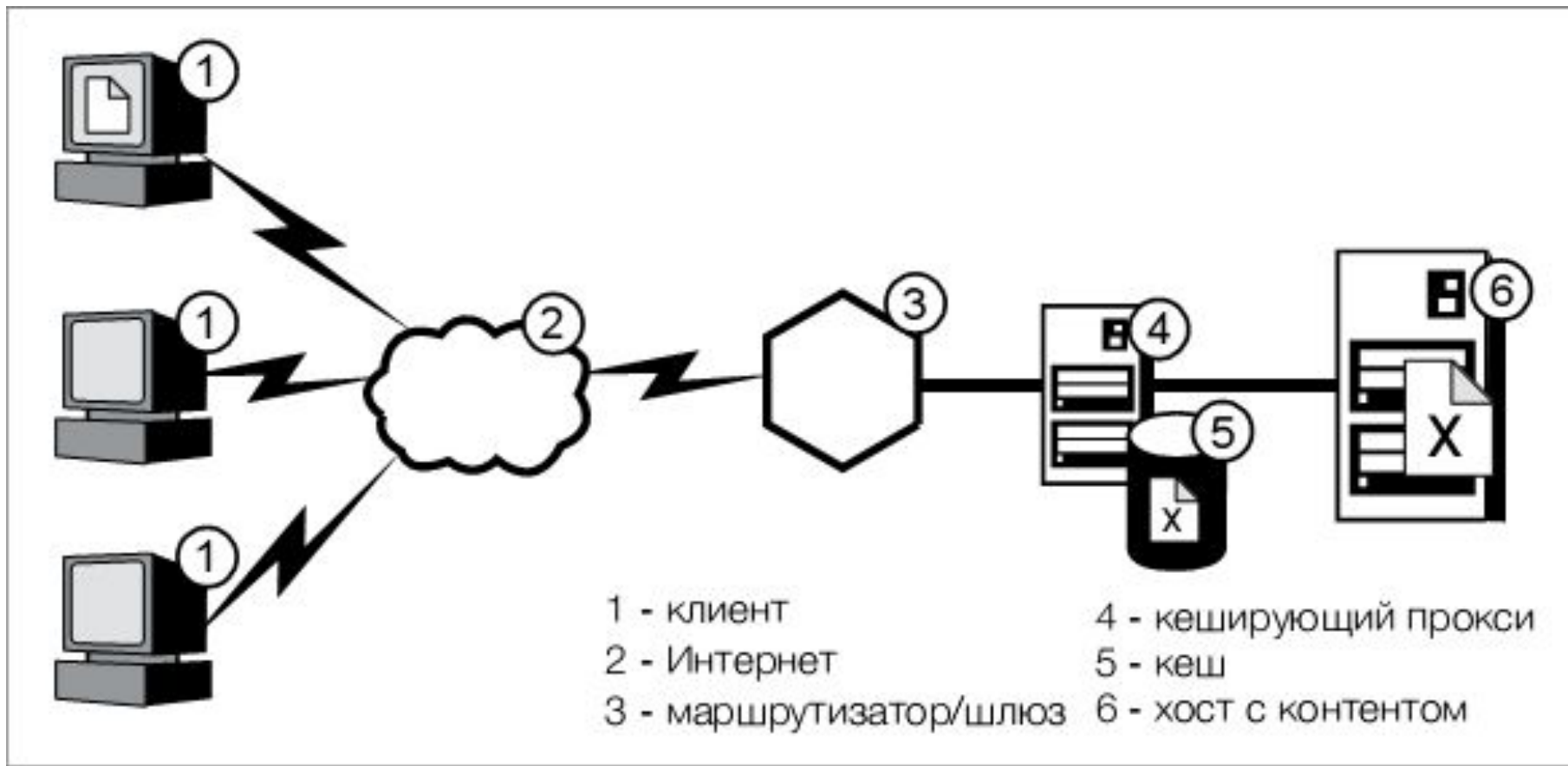
Прокси-сервер

Виды прокси-серверов

- ▶ **Прозрачный прокси** — схема связи, при которой трафик, или его часть, перенаправляется на прокси-сервер неявно (средствами маршрутизатора). При этом клиент может использовать все преимущества прокси-сервера без дополнительных настроек браузера (или другого приложения для работы с интернетом). Пример: `route -p add 10.32.5.5 mask 255.255.255.255 10.32.1.14`



Обратный прокси — прокси-сервер, который в отличие от прямого, ретранслирует запросы клиентов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети. Часто используется для балансировки сетевой нагрузки между несколькими веб-серверами и повышения их безопасности, играя при этом роль межсетевого экрана на прикладном уровне.



Технические подробности

Клиентский компьютер имеет настройку (конкретной программы или операционной системы), в соответствии с которой все сетевые соединения по некоторому протоколу совершаются не на IP-адрес сервера (ресурса), выделяемый из DNS-имени ресурса, или напрямую заданный, а на ip-адрес (и другой порт) прокси-сервера.

Прокси-серверы являются самым популярным способом выхода в Интернет из локальных сетей предприятий и организаций. Этому способствуют следующие обстоятельства:

- Основной используемый в интернете протокол — HTTP, в стандарте которого описана поддержка работы через прокси;
- Поддержка прокси большинством браузеров и операционных систем;
- Контроль доступа и учёт трафика по пользователям;
- Фильтрация трафика (интеграция прокси с антивирусами);
- Прокси-сервер — может работать с минимальными правами на любой ОС с поддержкой сети (стека TCP/IP);
- Многие приложения, использующие собственные специализированные протоколы, могут использовать HTTP как альтернативный транспорт или **SOCKS**-прокси как универсальный прокси, подходящий для практически любого протокола;
- Отсутствие доступа в Интернет по другим (нестандартным) протоколам может повысить безопасность в корпоративной сети.

Наиболее распространённые прокси-серверы

3 proxy

Зproxy (BSD, многоплатформенный)
CoolProxy (проприетарный, Windows)
Eserv (shareware, Windows)
HandyCache (shareware, Windows) бесплатен для домашнего использования
Kerio Control (проприетарный, Windows, Linux)
Microsoft Forefront Threat Management Gateway, ранее Microsoft ISA Server (proprietary, Windows)
Blue Coat Proxy SG (аппаратный/виртуальный appliance)
nginx (веб-сервер, имеющий режим работы в качестве reverse проху и часто для этого использующийся)
Squid (GPL, многоплатформенный)
Traffic Inspector (проприетарный, Windows)
UserGate (проприетарный, Windows)
Интернет Контроль Сервер (shareware, FreeBSD)
TOR (BSD, многоплатформенный)
Ideco ICS (проприетарный, Linux)
WinGate (проприетарный, Windows)
Cntlm (с авторизацией)

