Будет сложно, но найдут:

Как работает Луковая маршрутизация

Идея

Обеспечение свободы в Сети.

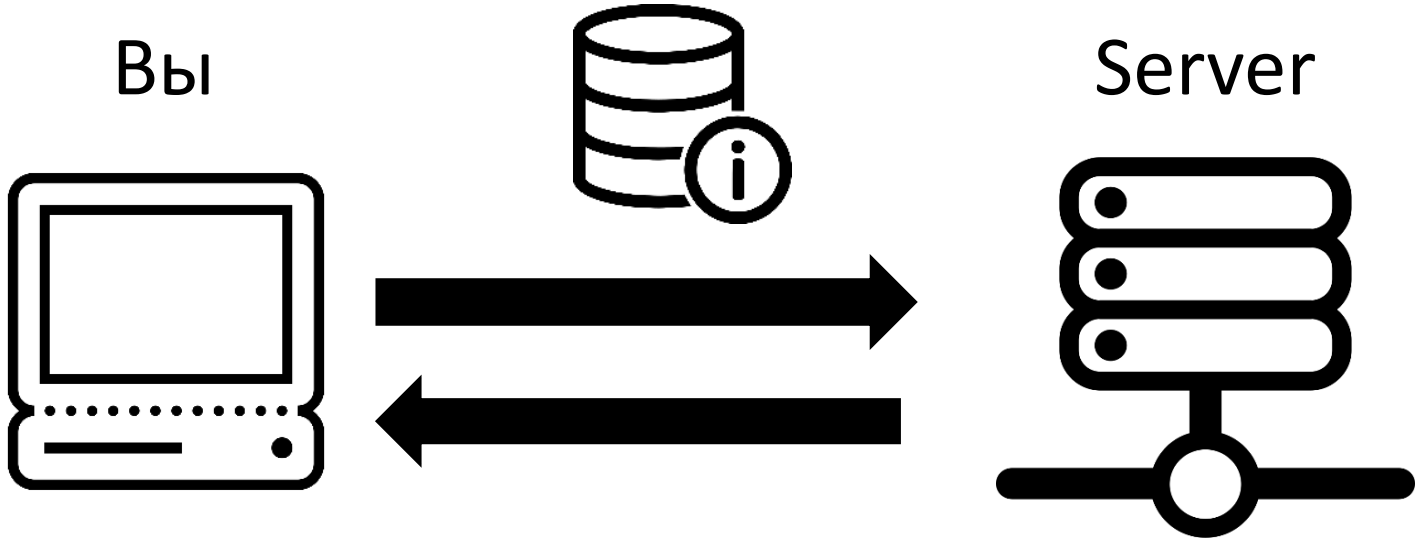
Обеспечение анонимности – обеспечение доступа.

«Обычный» интернет.

- Идентификация личности в Сети.
- Ограничение доступа к ресурсам.

«Обычный» интернет.

Проблема:
Потеря анонимности.



«Обычный» интернет.

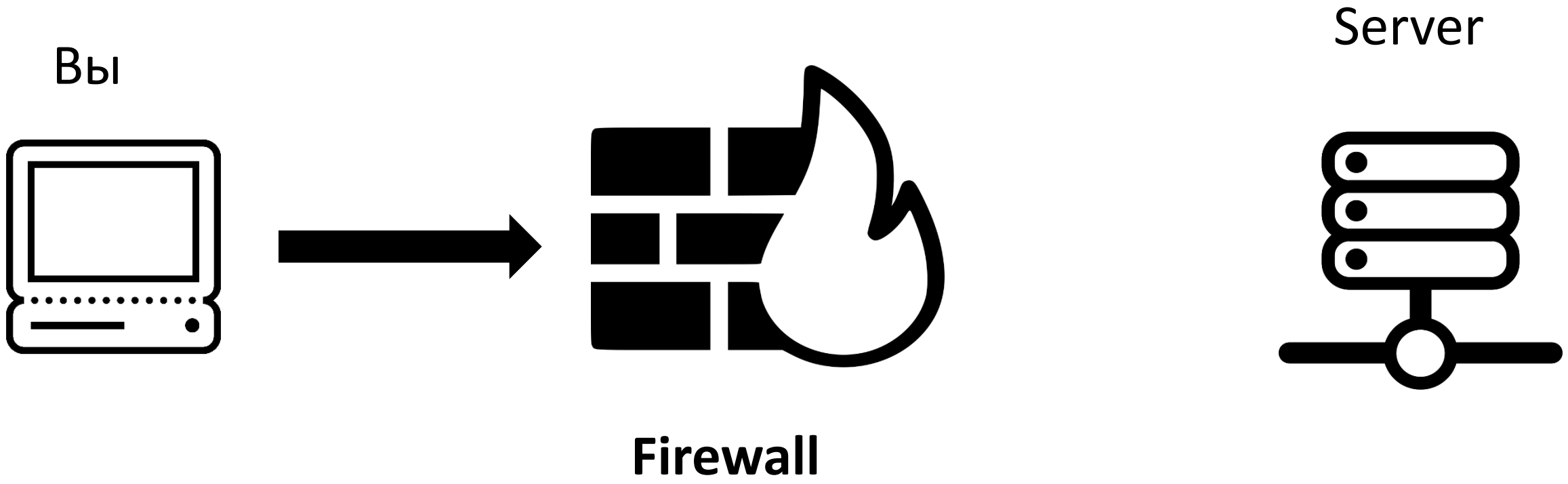
Проблема:
Блокировка доступа к ресурсам.

Server

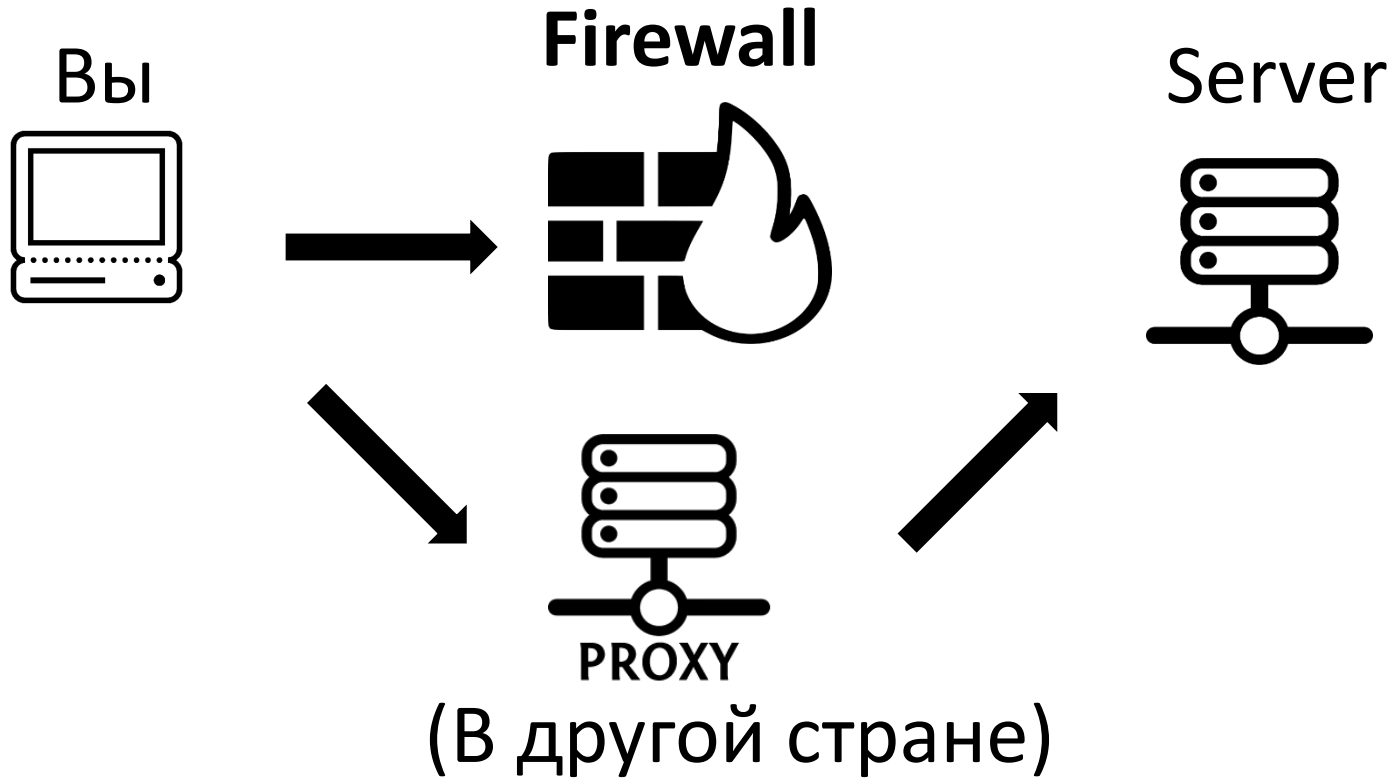
Вы

«Обычный» интернет.

Проблема:
Блокировка доступа к ресурсам.

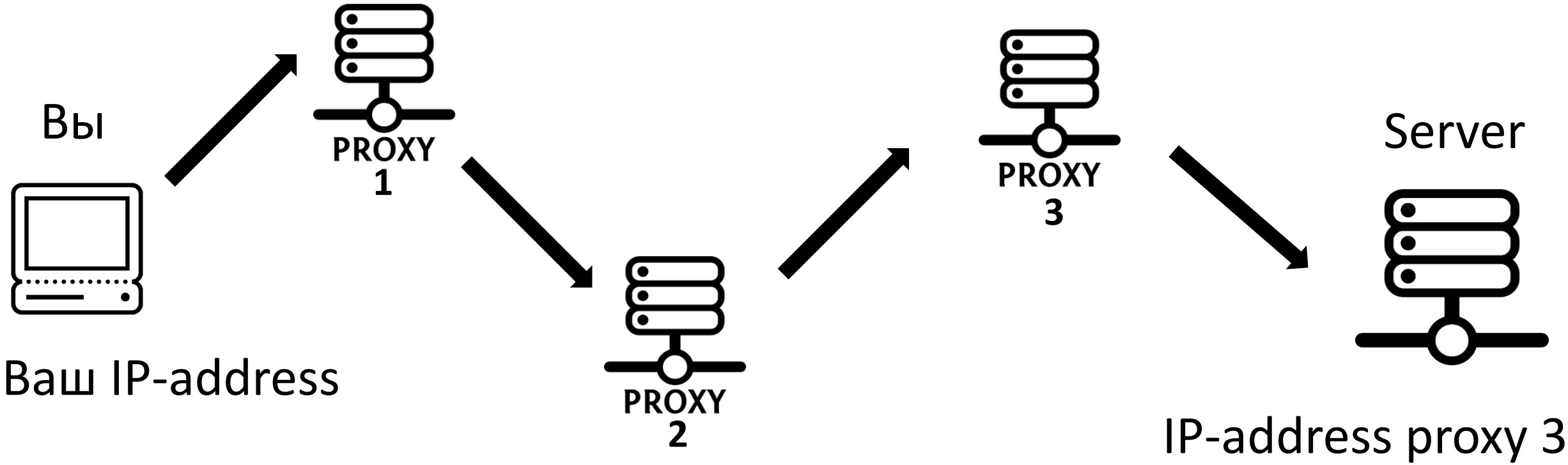


Почти «Обычный» интернет.



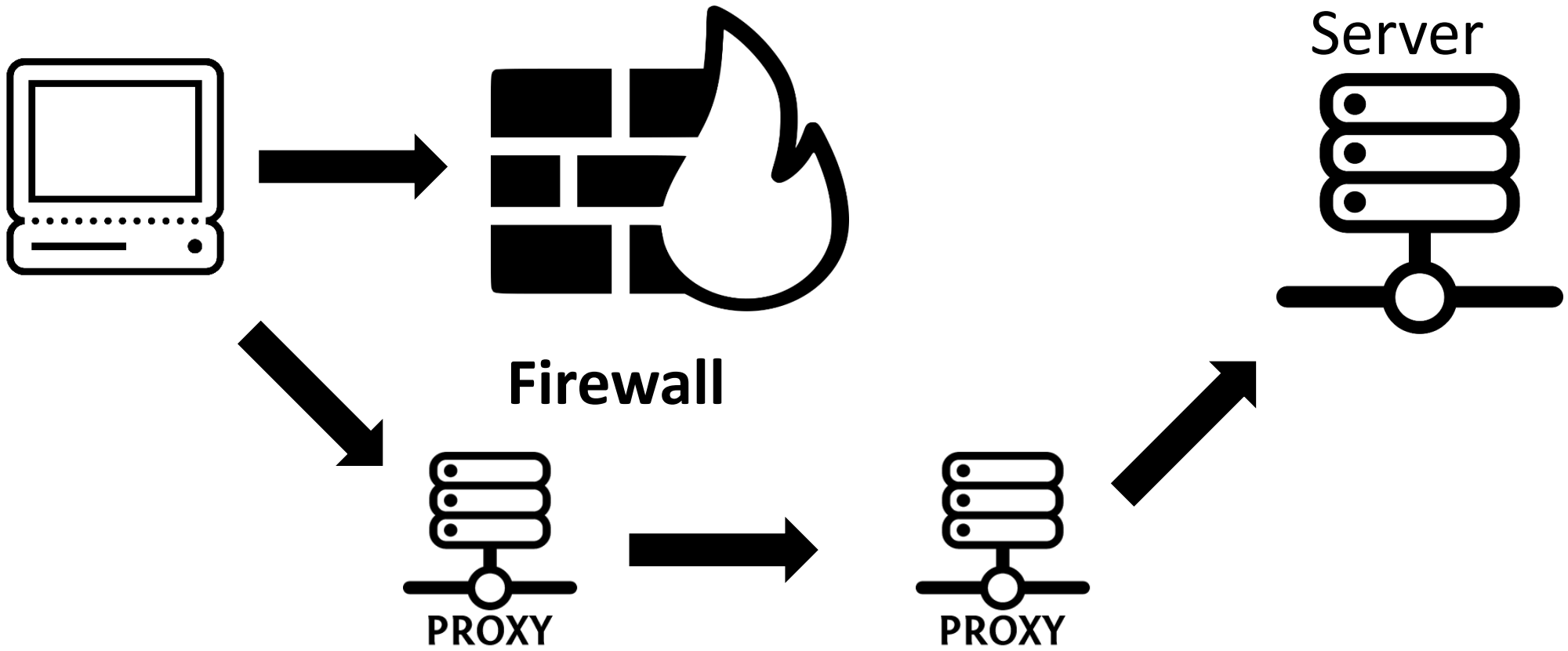
Принцип луковой маршрутизации.

Анонимность.



Принцип луковой маршрутизации.

Доступ к ресурсам.



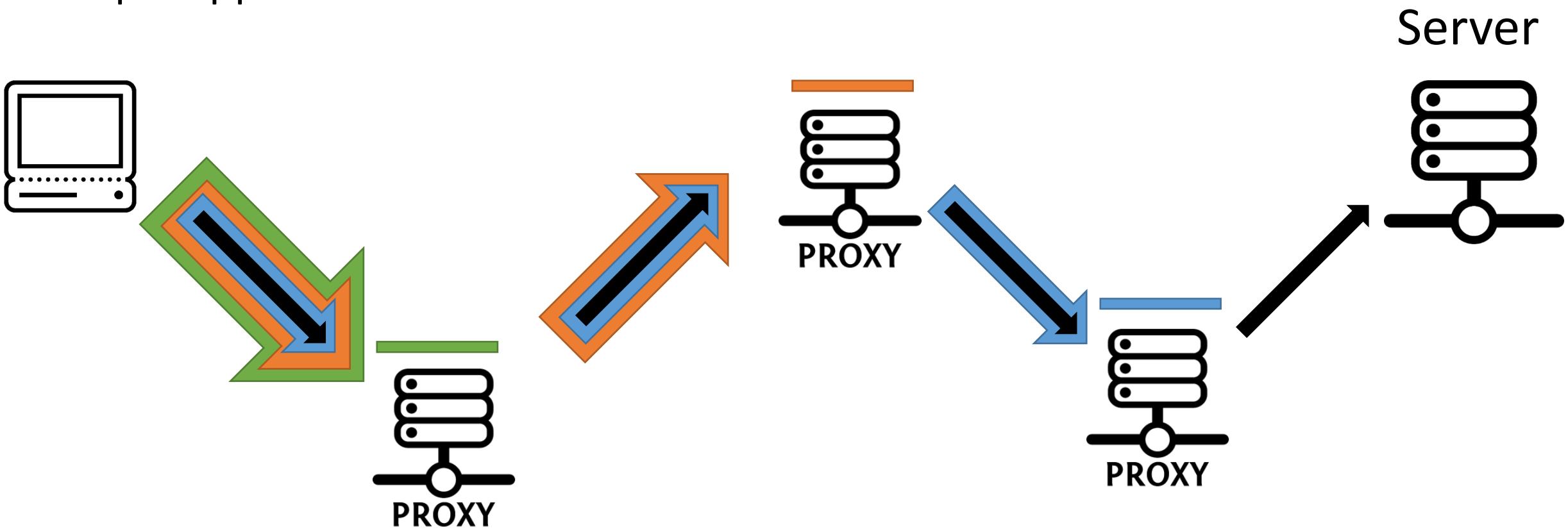
Принцип луковой маршрутизации.

Защита данных.

1-ый слой шифрования

2-ой слой шифрования

3-ий слой шифрования



Принцип луковой маршрутизации.

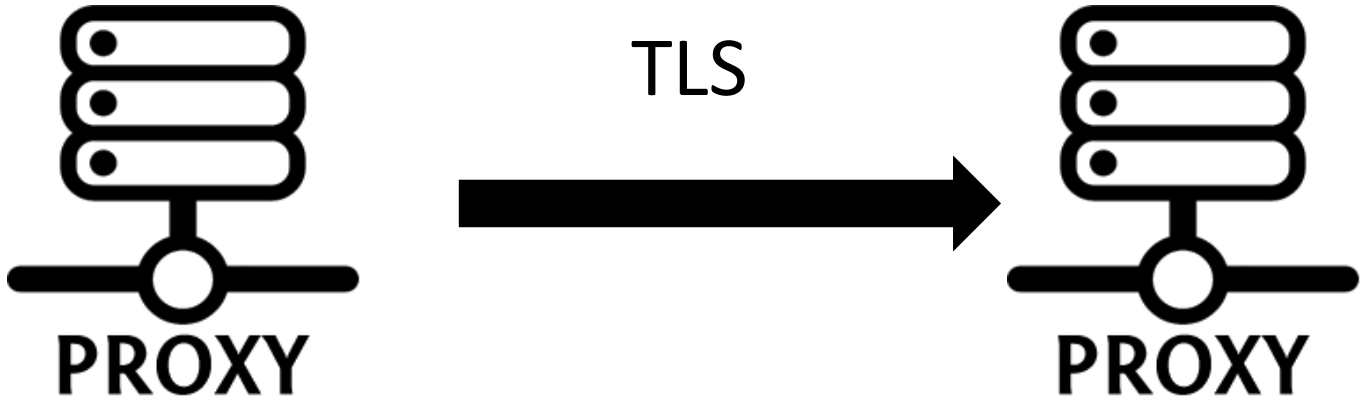
Защита данных.
Протоколы передачи и шифрование.

- TLS.
- Собственное луковичное шифрование

Принцип луковой маршрутизации.

Защита данных.
Протоколы передачи и шифрование.

TLS – используется между клиентом и маршрутизатором и самими маршрутизаторами.



Ассиметричное шифрование.

$$A = g^a \bmod p$$

Протокол Диффи – Хеллмана

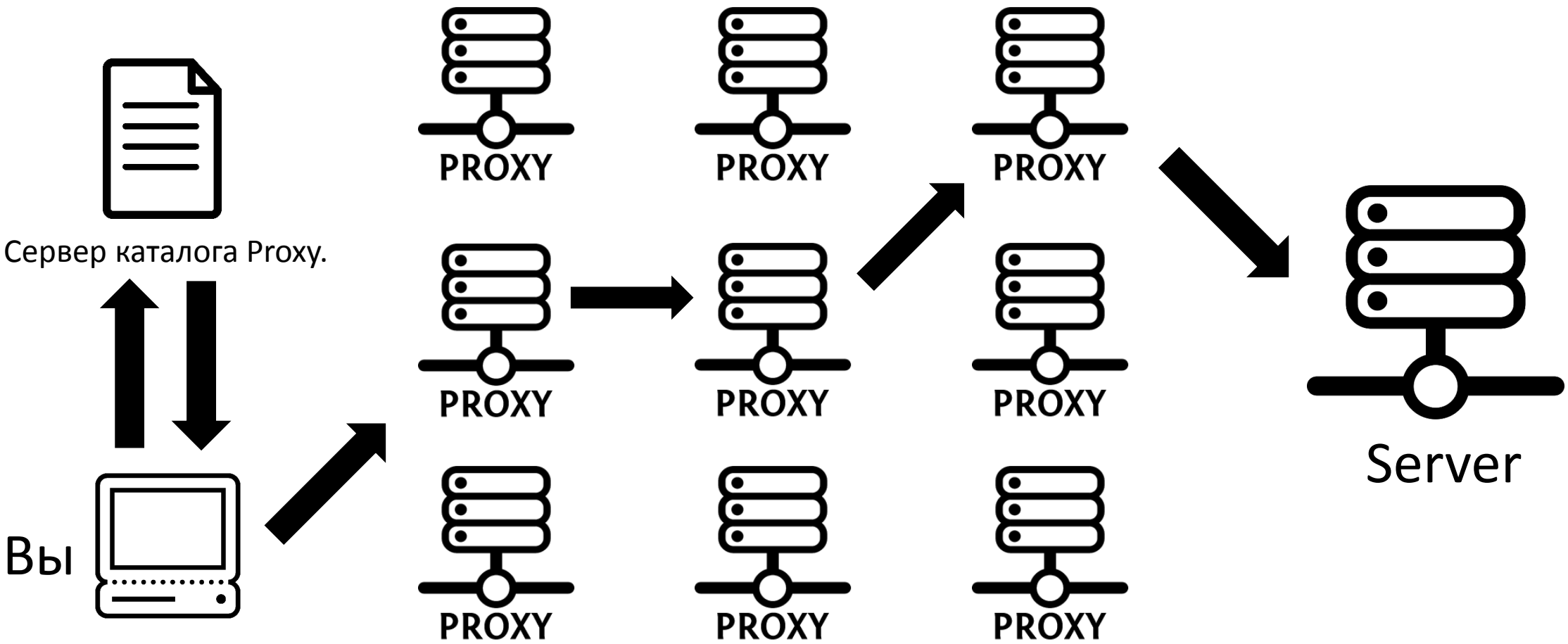
Где g и p - известные числа

Основа протокола Диффи – Хеллмана – односторонняя функция, преобразование аргумента которой очень просто, но его вычисление по значению функции крайне затруднено.

a = ?

Принцип луковой маршрутизации.

Формирование цепи маршрутизаторов.



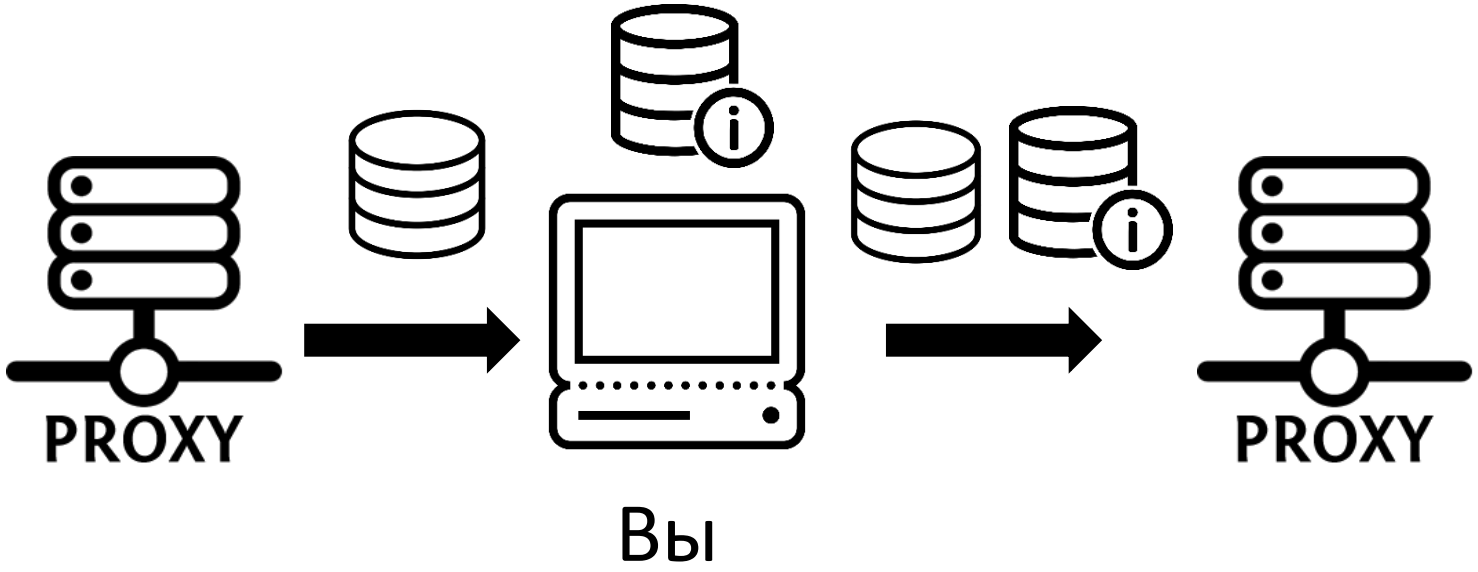
Принцип луковой маршрутизации.

Мосты. Обход обширной блокировки Tor.

- Адреса не хранятся на сервере каталога.
- Распространяются через электронную почту, веб-сервисы и иными путями.

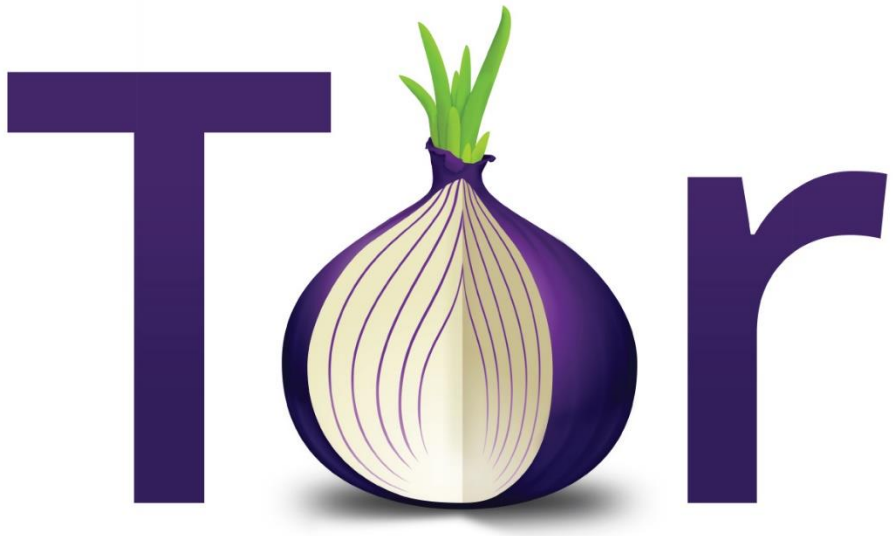
Чесночная маршрутизация.

Передача пакета сообщений от разных клиентов через один канал связи.



Область применения луковой маршрутизации.

- Тестирование информационных технологий
- Политическая организация полулегального и нелегального характера (в том числе борьба с цензурой)
- Бизнес
- Деятельность криминогенных элементов
- Обход блокировок в целях личного пользования (не для извлечения прибыли)
- Безопасная передача данных



Будет сложно, но..
Найдут?

Борьба правоохранительных органов и силовых структур с Tor.

Пассивные атаки.

Наблюдение за трафиком.

- Сопоставление по времени передачи сообщения.
- Сопоставление по объему данных.

Активные атаки

Компрометация ключей.

DDoS атака на маршрутизатор.

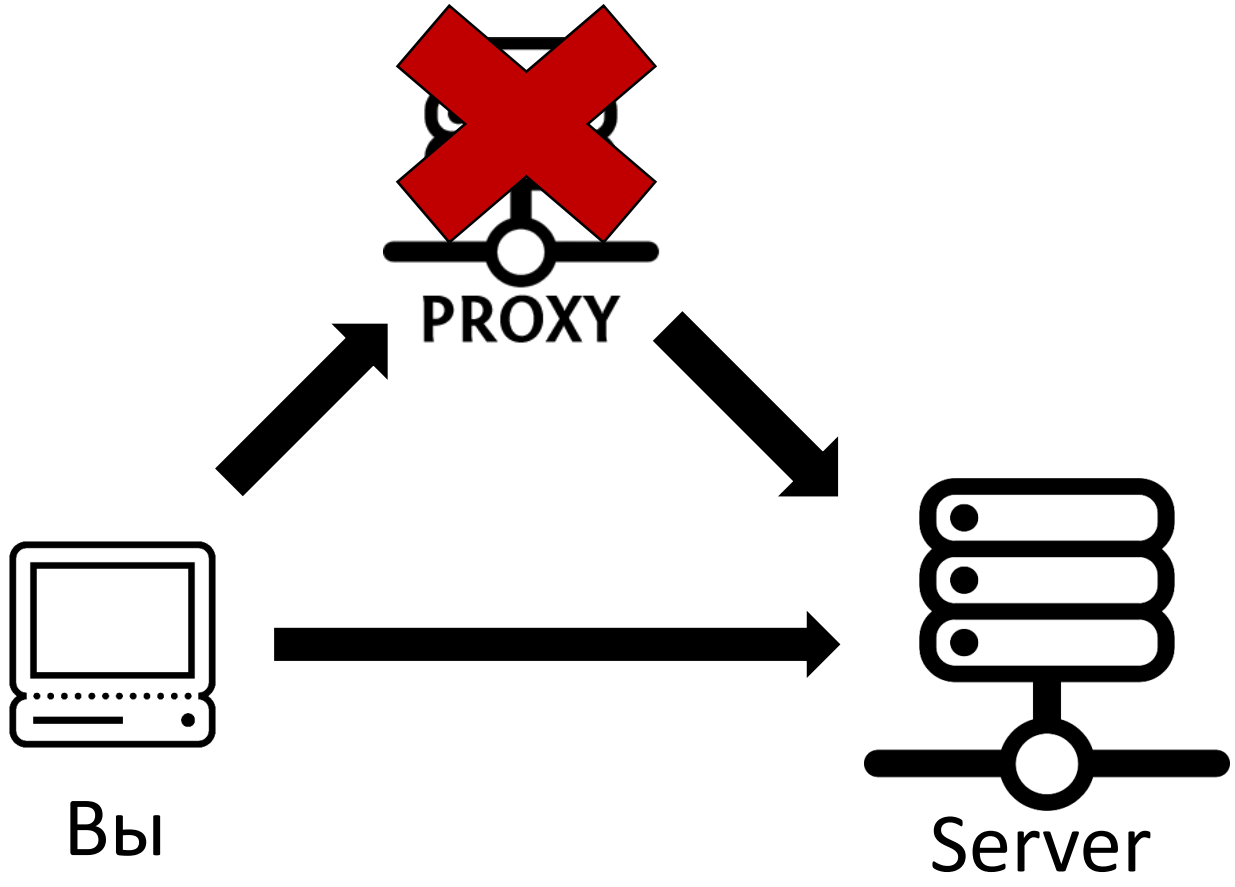
Введение «своих» маршрутизаторов в сеть.

Пометка данных.

Атака на каталоги.

Активные атаки

Размещение на сайтах вредоносного кода, который посредством перегрузки цепи заставляет клиент создавать прямое подключение.



Громкие луковые дела.

Дисклеймер.

Последующая информация несет исключительно ознакомительный характер. Автор доклада не одобряет распространение и употребление наркотических веществ, размещение запрещенного контента, пропаганду экстремизма.

P.S. Надеюсь она не шокирует вас и не сломает ваше представление о мире

Громкие луковые дела.

Дело Дмитрия Богатова

Был задержан 10 апреля 2017 года, за экстремистские высказывания. Которых он по итогам расследования не делал.

Дмитрий Богатов

Громкие луковые дела.

Дело о Silk Road

Создатель крупнейшего онлайн-ресурса по обороту наркотических веществ прокололся (по официальной версии) на таможне. В то время как его сайт так и остался неприступен.

Росс Уильям **Ульбрихт**

Громкие луковые дела.

Арест Эрика Маркеса. «Крупнейший на планете поставщик детской порнографии» попался ФБР.

Эрик Маркес

Анонимность под вашу ответственность.

Использование луковой маршрутизации и Tor в частности открывает вам огромные возможности. Но возможности не приходят одни. Будьте готовы к последствиям ваших действий в сети.

Следи за собой и будь осторожен.