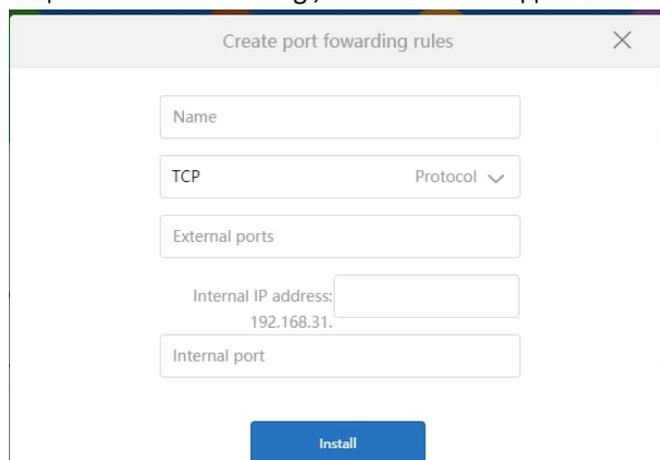


Для подключения к API Incogniton необходимо выполнить несколько манипуляций на вашем роутере и компьютере. А именно пробросить порт на роутере и открыть порт на компьютере. Давайте по порядку.

1. Проброс порта на Роутере (если у вас вдс, то переходите к п.2)

Самое простое это посмотреть вашу модель роутера и в поисковике найти полную инструкцию «как пробросить порты именно в вашей модели роутера». Нам нужно пробросить 35000 порт. Именно этот порт используется для работы с API Incogniton

1. Заходим в роутер (обычно <http://ip> адрес роутера , логин\пасс по умолчанию admin\admin
2. Ищем меню Forwarding , там нажимаем добавить правило (Add rule)



3. Имя указываем любое, протокол TCP, Порты 35000 и указываем внутренний адрес компьютера (именно внутренний 192.168.x.x.)
4. На этом настройка роутера окончена.

2. Теперь нам нужно открыть порт на компьютере.

1. Переходим в режим командной строки (вызывается из меню выполнить – командой cmd)
2. После перехода в режим cmd, набрать там powershell
3. Далее вводим вот такой скрипт:

```
New-NetFirewallRule -Name Allow35000 -DisplayName 'Allow 35000' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -Profile ANY -LocalPort 35000 -RemoteAddress 46.232.71.88
```

Должна появиться такая надпись:

```
Администратор: Командная строка - powershell
Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)
PS C:\Users\User> New-NetFirewallRule -Name Allow35000 -DisplayName 'Allow 35000' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -Profile ANY -LocalPort 35000 -RemoteAddress 193.124.186.255

Name                : Allow35000
DisplayName          : Allow 35000
Description         :
DisplayGroup        :
Group               :
Enabled             : True
Profile             : Any
Platform            : {}
Direction          : Inbound
Action              : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping  : False
LocalOnlyMapping    : False
Owner               :
PrimaryStatus       : OK
Status              : Правило было успешно проанализировано из хранилища. (65536)
EnforcementStatus  : NotApplicable
PolicyStoreSource   : PersistentStore
PolicyStoreSourceType : Local

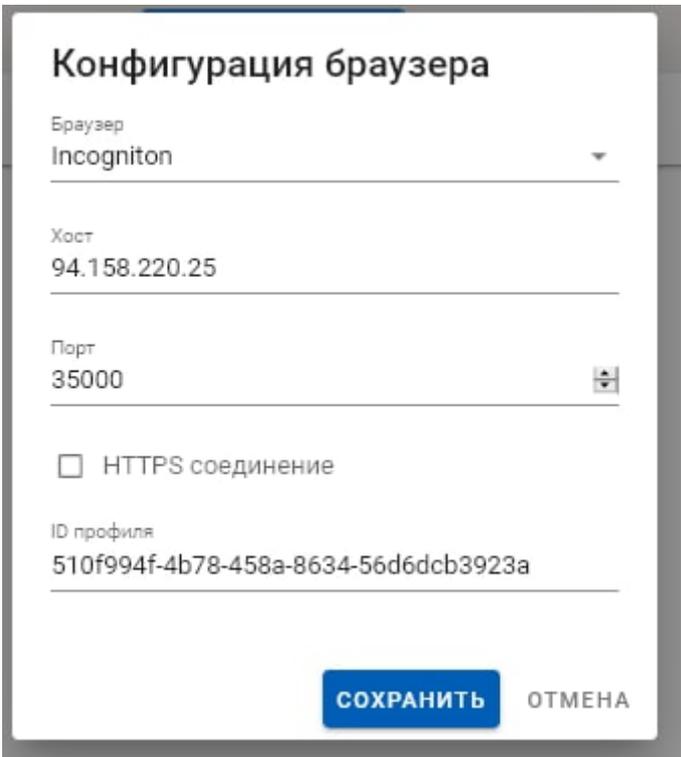
PS C:\Users\User>
```

На этом настройка проброса портов завершена.

ВАЖНО! У вас должен быть постоянный ип адрес. Возможно вам придется заказать эту опцию у вашего провайдера.

Настройка конфигурации API Incogniton

В каждой строчке расширения заполните конфигурацию для конкретного профиля, где:



Конфигурация браузера

Браузер
Incogniton

Хост
94.158.220.25

Порт
35000

HTTPS соединение

ID профиля
510f994f-4b78-458a-8634-56d6dcb3923a

СОХРАНИТЬ ОТМЕНА

Хост – это ваш внешний ип адрес (его можно посмотреть на сайте 2ip.ru)

ID профиля – это ид профиля инкогнитона

The screenshot shows the Windows Settings application, specifically the 'Profiles' section. On the left is a dark navigation pane with options like 'Главная страница', 'Новый профиль браузера', 'Автоматическое создание профилей', 'Свой аккаунт', 'Помощь и поддержка', 'Группы', and 'Назначено (20)'. The main content area has two tabs: 'Список профилей' (selected) and 'Группы'. Below the tabs is a search bar 'Поиск профилей...' and a table of profiles. The table has columns for 'Имя', 'Прокси-сервер', 'Статус', and 'Группа'. One profile is listed with a checkmark icon and the name 'Unassi'. Below the table, the 'Profile ID' is displayed as 'c171c4c8-01b9-415d-bcc5-7bbb195858b0', which is highlighted with a red box. A 'Копировать' button is next to it. Below the ID is a 'Примечания' section with a text input field containing 'Добавить примечания...' and a 'Сохранить примечания' button.

После этого ваши профили будут запускаться и закрываться автоматически.