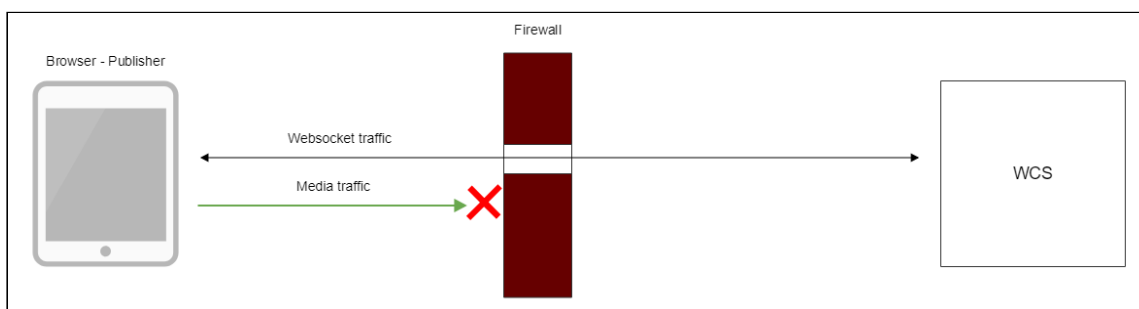


TURN server

Описание

TURN сервер используется для установки WebRTC соединения и передачи медиатрафика, если брандмауэр блокирует обмен по UDP между клиентом и сервером



Возможны следующие варианты использования TURN сервера совместно с WCS-сервером:

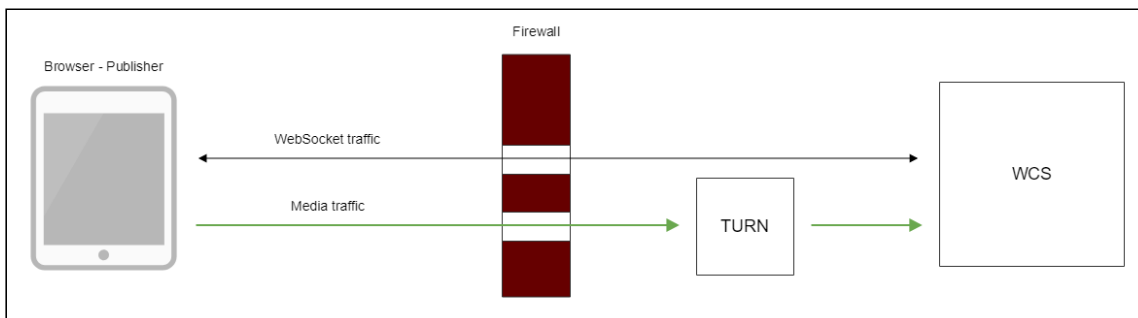
1. Использование внешнего TURN сервера. Данный вариант подходит корпоративным пользователям с развитой инфраструктурой, а также пользователям, предпочитающим разделять выполняемые задачи по серверам.
2. Использование внутреннего TURN сервера, встроенного в WCS. Данный вариант подходит малым предприятиям и пользователям, предпочитающим решения "из коробки".

Поддерживаемые платформы и браузеры

	Chrome	Firefox	Safari	Chromium Edge
Windows	✓	✗	✗	✓
Mac OS	✓	✗	✓	✓
Android	✓	✗	✗	✓
iOS	✓	✗	✓	✓

Использование внешнего TURN-сервера

При использовании внешнего TURN сервера трафик через доступные TCP-порты проходит следующим образом:



Установка и настройка TURN-сервера на CentOS 7

1. Скачайте и установите [turnserver](#)

Для компиляции из исходных текстов можно воспользоваться следующим [руководством](#)

2. Создайте файл конфигурации `turnserver.conf`

Пример конфигурационного файла `turnserver.conf.default` находится в директории `/usr/local/etc`. Можно переименовать его в `turnserver.conf` или создать новый файл

Ниже приведен пример минимального конфигурационного файла:

```
fingerprint
lt-cred-mech
user=username1:password1
realm=flashphoner.com
cert=/usr/local/etc/turn_server_cert.pem
pkey=/usr/local/etc/turn_server_pkey.pem
pkey-pwd=qweasd
```

3. Как видно из этого примера, для работы TURN-сервера необходимы сертификат и приватный ключ

Если TURN-сервер установлен на том же сервере, что WCS-сервер, то можно воспользоваться сертификатами WCS-сервера.

Если TURN-сервер установлен на другом сервере, то можно воспользоваться `openssl`, чтобы сгенерировать сертификат и приватный ключ:

```
openssl req -x509 -newkey rsa:4096 -keyout
/usr/local/etc/turn_server_pkey.pem -out
usr/local/etc/turn_server_cert.pem -days 365
```

4. **ОБЯЗАТЕЛЬНО:** В конфигурационном файле TURN-сервера должна быть включена авторизация и указаны пользователи для авторизации (первые три строки примера конфигурационного файла).

5. Запустите turnserver

```
turnserver
```

Соединение с использованием внешнего TURN-сервера

При создании сессии с помощью Flashphoner WebSDK необходимо передать параметр `mediaOptions`, в котором следует указать параметры TURN-сервера. Ниже приведен пример создания такой сессии:

```
Flashphoner.createSession({urlServer: url, mediaOptions: {"iceServers": [ {  
'url': 'turn:192.168.0.1:3478?transport=tcp', 'credential': 'password1',  
'username': 'username1' } ], "iceTransportPolicy": "relay"}})
```

Использование внутреннего TURN-сервера

При использовании внешнего TURN сервера трафик через доступные TCP-порты проходит следующим образом:



Браузер клиента устанавливает TCP-соединение на порт встроенного TURN сервера (по умолчанию 3478), затем встроенный TURN соединяется по UDP, используя заданный диапазон портов, на локальный интерфейс WCS. Таким образом, с точки зрения клиента медиатрафик идет через TCP-туннель, а с точки зрения WCS ничего не изменяется, трафик идет через UDP-порты.

Побочный эффект данной схемы в том, что медиатрафик от клиента до WCS-сервера идет по TCP, что может серьезно улучшить качество HD трансляций с высоким битрейтом.

Настройка внутреннего TURN-сервера

Внутренний TURN сервер настраивается при помощи следующих параметров в файле [flashphoner.properties](#):

Параметр	Значение по умолчанию	Описание
<code>turn_ip</code>	<code>ip</code>	Внешний IP адрес встроенного TURN сервера (по умолчанию совпадает с <code>ip</code>)
<code>turn_ip_local</code>	<code>ip_local</code>	Внутренний адрес встроенного TURN сервера, используется для привязки порта (по умолчанию совпадает с <code>ip_local</code>)
<code>turn_port</code>	3478	TCP порт встроенного TURN сервера
<code>turn_password</code>	coM77EMrV7Cwhyhan	пароль на доступ к TURN серверу (имя пользователя всегда <code>flashphoner</code>)
<code>turn_media_port_from</code>	36001	Начало диапазона UDP портов, используемых TURN для пропуска медиа трафика при подключении к WCS
<code>turn_media_port_to</code>	37000	Окончание диапазона UDP портов
<code>turn_media_ports_auditor_interval</code>	5000	Интервал проверки занятых портов в миллисекундах
<code>turn_media_ports_auditor_max_attempts</code>	3	Количество проверок, освобожден ли порт
<code>turn.server_channel_receive_buffer_size</code>	1048576	Размер буфера на прием данных в байтах
<code>turn.server_channel_send_buffer_size</code>	1048576	Размер буфера на передачу данных в байтах

Соединение с использованием внутреннего TURN-сервера

Как и для внешнего TURN сервера, при создании сессии с помощью Flashphoner WebSDK необходимо передать параметр `mediaOptions`, в котором следует указать параметры встроенного TURN-сервера:

```
Flashphoner.createSession({urlServer: url, mediaOptions: {"iceServers": [ {
  'url': 'turn:test.flashphoner.com:3478?transport=tcp', 'credential':
  'coM77EMrV7Cwhyhan', 'username': 'flashphoner' } ]}})
```

Если UDP-порты закрыты брандмауэром, браузер не может установить WebRTC соединение по UDP. В этом случае необходимо в `mediaOptions` указать параметр `"iceTransportPolicy": "relay"`

```
Flashphoner.createSession({urlServer: url, mediaOptions: {"iceServers": [ {  
'url': 'turn:test.flashphoner.com:3478?transport=tcp', 'credential':  
'coM77EMrV7Cwhyan', 'username': 'flashphoner' } ], "iceTransportPolicy":  
"relay"}})
```

для того, чтобы медиатрафик пошел через TURN сервер.

Краткое руководство по тестированию

1. Для теста используем:
2. WCS сервер с активированным встроенным TURN сервером
3. веб-приложение [Firewall Traversal Streaming](#) в браузере Chrome
4. `iptables` для закрытия UDP портов на сервере
5. Закройте UDP порты на внешнем сетевом интерфейсе WCS сервера

```
iptables -i ens192 -I INPUT -m udp -p udp --dport 0:65535 -j DROP
```

Здесь `ens192` - внешний сетевой интерфейс WCS сервера.

6. Откройте приложение Firewall Traversal Streaming, укажите в поле `TURN server`

```
turn:test.flashphoner.com:3478?transport=tcp
```

Здесь

7. `test.flashphoner.com` - адрес WCS сервера
8. `3478` - порт встроенного TURN сервера
9. Настройте перенаправление медиа трафика

10. если UDP порты на WCS сервере открыты, снимите переключатель **Force relay**


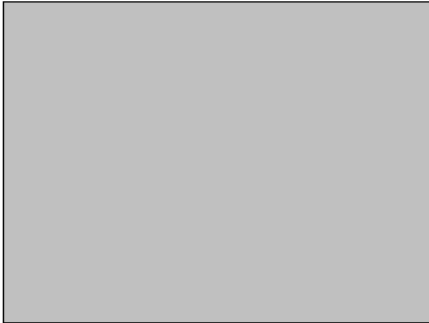
WCS Server	<input type="text" value="wss://test1.flashphoner.com"/>
Turn Server	<input type="text" value="turn:test1.flashphoner.com:"/>
Username of turn server	<input type="text" value="flashphoner"/>
Credential of turn server	<input type="text" value="coM77EMrV7Cwhyan"/>
Force relay	<input type="checkbox"/>
<input type="button" value="Connect"/>	

11. если UDP порты на WCS сервере закрыты, установите переключатель **Force relay**

WCS Server	<input type="text" value="wss://test1.flashphoner.com"/>
Turn Server	<input type="text" value="turn:test1.flashphoner.com:"/>
Username of turn server	<input type="text" value="flashphoner"/>
Credential of turn server	<input type="text" value="coM77EMrV7Cwhyan"/>
Force relay	<input checked="" type="checkbox"/>
<input type="button" value="Connect"/>	

12. Нажмите **Connect**, введите имя потока **test** и нажмите **Publish**. Начнется публикация потока через встроенный TURN сервер

Firewall Traversal Streaming

Local	Player
	
<input type="text" value="test"/> <input type="button" value="Stop"/>	<input type="text" value="3729"/> <input type="button" value="Play"/>
PUBLISHING	

Известные проблемы

1. Некоторые браузеры не поддерживают работу через TURN сервер

Браузеры Microsoft Legacy Edge и Mozilla Firefox не поддерживают работу через TURN сервер

Симптомы

При попытке установить соединение через TURN сервер публикация/воспроизведение не работают

Решение

Использовать браузер Chrome или его производные