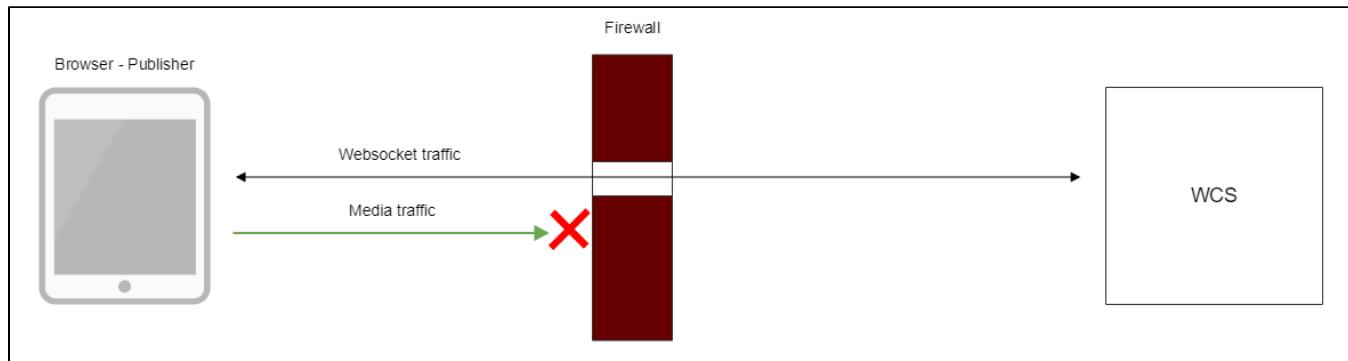


TURN server

- Описание
 - Поддерживаемые платформы и браузеры
- Использование внешнего TURN-сервера
 - Установка и настройка TURN-сервера на CentOS 7
 - Соединение с использованием внешнего TURN-сервера
- Использование внутреннего TURN-сервера
 - Настройка внутреннего TURN-сервера
 - Соединение с использованием внутреннего TURN-сервера
- Краткое руководство по тестированию
- Известные проблемы

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:

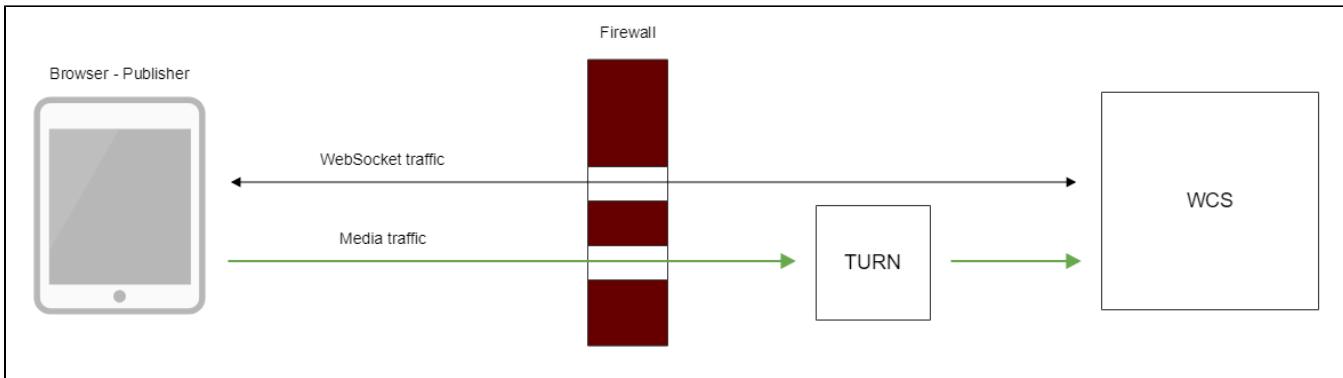
1. Использование внешнего TURN сервера. Данный вариант подходит корпоративным пользователям с развитой инфраструктурой, а также пользователям, предпочитающим разделять выполняемые задачи по серверам.
2. Использование внутреннего TURN сервера, встроенного в WCS. Данный вариант подходит малым предприятиям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

Поддерживаемые платформы и браузеры

	Chrome	Firefox	Safari 11	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 исходников 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
```

а) 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
```

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

3. Запустите turnserver

```
turnserver
```

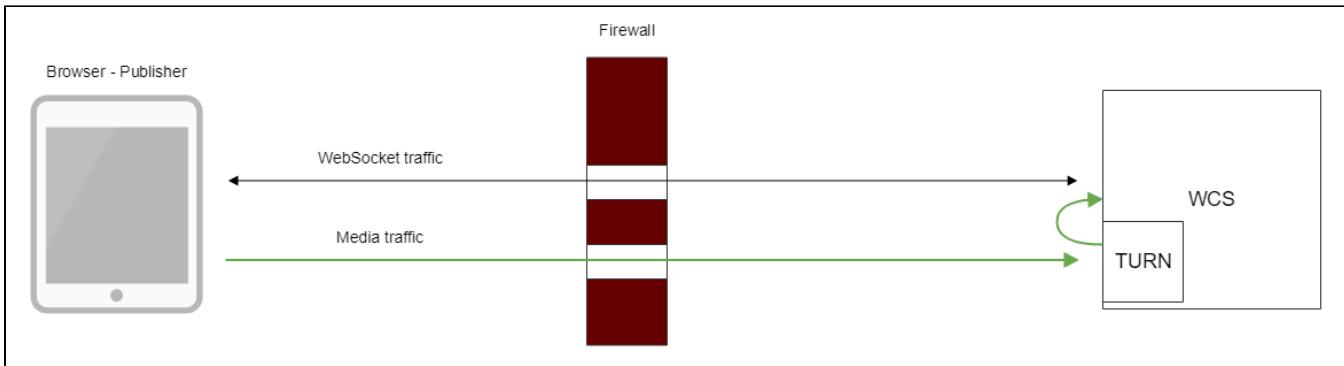
Соединение с использованием внешнего TURN-сервера

При создании сессии с помощью Flashphoner API необходимо передать параметр mediaOptions, в котором следует указать координаты 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
turn_ip	-	Внешний IP адрес встроенного TURN сервера (по умолчанию совпадает с ip)
turn_ip_local	-	Внутренний адрес встроенного TURN сервера, используется для привязки порта(по умолчанию совпадает с ip_local)
turn_port	3478	TCP порт встроенного TURN сервера
turn_password	coM77EMrV7Cwhyan	пароль на доступ к TURN серверу (имя пользователя всегда flashphoner)
turn_media_port_from	36001	Начало диапазона UDP портов, используемых TURN для пропуска медиатрафика при подключении к WCS
turn_media_port_to	37000	Окончание диапазона UDP портов
turn_media_ports_auditor_interval	5000	Интервал проверки занятых портов в миллисекундах
turn_media_ports_auditor_max_attempts	3	Количество проверок, освобожден ли порт
turn_server_channel_receive_buffer_size	1048576	Размер буфера на прием данных в байтах
turn_server_channel_send_buffer_size	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 API необходимо передать параметр `mediaOptions`, в котором следует указать координаты встроенного TURN-сервера:

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

Если UDP-порты не закрыты брандмауэром, браузер 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:

- WCS сервер с активированным встроенным TURN сервером
- веб-приложение [Firewall Traversal Streaming](#) в браузере Chrome
- iptables для закрытия UDP портов на сервере

2. 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.

Если данный шаг выполнен успешно, переходите к шагу 3b, если порты закрыть не удалось, то к шагу 3a

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

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

Здесь

- test.flashphoner.com - адрес WCS сервера
- 3478 - порт встроенного TURN сервера

a) если UDP порты на WCS сервере открыты, снимите переключатель Force relay

The screenshot shows the configuration interface for the Firewall Traversal Streaming application. It includes the following fields:

- WCS Server:** wss://test1.flashphoner.com/
- Turn Server:** turn:test1.flashphoner.com:3478
- Username of turn server:** flashphoner
- Credential of turn server:** coM77EMrV7Cwhyan
- Force relay:**
- Connect:** A button at the bottom right.

b)если UDP порты на WCS сервере закрыты, установите переключательForce relay

WCS Server	wss://test1.flashphoner.com
Turn Server	turn:test1.flashphoner.com:
Username of turn server	flashphoner <input type="button" value="..."/>
Credential of turn server	coM77EMrV7CwhyAn
Force relay	<input checked="" type="checkbox"/>
<input type="button" value="Connect"/>	

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

Firewall Traversal Streaming

Local



test Stop

PUBLISHING

Player

3729

Известные проблемы

1. 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.