

# Turnserver (stun/turn)

---

When you do a one to one communication with a peer, you have 3 possibilities:

- Direct P2P
- P2P over a turn server
- Jitsi VideoBridge

If you and your peer can't connect together then a proxy is necessary. In that case, the best way to communicate is to go through a turn server. It uses few resources and is far more efficient than going through the jitsi VideoBridge service.

To advertise your system that a turn server exists, you need to call a stun server. It returns the list of all p2p possibilities, including the turn server.

When you do a peer to peer videoconference, and each peer can't connect directly to each other, you may use a turnserver to act as a proxy between the peers.

## Configuration

---

```
cp /usr/share/doc/jitsi-meet-turnserver/turnserver.conf /etc/turnserver/turnserver.conf
```

/etc/turnserver/turnserver.conf

```
# Do not remove any line
# Replace this line
static-auth-secret=turnSecretPassword
server-name=YOUR_DOMAIN
realm=YOUR_DOMAIN
# Change the path to fix one (we will use it below)
cert=/etc/turnserver/certs/cert.pem
pkey=/etc/turnserver/certs/pkey.pem
# Add this line at the end (it force turnserver to only listen on this ips)
listening-ip=YOUR_PUBLIC_IPV4
listening-ip=YOUR__PUBLIC_IPV6
relay-ip=YOUR_IPV4
relay-ip=YOUR_IPV6
# If you are behind nat, don't use the relay-ip and use listening-ip that way
```

```
listening-ip=YOUR_PUBLIC_IPV4/YOUR_PRIVATE_IPV4  
listening-ip=YOUR_PUBLIC_IPV6/YOUR_PRIVATE_IPV6
```

# Certificates

You need to copy the certificates for turnserver. The process uses the user “turnserver” to run and need to be able to read the certificates.

## Self-signed

```
mkdir /etc/turnserver/certs  
cp /etc/prosody/certs/YOUR_DOMAIN.crt /etc/turnserver/certs/cert.pem  
cp /etc/prosody/certs/YOUR_DOMAIN.key /etc/turnserver/certs/pkey.pem  
chown -R turnserver: /etc/turnserver/certs
```

## Letsencrypt

/etc/letsencrypt/renewal-hooks/deploy/turn.sh

```
#!/bin/sh  
### turnserver  
/usr/bin/install -d -m770 -o turnserver -g turnserver /etc/turnserver/certs  
/usr/bin/install -m640 -o turnserver -g turnserver /etc/letsencrypt/live/YOUR_DOMAIN/fullchain.pem  
/etc/turnserver/certs/cert.pem  
/usr/bin/install -m600 -o turnserver -g turnserver /etc/letsencrypt/live/YOUR_DOMAIN/privkey.pem  
/etc/turnserver/certs/pkey.pem  
/bin/systemctl restart turnserver.service
```

The set execution flag to the file and run it once

```
chmod +x /etc/letsencrypt/renewal-hooks/deploy/turn.sh  
/etc/letsencrypt/renewal-hooks/deploy/turn.sh
```

## Jitsi meet

/etc/webapps/jitsi-meet/config.js

```
{  
  p2p: {  
    enabled: true,
```

```
stunServers: [
    { urls: 'stun:YOUR_DOMAIN:3478' }
],
// activate this option to force the usage of the relay
// it will force the usage of turnserver or jvb and avoid direct connection
// it is nice for testing, it seems to improve the stability of the connection,
// remove it if you want to allow direct connection without your server as a relay
iceTransportPolicy: 'relay',
// take care to avoid extra coma, or the json will became invalid
backToP2PDelay: 5
}
}
```

## Prosody

/etc/prosody/conf.d/jitsi.cfg.lua

```
external_service_secret = "turnSecretPassword";
external_services = {
    { type = "stun", host = "YOUR_DOMAIN", port = 3478 },
    { type = "turn", host = "YOUR_DOMAIN", port = 3478, transport = "udp", secret = true, ttl = 86400,
algorithm = "turn" },
    { type = "turns", host = "YOUR_DOMAIN", port = 5349, transport = "tcp", secret = true, ttl = 86400,
algorithm = "turn" }
};
```

## Start services

```
# restart prosody
systemctl restart prosody
# start turnserver
systemctl start turnserver
# check turnserver
systemctl status turnserver
# activate at boot
systemctl enable turnserver
```

Revision #1

Created 8 June 2023 06:48:17 by Celogeek

Updated 8 June 2023 06:52:39 by Celogeek