¿What is Watchity?

Watchity is a cloud platform based on the production, editing and distribution of live video. To meet these objectives, there are different tools within the platform that allow capturing, monitoring, performing/editing and broadcasting live video streams.

In order to ensure the proper functioning of these tools, we recommend the following configuration:

Firewall requirements

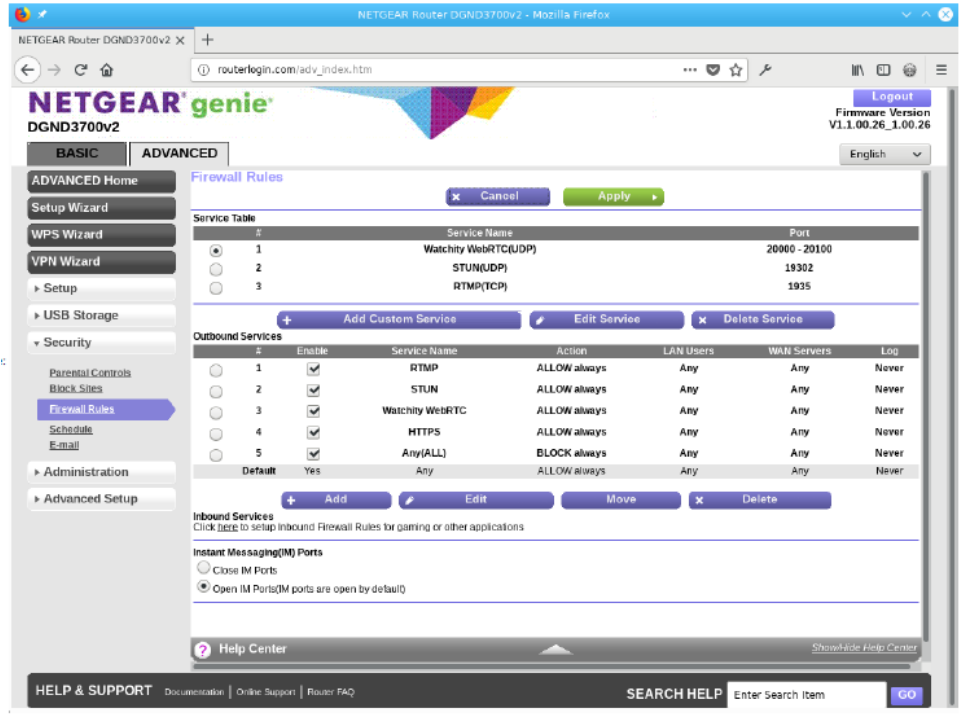
This applies especially to corporate networks that have restricted outgoing traffic. This is not the most common case, as Firewalls do not usually restrict outgoing traffic. If it is restricted, the output ports detailed below must be opened.

Outbound:

- **19302 / UDP** (STUN for WebRTC monitor in the Mixer tool)
- **20000-20100 / UDP** (for audio/video WebRTC monitor in the Mixer tool)
- **443 / TCP** (to operate the Mixer in HTTPS)
- **1935 / TCP** (RTMP for live streaming) (**only needed if you want to stream to Watchity streaming servers**)

Inbound:

- (no needs)



IP addresses pool from AWS

Some organizations have firewalls to limit access to and from Internet. In order to have Watchity services running, they need to grant access to some numerical IP addresses.

Numerical IP addresses in AWS are not fixed. They use AWS IP Address Ranges (https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html). AWS provides a list of all their numerical IP addresses in json format:

```
wget https://ip-ranges.amazonaws.com/ip-ranges.json
```

You can then filter this json to get a range related to a service in a specific region. These are typical use cases related to which services need to be enabled:

	frontend	streaming input RTMP	audio/video in WebRTC monitor	stun server in WebRTC monitor	streaming output HLS (live)	streaming output HLS (vod)	media library
access to:	https://app.watchity.com/ , https://<organization>.watchity.com/	rtmp://lb-<watchit_uuid>.watchity.net/...	x.x.x.x	stun.l.google.com (http://stun.l.google.com)	https://xxxxxx.cloudfront.net/...m3u8	https://watchity-videos-ireland.s3.amazonaws.com/wct-<watchit_uuid>/...m3u8	https://media.watchity.com/<organization>/...mp4
ports:	443 tcp	1935 tcp	20000-20100 udp	19302 udp	443 tcp	443 tcp	443 tcp
filter to get ip addresses range:	jq -r '.prefixes[] | select(.region=="GLOBAL") | select(.service=="CLOUDFRONT") | .ip_prefix' < ip-ranges.json	jq -r '.prefixes[] | select(.region=="eu-west-1") | select(.service=="EC2") | .ip_prefix' < ip-ranges.json	jq -r '.prefixes[] | select(.region=="eu-west-1") | select(.service=="EC2") | .ip_prefix' <ip-ranges.json	stun.l.google.com (http://stun.l.google.com)	jq -r '.prefixes[] | select(.region=="GLOBAL") | select(.service=="CLOUDFRONT") | .ip_prefix' <ip-ranges.json	jq -r '.prefixes[] | select(.region=="eu-west-1") | select(.service=="S3") | .ip_prefix' <ip-ranges.json	jq -r '.prefixes[] | select(.region=="GLOBAL") | select(.service=="CLOUDFRONT") | .ip_prefix' <ip-ranges.json
camera	–	✓	–	–	–	–	–
mixer	✓	–	✓	✓	–	–	✓
player	✓	–	–	–	✓	✓	–

Next sections detail how to filter the json file to get the IP ranges for each service used by Watchity.

Frontend:

Web frontend to admin watchits.

Access to: https://app.watchity.com/ , https://<organization>.watchity.com/

Cloudfront from global region:

```
jq -r '.prefixes[] | select(.region=="GLOBAL") |
select(.service=="CLOUDFRONT") | .ip_prefix' <  ip-ranges.json
```

Stream inputs (puntos de publicación)

Publication points where rtmp streams are sent.

Access to: rtmp://lb-<watchit_uuid>.watchity.net/... EC2 from eu-west-1

```
jq -r '.prefixes[] | select(.region=="eu-west-1") |
select(.service=="EC2") | .ip_prefix' <  ip-ranges.json
```