socialive®

Network / Firewall Guide

Last update: March 11, 2024

CDNs

Networks that allow TLS traffic by default should not need to explicitly allow CDN properties. However, for more restrictive environments where destinations outside your network must be specified, please reference the table below:

Protocol	**Port(s)**	**Domain**
https	443	**cc-overlays.s3.amazonaws.com**
		In-broadcast graphic overlays
https	443	**d10pibf47uu4kg.cloudfront.net**
		Video thumbnails
https	443	**d23f9rdkw0nh8n.cloudfront.net**
https	443	**sl-recording-clips.s3.amazonaws.com**
		Video playback hosts
https	443	**cc-static-js.s3.amazonaws.com**
		Static JavaScript host
https	443	**fonts.googleapis.com**
		Static font host
https	443	**webrtc.github.io**
		Static host for adapter.js shim used for x-browser and x-version adaptability
https	443	**cdnjs.cloudflare.com**
		Static JavaScript host
https	443	**www.gstatic.com**
		Static JavaScript host

APIs

Networks that allow TLS traffic by default should not need to make allowances for API properties. However, for more restrictive environments where destinations outside your network must be specified, please reference the table below:

Protocol	Port(s)	Domain
https	443	**api.socialive.us**
wss	443	**broker.socialive.us**
wss	443	**origin.socialive.us**
https, wss	443	**graphql-gateway.service.socialive.us**
https	443	**firestore.googleapis.com**
		Domains for REST API and Signaling
https	443	**turn.us-east-1.socialive.us**
		STUN/TURN for NAT traversal
https	443	**api-iam.intercom.io**
		Support and Customer Success communication, in-app notifications and tutorials
https	443	**sdk.amazonaws.com**
		Static JavaScript host

- **firestore.googleapis.com** (signaling service) will not function properly if traffic to this domain passes through a proxy. As proxies typically do not handle persistent connections correctly (waiting for a full response from destination before flushing), the proxy should be configured to bypass this domain

Streaming

The IPs in the below table are used to facilitate the transmission of real-time media in the browser. In restrictive networks where destinations must be explicitly allowed, all IPs and corresponding port ranges below should be allowed.

Protocol	Port(s)	Domain/IP	Class
tcp	1935	**54.221.33.151**	TCP Stream
tcp	1935	**52.7.176.185**	TCP Stream
tcp	1935	**54.145.113.113**	TCP Stream
tcp	1935	**52.2.236.53**	TCP Stream
		Live broadcast monitoring	
tls,tcp,udp	443	**52.204.129.114**	RTP Stream
		STUN/TURN for NAT traversal	
udp	5002-65535	**52.91.211.53**	RTP Stream
udp	5002-65535	**3.213.245.201**	RTP Stream
		Real-time streaming	

- The udp destinations with the large port ranges above are for connections to a fleet of Selective Forwarding Units (real-time streaming). For best performance/quality in your streams, ensure that these destinations and port ranges are allowed.
- If your organization uses a proxy, the IP destinations and ports above should be bypassed by the proxy.

FAQ:
You specified UDP but you are using SRTP why the difference?

RTP over UDP protocols are addressed in this document. **SRTP is not a protocol.** It is a **profile** for Real-time Transport Protocol (RTP) intended to provide encryption, authentication and integrity. Socialive uses SRTP for our WebRTC communications over RTP/UDP.