Easy Teams Firewall Settings

Notes to observe

- SIP-ALG/proxy regarding standard RFC SIP-ports 5060/5061 will not interfere, otherwise disable (SIP traffic inspection)
- Packet proxy regarding documented ports should be disabled in the local firewall. If services aren´t working as expected, please allow the rules from the inside of the local firewall as well.
- Media/Speech is negotiated dynamically in the SDP for every call. Therefore it is necessary to allow the whole port span.
- If your firewall supports DNS lookups in firewall rules, use **"allowlist.easyteams.se"**, otherwise, you may use these subnets.

To	Desitnation port	Source port	Protocol	Transport	Rule
99.77.137.0/24	80 / 443	Any	HTTP/HTTPS	TCP	Allow
52.95.227.0/24	80 / 443	Any	HTTP/HTTPS	TCP	Allow
13.50.0.0/16	80 / 443	Any	HTTP/HTTPS	TCP	Allow
63.246.112.0/24	80 / 443	Any	HTTP/HTTPS	TCP	Allow
13.53.0.0/16	80 / 443	Any	HTTP/HTTPS	TCP	Allow
13.51.0.0/16	80 / 443	Any	HTTP/HTTPS	TCP	Allow
13.48.0.0/15	80 / 443	Any	HTTP/HTTPS	TCP	Allow
16.170.0.0/15	80 / 443	Any	HTTP/HTTPS	TCP	Allow
3.5.216.0/22	80 / 443	Any	HTTP/HTTPS	TCP	Allow
15.177.72.0/24	80 / 443	Any	HTTP/HTTPS	TCP	Allow
52.94.249.128/28	80 / 443	Any	HTTP/HTTPS	TCP	Allow
99.150.64.0/21	80 / 443	Any	HTTP/HTTPS	TCP	Allow
13.48.186.128/27	80 / 443	Any	HTTP/HTTPS	TCP	Allow
99.77.137.0/24	Any	Any	None	UDP	Allow
52.95.227.0/24	Any	Any	None	UDP	Allow
13.50.0.0/16	Any	Any	None	UDP	Allow
63.246.112.0/24	Any	Any	None	UDP	Allow
13.53.0.0/16	Any	Any	None	UDP	Allow
13.51.0.0/16	Any	Any	None	UDP	Allow
13.48.0.0/15	Any	Any	None	UDP	Allow
16.170.0.0/15	Any	Any	None	UDP	Allow
3.5.216.0/22	Any	Any	None	UDP	Allow
15.177.72.0/24	Any	Any	None	UDP	Allow
52.94.249.128/28	Any	Any	None	UDP	Allow
99.150.64.0/21	Any	Any	None	UDP	Allow
13.48.186.128/27	Any	Any	None	UDP	Allow