Vevox Whitelisting Instructions

Customers should whitelist the following domains:

*.meetoo.io

*.meetoo.com

*.lumireactor.com

*.vevox.com

*.vevox.app

Here's a list of the ports in-use:

80 (HTTP) and 443 (HTTPS) for dashboard and all clients (80 is only used to perform a HTTP 301 redirect to the HTTPS port). **Vevox never transmits data over unencrypted channels. All data to/from our systems is encrypted in-transit.**

Persistent connections:

All Vevox clients (native and web-based attendee apps, and the web dashboard) make use of persistent TCP connections to enable the server to push state changes directly to the client. In the case of the dashboard and the HTML web apps, this is done through a WebSocket connection on port 443 (HTTPS). In the case of the native attendee apps, this is also done on port 443, however the traffic is not HTTPS. Instead, it is TLS-encrypted TCP traffic using a proprietary protocol at the layer 7 (Application) layer. (TLS is sometimes referred to as SSL, however TLS is technically the correct name).

The persistent connection is a requirement for all clients; there is no "fall back" to a non-persistent connection mechanism. Therefore, customers' networks must allow for these sorts of connections otherwise operation will fail. Proxy servers or firewalls that disallow connections of this type should be configured to allow them for Vevox. Also, DPI firewalls/routers that inspect traffic on port 443 and disallow traffic that is not HTTPS should be configured to allow our proprietary connection to succeed, otherwise native attendee apps will be unable to operate (however, all web apps will operate fine).

FAQ

Q: Why can't Vevox give us a list or block of IP addresses for us to whitelist?

Unfortunately, whitelisting by IP address(es) is not possible because:

1. Our servers make use of redundant load balancers whose IP addresses are subject to change without notice. Because of this, they must be referred to by their DNS names.
2. Much of the content that is delivered to our clients (web dashboards and attendee apps) comes from our AWS CloudFront CDN. This content must be referred to by DNS name because the content is stored on many edge node servers all over the world. Two clients will access this content from completely different IPs depending on their physical geography.