grouptalk

Introduction

This document describes how a firewall needs to be configured to allow the GroupTalk service to work properly. It applies to mobile clients (GroupTalk app for Android and iOS), PC web dispatcher and web administration.

Firewall Settings

GroupTalk mobile clients connects to a GroupTalk server through a single, persistent TCP connection, using a proprietary protocol. The connection is always initiated by the client. The client uses DNS to determine server IP:s and ports via DNS SRV records. Besides the persistent TCP connection a transient UDP connection is needed for transmission of audio. The UDP connection is also always initiated by the client and server port range and IP is the same as for the TCP connection (e.g. if the client is connected to the server via TCP on 212.37.20.202:10002 the UDP packets will be sent to and received from 212.37.20.202:10002).

Thus, the firewall needs to open the same ports for UDP as for TCP. If the firewall is using NAT it must be symmetric. The firewall needs to keep UDP sessions open for at least 20 seconds after the last packet sent from the client to the server. This behavior is default for most firewalls.

Multiple GroupTalk servers are used for redundancy. The port ranges may be expanded in the future.

For the web dispatcher and web administration the standard HTTP and HTTPS ports must be opened for outgoing connections.

Type:	Mobile client access
Port range:	10000-10020 (TCP+UDP)
IP:	212.37.20.202 and 82.193.182.108
Direction:	outgoing connections

Type:	Web dispatcher and admin
Ports:	80 and 443 (TCP)
IP:	212.37.20.202 and 82.193.182.108
Direction:	outgoing connections