WESTCOAST CLOUD VOICE
powered by **Blueface**

FIREWALL GUIDE

Version 1 – Updated: Monday, March 9th, 2020

FIREWALLS

Firewalls sit between a computer (or local network) and another network (such as the internet), controlling the incoming and outgoing network traffic.

- With a firewall, rules determine which traffic is allowed through and which isn't
- Without a firewall, you are unprotected

A firewall's primary security function is to block unsolicited incoming network traffic. Because a firewall is sitting between two networks, it can analyse all incoming and outgoing network traffic and decide what to do with it. Firewalls can be configured with multiple conditions for certain types of traffic.

EXAMPLE

For security purposes, a firewall can allow server connections from a specific IP address while blocking all connection requests from elsewhere.

FIREWALL SETTINGS

Please be aware that these settings are simple best SIP practices. The **Westcoast Cloud Voice support team** is not equipped to manage complex firewall queries.

- Allow IP range: 194.213.29.0/24 (whole subnet)
- Disable SIP ALG
- Set UDP alive timeout to 200 Seconds
- Set QoS (Quality of Service)

Should you continue to experience difficulty with your call quality, please contact an IT firewall third party.

WESTCOAST CLOUD VOICE
powered by **Blueface**

USEFUL CONTACTS

To set up partner or customer accounts on Westcoast Cloud Voice portal please email: **admin@westcoastcloud.co.uk**

For sales info: **voice@westcoastcloud.co.uk**, or support: **support@westcoastcloud.co.uk**