Nextiva Firewall Guidelines

Ensure your network is open for your Nextiva traffic

General Information

Firewalls are primarily designed to keep unauthorized traffic from accessing your private network. In some cases the default firewall rules might cause Nextiva's traffic to be blocked. The simplest way to avoid issues is to open up inbound and outbound traffic to/from Nextiva's IP addresses.

- IP Addresses: **208.73.144.0/21** and **208.89.108.0/22.** This range covers the IP addresses from **208.73.144.1 - 208.73.151.255** and **208.89.108.0 – 208.89.111.255**.
- Ports: **5060-5090**
- Transport Method: **TCP** & **UDP**
- Permission: **Allow All Traffic**

Online Support

nextiva.com/support/nextiva-networking-guidelines.html

Firewall Rules

When setting up firewall rules, please ensure you are creating a firewall rule to allow access through the entire Nextiva IP address range. All Nextiva servers are located in the following IP range:

CIDR: 208.73.144.0/21 & 208.89.108.0/22

Range: 208.73.144.0 - 208.73.151.255 and 208.89.108.0 – 208.89.111.255

Cisco Firewall Rules

To whitelist Nextiva's IP range in a Cisco command line device, the following rules must be set:

- access-list permit ip 208.73.144.0 0.0.7.255
- access-list permit ip 208.89.108.0 0.0.3.255