Firewall configuration guide

TCP/UDP required for CallSwitch. The following is configured on your firewall/router to allow traffic outbound to the internet.

TCP/UDP Ports used by handsets:

**TCP Ports**

* 10001 (Presence)
* 10005 (Presence)
* 5060 to 5069 (SIP)
* 80 (HTTP Config & Web GUI)
* 443  (HTTPS Config & Web GUI)
* 11389 (LDAP Phonebook)

**UDP Ports**

* 5060 to 5069 (SIP)
* 10000 to 20000 (RTP Traffic)

⚠️ **Important note: You must ensure SIP ALG is disabled across all firewall devices.**

Additional ports for Communicator Apps:

**TCP Ports**

* 10005 (Communicator Login proxy)
* 10007 (Communicator Login proxy)
* 10009 (Communicator Login proxy)
* 5222 (Jabber)
* 5223 (Jabber)

**Additional Ports (non-critical):**

* UDP 4000 to 4999 (T.38 Fax)

**CallSwitch Meetings**

IP addresses/domains that need whitelisting for CallSwitch Meetings.(video). If you have issues starting the video in CallSwitch Meetings you may need to whitelist the domain.

* sfu-chi.commsware.com

**iOS Firewall rules**

If the iOS app crashes on start-up (whilst using Wifi), it could be that the network is blocking traffic to the analytics server used for crash reports. To resolve this, please allow traffic to the following FQDNs using UDP port 19302:

* lg-in-f127.1e100.net
* wq-in-f127.1e100.net

Firewall Best practices

The best practice for allowing traffic is to open the firewall to your CallSwitch server hostname (example MT510.callswitch.net , your actual server may start LT or CC , please ask Phoenix Link Support for your server name). Please make sure that you use trusted DNS servers to allow for automatic DNS name resolution.

⚠️ **Important note: services are built into Public Cloud services. Please make sure that your firewall is configured to use DNS lookups regularly.**

⚠️ **Do not configure inbound firewalls that allow direct access to handsets (SIP, HTTP UI etc). Direct traffic to the handset either directly via public IP address or via NAT may lead to the handset being compromised and open to fraud.**

⚠️ **Important note: Please make sure that your firewall is also configured not to use uPnP from your VOIP VLAN or network.**

Example firewall configuration

**Handsets**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source IP address** | **Protocol** | **Source Port** | **Destination address** | **Destination port** | **Purpose** |
| LAN network/Voice VLAN | TCP | 1023 to 65535 | MT501.callswitch.net | 10001 | Presence |
| LAN network/Voice VLAN | TCP | 1023 to 65535 | MT501.callswitch.net | 10005 | Presence |
| LAN network/Voice VLAN | TCP | 1023 to 65535 | MT501.callswitch.net | 5060 to 5069 | TCP SIP and TLS |
| LAN network/Voice VLAN | TCP | 1023 to 65535 | MT501.callswitch.net | 80 | HTTP Config & Web GUI (Plain-text) |
| LAN network/Voice VLAN | TCP | 1023 to 65535 | MT501.callswitch.net | 443 | HTTPS Config & Web GUI (Encrypted) |
| LAN network/Voice VLAN | TCP | 1023 to 65535 | MT501.callswitch.net | 11389 | LDAP Phonebook (plain-text) |
| LAN network/Voice VLAN | TCP | 1023 to 65535 | MT501.callswitch.net | 11636 | LDAP Phonebook (Encrypted) |
| LAN network/Voice VLAN | UDP | 1023 to 65535 | MT501.callswitch.net | 5060 to 5069 | SIP |
| LAN network/Voice VLAN | UDP | 1023 to 65535 | MT501.callswitch.net | 10000 to 20000 | RTP |

⚠️ **Important note: If you are operating a stateless firewall make sure you have return traffic rules configured for traffic flows. - Most modern firewalls are stateful and will not require any return firewall rules.**

**Additional ports**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source IP address** | **Protocol** | **Source Port** | **Destination address** | **Destination port** | **Purpose** |
| LAN network | TCP | 1023 to 65535 | MT501.callswitch.net | 10005 | Communicator Login proxy |
| LAN network | TCP | 1023 to 65535 | MT501.callswitch.net | 10007 | Communicator Login proxy |
| LAN network | TCP | 1023 to 65535 | MT501.callswitch.net | 10009 | Communicator Login proxy |
| LAN network | TCP | 1023 to 65535 | MT501.callswitch.net | 5222 | Jabber traffic (deprecated from v6.0) |
| LAN network | TCP | 1023 to 65535 | MT501.callswitch.net | 5223 | Jabber traffic (deprecated from v6.0) |
| LAN network | UDP | 1023 to 65535 | MT501.callswitch.net | 4000 to 4999 | T.38 Fax |

**CallSwitch Meetings**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source IP address** | **Protocol** | **Source Port** | **Destination address** | **Destination port** | **Purpose** |
| LAN network | TCP | 1023 to 65535 | sfu-chi.commsware.com | 5222 | Jabber traffic Proxy (deprecated from v6.0) |
| LAN network | TCP | 1023 to 65535 | sfu-chi.commsware.com | 5500 | CallSwitch Meetings |
| LAN network | TCP | 1023 to 65535 | sfu-chi.commsware.com | 5900 | CallSwitch Meetings |
| LAN network | TCP | 1023 to 65535 | sfu-chi.commsware.com | 8088 | CallSwitch Meetings |
| LAN network | TCP | 1023 to 65535 | sfu-chi.commsware.com | 8181 | CallSwitch Meetings |

**Yealink Provisioning (RPS)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source IP address** | **Protocol** | **Source Port** | **Destination address** | **Destination ports** | **Purpose** |
| LAN network/Voice VLAN | TCP | 1023 to 65535 | 52.71.103.102  52.29.124.181  3.124.165.251 | 80,443,8443 | Yealink (RPS (dm)) Auto Provisioning service |