



White Paper

Firewall Requirements for the OnSight Mobile Collaboration System and Hosted Librestream SIP Service



Librestream

Table of Contents

1	FIREWALL REQUIREMENTS FOR ONSIGHT MOBILE COLLABORATION SYSTEM AND HOSTED SIP SERVICE	3
1.1	Overview.....	3
1.2	Endpoint Registration to SIP Server	3
2	FIREWALL REQUIREMENTS – ALLOWING SIP TRAFFIC	3
2.1	Firewall Diagram.....	4
2.2	Example Firewall Configuration.....	5
3	ONSIGHT: NETWORK PROTOCOLS AND PORTS	6
3.1	Network Protocols and Ports Table	6
4	ONSIGHT ENDPOINT INGATE SIPARATOR CALLS OVER FIREWALL	7
4.1	Session Initiation Protocol – Communication Exchange.....	7
5	KNOWN ISSUES:.....	8
6	SIP SERVICE CHECK LIST	8

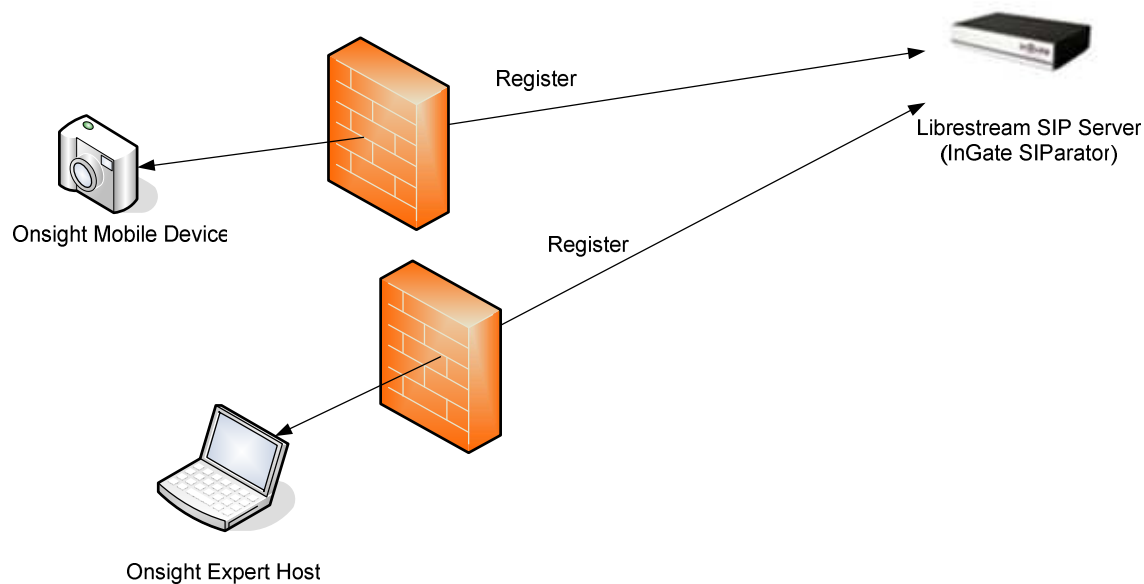
1 Firewall Requirements for Onsight Mobile Collaboration System and Hosted SIP Service

1.1 Overview

This document provides a high level description of the firewall configuration required to allow communication for the Onsight Mobile Collaboration system as well as the hosted Librestream SIP Service.

The Onsight Mobile Collaboration System uses Session Initiation Protocol (SIP) to establish audio and video communication sessions between endpoints. Firewall traversal is required to establish a session when the endpoints are not located on the same LAN. This is accomplished by using a SIP Proxy Server such as the InGate SIParator. Each endpoint registers to the SIP Server which is located outside of the Firewall. The SIParator acts as a proxy and directs SIP messaging and data traffic between the endpoints.

1.2 Endpoint Registration to SIP Server



When the Onsight endpoints are registered to the SIP Server, both the Onsight mobile devices and the Onsight Expert endpoints can initiate calls.

2 Firewall Requirements – Allowing SIP Traffic

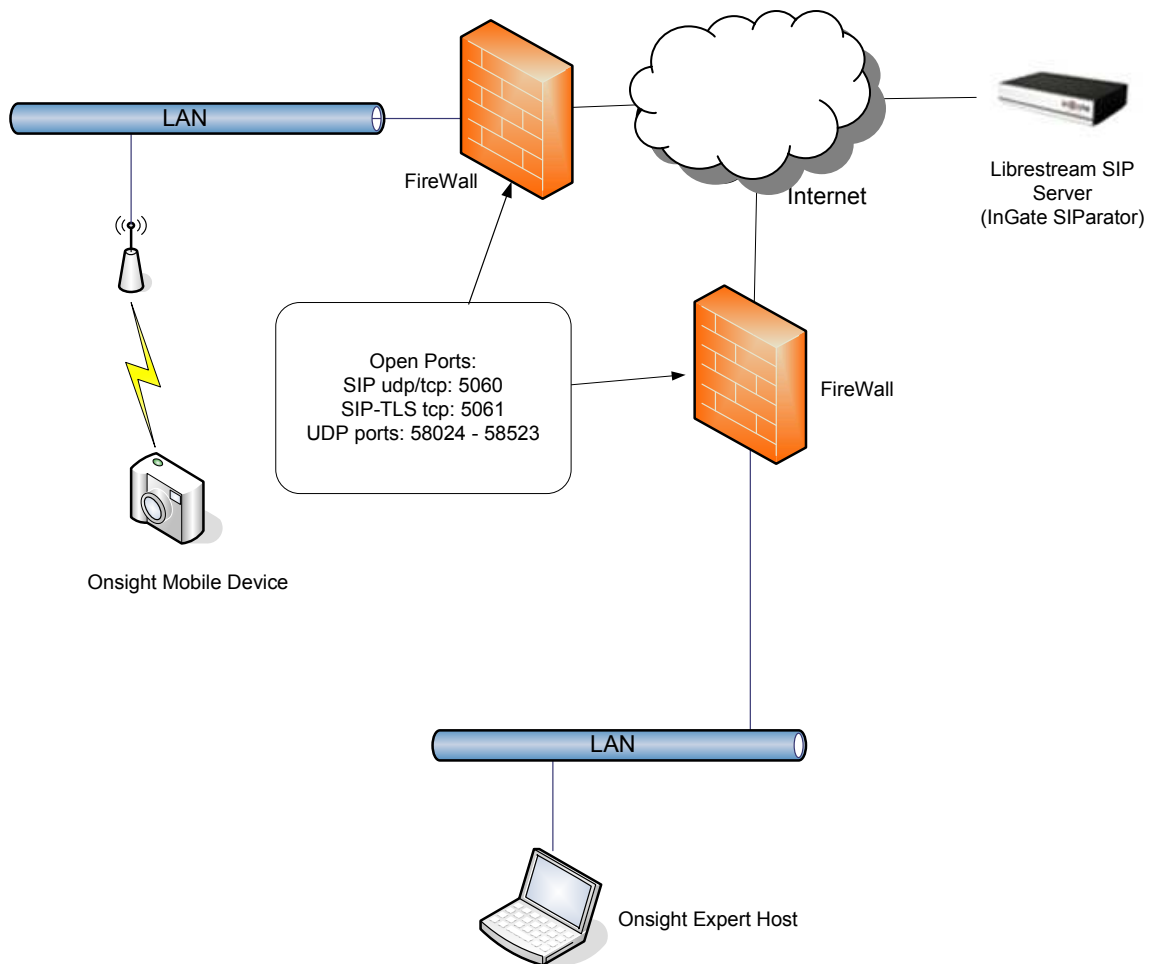
The following ports must be opened to allow SIP and data traffic to the Librestream SIP Server:

- SIP TCP/UDP: 5060 (The Onsight endpoints use SIP TCP 5060 by default but the option to use SIP UDP 5060 is provided.)

- SIP-TLS TCP 5061 (Optional, but required if using TLS encryption for SIP messaging on the SIParator. SIP-TLS provides encrypted SIP messages and requires the installation of certificates on the Onsite endpoints.)
- UDP Media Ports (see NOTE 1). The range of media ports allows the following data streams:
 - Video
 - Voice
 - Subject Audio
 - Data

NOTE 1: The SIP Server passes video/audio/subject audio/data over the UDP Media Ports. The range of ports that must be opened for Media traffic are: UDP 58024-58523.

2.1 Firewall Diagram



2.2 Example Firewall Configuration

The following sample configuration allows 3 specific IP addresses to send (and receive) SIP (TCP and UDP) messages and data (UDP) to the hosted Librestream SIP server at IP address 64.4.89.118 (siphost.librestream.com). The firewall could also be configured to allow any internal IP address to send/receive on the required ports.

ACTION	Source IP Address	Destination	IP Type	Protocol / Port #
<i>Permit or Deny</i>	<i>IP Address, Hostname that INITIATES</i>	<i>IP Address, Hostname</i>	<i>UDP or TCP</i>	<i>Media Port Range</i>
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060

3 Onsite: Network Protocols and Ports

3.1 Network Protocols and Ports Table

This table describes the protocols and ports used by the Onsite Mobile Collaboration System for SIP messaging and data transfer.

Category	Protocol	SRC Port(s)	Notes	Detail ^{3,8}	
SIP Signaling	TCP ⁵	Random ⁷	Used for calls that do not use a SIP proxy server	PC/Device sends SIP/TCP pkts out with SRC=x and DST=5060	PC/Device receives SIP/TCP pkts with SRC=5060 and DST=x
SIP Signaling	TCP	Random ⁷	SIP proxy server based calls	PC/Device sends SIP/TCP pkts out with SRC=x and DST=5060	PC/Device receives SIP/TCP pkts with SRC=5060 and DST=x
Video	RTP	6000/6001 ²		PC/Device sends RTP/RTCP/UDP pkts out with SRC=6000-6001 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6000-6001
Subject Audio	RTP	6002/6003 ²		PC/Device sends RTP/RTCP/UDP pkts out with SRC=6002-6003 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6002-6003
Voice	RTP	6004/6005 ^{2,1}	Two-way voice	PC/Device sends RTP/RTCP/UDP pkts out with SRC=6004-6005 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6004-6005
Data	RTP ⁴	6006 ^{2,6}	Status, control, data, etc.	PC/Device sends RTP/RTCP/UDP pkts out with SRC=6006 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6006

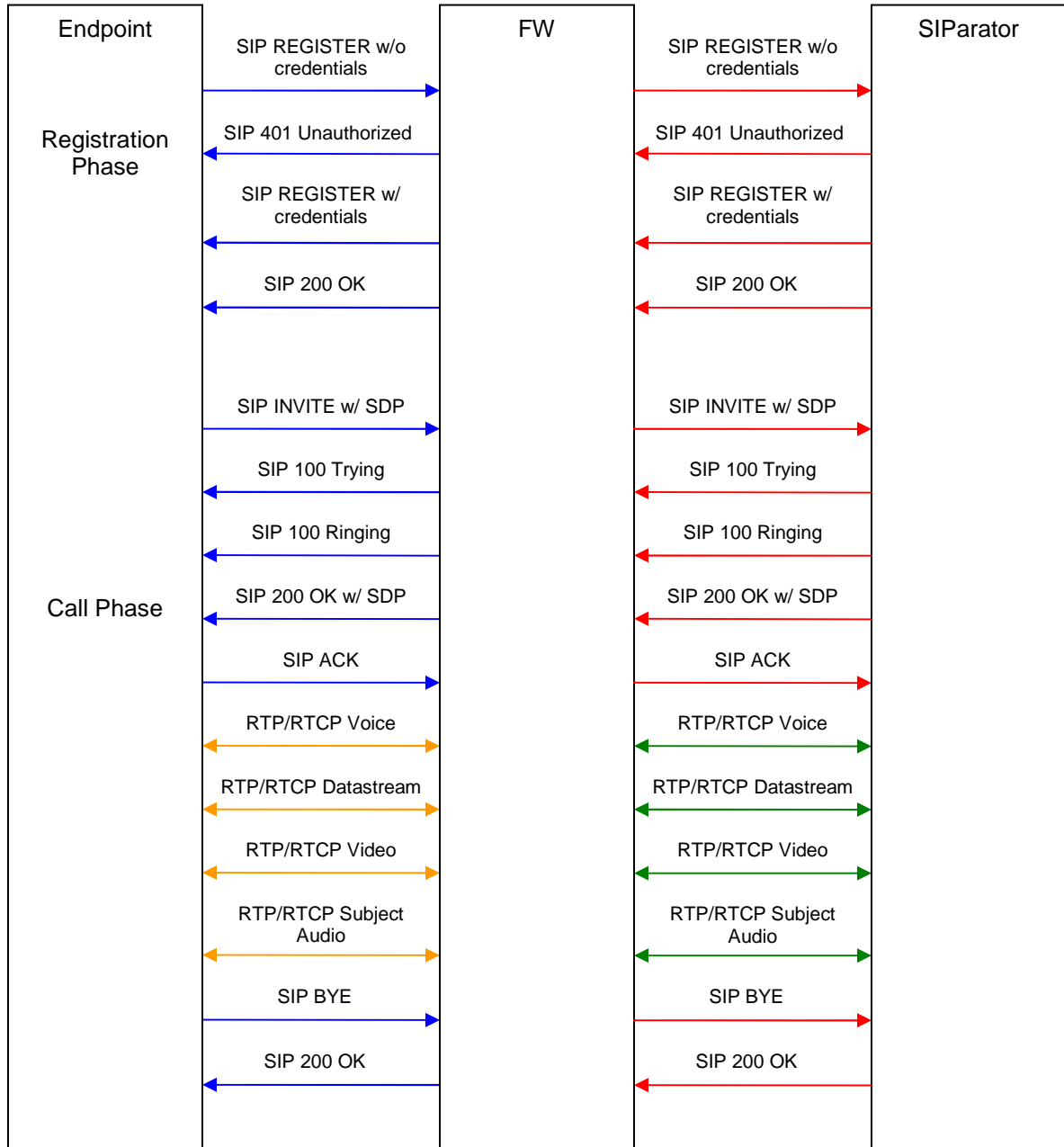
1. Device OS 2.34 (and lower) used random ports. PC Application 2.5.1 (and lower) used random ports.
2. The SRC ports shown are the first choice when a call is established. If a requested port is in use on the PC, the port number will increment (to a limit of 6200) until an available port is located. The Device will not have conflicts and will use the ports shown.
3. 'x' are random ports determined during SIP negotiation.
4. Device OS 2.xx used UDP. PC Application 2.x.x used UDP.
5. Optionally configurable as UDP.
6. Device OS 3.76 (and lower) used port 8888. PC Application 3.1.2 (and lower) used port 8888.
7. Send DST port is 5060, or 5061 if TLS is enabled.
8. 'y' are ports determined by the SIP proxy server during call negotiation usually from a limited range configured by the SIP proxy server administrator.

4 Onsite Endpoint InGate SIParator calls over Firewall

The Onsite endpoints (Onsite mobile device or Onsite Expert) must register with the InGate SIParator. Any calls between the Onsite Endpoints are managed by the SIParator.

Note: There is an option on the SIParator to allow two endpoints located behind the same Firewall/NAT to send data directly between each other, but normally all data traffic is routed through the SIParator.

4.1 Session Initiation Protocol – Communication Exchange



5 Known Issues:

Cisco Routers have a SIP aware feature that is enabled by default. It rewrites header information in the SIP packets, which confuses the SIPParator and must be turned OFF in order for the SIPParator communication to work correctly.

To turn OFF Cisco SIP aware:

- show fixup sip 5060
- no fixup protocol sip 5060

Or

- no ip nat service sip udp port 5060
- no ip nat service sip tcp port 5060

Alternatively, the Onsite endpoints can be configured to use SIP-TLS for the Authentication transport. This requires a certificate to be installed on the endpoints. SIP-TLS encrypts the SIP messaging headers and therefore the headers are ignored by the SIP aware feature of the Cisco router.

6 SIP Service Check List

- Firewall ports have been configured
- Onsite devices are connected to the network (WiFi or Ethernet)
- Endpoints have been configured with SIP Account information
- SIP server address
 - URI
 - User name and password
 - Authentication Transport Setting
- Install Certificates (if necessary, for SIP-TLS)

For further information regarding SIP Registration Setup consult the Onsite mobile device and Onsite Expert User Manuals.