ALCATEL-LUCENT RAINBOW™

Network Requirements

GETTING STARTED GUIDE Ed 5

APRIL 2017

Author: R&D - Cloud Services
Disclaimer

This documentation is provided for reference purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this documentation is provided “as is” without any warranty whatsoever and to the maximum extent permitted.

In the interest of continued product development, ALE International reserves the right to make improvements to this document and the products it describes at any time without notice or obligation.

Copyright

©2017 ALE International. Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for a commercial purpose is prohibited unless prior permission is obtained from Alcatel-Lucent.

Alcatel-Lucent, OmniPCX, and OpenTouch and Rainbow are either registered trademarks or trademarks of Alcatel-Lucent.

All other trademarks are the property of their respective owners.
Contents

Glossary.................................................................................................................. 4

1 Introduction ............................................................................................................ 5

2 Overview .................................................................................................................. 5

3 History ...................................................................................................................... 5

4 Related documents .................................................................................................. 5

5 Requirements .......................................................................................................... 6
  5.1 Global Overview .................................................................................................... 6
  5.2 Used Protocols ....................................................................................................... 6
  5.3 Connections and Ports used ................................................................................... 7
  5.4 Domain used .......................................................................................................... 7
  5.5 Bandwidth requirement .......................................................................................... 8
    5.5.1 WebRTC ............................................................................................................ 8
  5.6 Configuration of border elements in enterprise .................................................. 8
  5.7 Connections illustrated .......................................................................................... 8
    5.7.1 Signaling ............................................................................................................ 8
    5.7.2 WebRTC/Media .................................................................................................. 9
    5.7.3 Detailed call-flow of HTTPS/REST, XMPP and ICE connections................. 12

6 Limitations, Restrictions and workarounds ......................................................... 16
  6.1 HTTP Proxy .......................................................................................................... 16
Glossary

ALE: Alcatel-Lucent Enterprise
PBX: Private Branch Exchange
HTTP: Hyper Text Transfer Protocol
HTTPS: Hyper Text Transfer Protocol Secured
ICE: Interactive Connectivity Establishment - RFC 5245
STUN: Simple Traversal of UDP through NAT - RFC 5389
TURN: Traversal Using Relays around NAT - RFC 5766
DTLS-SRTP: Datagram Transport Layer Security - Secured Real Time Protocol
1 Introduction

This guide provides technical requirements to connect Rainbow clients and Agent to Rainbow Cloud services.

2 Overview

Alcatel-Lucent Enterprise (ALE) is introducing Alcatel-Lucent Rainbow, an overlay cloud service operated by ALE. Rainbow offers contact management, presence, persistent messaging, audio/video, screen and file sharing, with PSTN termination and API openness to integrate with existing customer PBXs, machines and apps.

Rainbow’s clients and agents connect to Rainbow cloud services using Web protocols.

More details about Web protocols used are provided in this document.

3 History

<table>
<thead>
<tr>
<th>Modifications</th>
<th>Date</th>
<th>Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP vs. HTTPS cleanup</td>
<td>04/04/2017</td>
<td>Ed 05</td>
</tr>
<tr>
<td>Minor change (legacy PBX Agent removed)</td>
<td>31/03/2017</td>
<td>Ed 04</td>
</tr>
<tr>
<td>Information on bandwidth added (chapter 5.5)</td>
<td>08/03/2017</td>
<td>Ed 03</td>
</tr>
<tr>
<td>Chapter 5.7.3 added, Chapter 6.1 modified</td>
<td>05/01/2017</td>
<td>Ed 02</td>
</tr>
<tr>
<td>Creation of document</td>
<td>27/10/2016</td>
<td>Ed 01</td>
</tr>
</tbody>
</table>

4 Related documents

None
5 Requirements

5.1 Global Overview

The following picture provides the global overview of Rainbow from network perspective:

Rainbow global picture

5.2 Used Protocols

The Rainbow solution provides multiple client-side applications to connect to the service:

- A Web-based Qt-contained Desktop application for Windows and OSX.
- A Web application for Chrome/Firefox browsers.
- An iOS native application.
- An Android native application.
- An Agent to connect the PBX (can be integrated with the PBX)

All applications aim at providing the same level of services and features and interact with server-side components the following way:
• Through HTTPS (443) for all REST API communications and resources loading.
• Through secure Web Sockets (WSS, 443) for all XMPP messages and notifications.
• Through DTLS and SRTP with or without STUN/TURN for WebRTC-based audio/video media streams.

5.3 Connections and Ports used

Depending on the presence of an HTTP Proxy (Web Proxy), following connections take place between Rainbow client/Agent and Rainbow Cloud Services

<table>
<thead>
<tr>
<th>Protocols</th>
<th>no Proxy</th>
<th>HTTP Proxy configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS (Resources and REST API)</td>
<td>Direct, TCP port 443</td>
<td>Enforced through the Proxy, TCP port 80/443</td>
</tr>
<tr>
<td>Web Sockets (XMPP)</td>
<td>Direct, TCP port 443</td>
<td>WebSocket, enforced through the Proxy, via HTTP switch, TCP port 443</td>
</tr>
<tr>
<td>ICE/TURN(s)</td>
<td>Direct, TCP port 80 and 443</td>
<td>Enforced through the proxy via HTTP Connect tunnel TCP port 80 or 443</td>
</tr>
<tr>
<td>DTLS-SRTP (Media)</td>
<td>Direct, TCP or UDP, dynamic port range (49152 - 65535)</td>
<td>Encapsulated in TURN(s), enforced through the proxy via HTTP Connect tunnel TCP port 80</td>
</tr>
</tbody>
</table>

5.4 Domain used

Rainbow cloud services use the following domains:

<table>
<thead>
<tr>
<th>Used by</th>
<th>Purpose</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rainbow Clients</td>
<td>Resources (website, images, client package, Agent package, ...)</td>
<td>openrainbow.com</td>
</tr>
<tr>
<td>Rainbow Clients</td>
<td>REST API</td>
<td>openrainbow.com</td>
</tr>
<tr>
<td>Rainbow Clients</td>
<td>XMPP over Secured WebSockets</td>
<td>openrainbow.com</td>
</tr>
<tr>
<td>Rainbow Clients</td>
<td>STUN/TURN</td>
<td>openrainbow.com</td>
</tr>
</tbody>
</table>
5.5 Bandwidth requirement

5.5.1 WebRTC
Rainbow WebRTC communication currently relay on the following codecs :
- opus for audio
- vp8 for Video and Screen Sharing,
WebRTC codecs are able to dynamically throttle their bitrates, depending on network performance observed. The following table provides bandwidth requirement per media :

<table>
<thead>
<tr>
<th>Media</th>
<th>Nominal bandwidth</th>
<th>Lowest Bandwidth</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>80kbps</td>
<td>15kbps</td>
<td></td>
</tr>
<tr>
<td>Video</td>
<td>350kbps</td>
<td>150kbps</td>
<td></td>
</tr>
<tr>
<td>Screen Sharing</td>
<td>15-400kbps</td>
<td></td>
<td>Depends if shared content is dynamic</td>
</tr>
</tbody>
</table>

5.6 Configuration of border elements in enterprise

To allow Rainbow to operate properly, border elements like DNS, HTTP Proxy or Firewall must be configured to allow accessing domains and protocols listed in the table chapter 5.3 and 5.4.

Regarding range of ports, if you are in one of the two following cases, there is no specific port range to configure in border elements:
If an HTTP Proxy is configured, all the traffic will be directed through the proxy (HTTP Connect method),
If no HTTP Proxy is configured, that probably means that any direct traffic over arbitrary TCP/UDP ports is allowed.

If you are in the second case, but traffic is filtered by a border element, please, check chapter 5.3 and 5.4.

5.7 Connections illustrated

5.7.1 Signaling
For signaling, HTTPS/REST and Secured WebSockets protocols are used.
If a HTTP Proxy is configured, HTTP Proxy is used. In such case, HTTP Proxy must support Secured WebSocket (HTTP Upgrade to switch to wss protocol).
5.7.2 WebRTC/Media

ICE (Internet Connectivity Establishment) procedure and STUN/TURN protocols are used to dynamically determine how the media will be routed between two Rainbow clients.

Basically, when a WebRTC communication takes place, client proceeds to the following steps:

- For each client, gather candidates addresses (A candidate is a transport address, a combination of IP address and port for a particular transport protocol, allocated on local interface and on TURN server in case of TURN is required, local interface are for example wired Ethernet interface or WiFi interface for a PC),
- Exchange candidates with the peer client,
- Check connectivity for candidates between both clients and select a working peer of candidates.

5.6.2.1 Exemple 1: P2P WebRTC (Basic network)

This is the simplest case. When network elements between the two parties are simple NAT/FW (like home router), in most of the time, WebRTC is able to establish a direct media path (UDP or TCP).
P2P WebRTC (SoHo/Home network)
5.6.2.1 Exemple 2 : P2P WebRTC (Enterprise network)

When it comes to enterprise network, most likely an HTTP Proxy will be there. In such case, HTTP Tunnel and TURN are used to establish the media path.

P2P WebRTC (Enterprise Network)

Note: to simplify figures, only one TURN server is illustrated. For a P2P communication, depending on geography and network performance, up to two TURN server could be used to establish a communication.
5.7.3 Detailed call-flow of HTTPS/REST, XMPP and ICE connections

The following figures illustrate a case where Rainbow Client1 make an Audio/Video call to Rainbow Client2. Rainbow Client1 is in an enterprise environment with NAT/FW and HTTP Proxy border elements. Rainbow Client2 is in a Home network with simple NAT/FW as border element (home router/box).

Network layers (Rest API):

[Diagram showing network layers with HTTP and HTTPS protocols]

Network layers (XMPP):

[Diagram showing network layers with XMPP and WSS protocols]

HTTPs is used to setup WSS protocol (RFC6455)
Network layers (Media):

HTTPs is used to setup HTTP Tunnel to TURN server
STUN is a protocol helper to check connectivity
TURN is a protocol helper to pass-through NAT/FW/HTTP Proxy
Call Flow:

Illustration of a Rainbow WebRTC Call
In this example, Client1 is in enterprise Lan, behind a NAT/FW/Web Proxy and will rely on TURN service to reach Client2. Client2 is behind a simple NAT (Home Gateway)

1. HTTPS/HTTP Connect https://openrainbow.com:443
2. Setting up TCP connection
3. HTTPS/HTTP Connection established
4. REGISTER Connection
5. HTTPS/HTTP Connect https://openrainbow.com:443
6. Setting up HTTPS connection
7. HTTPS/HTTP Connection established
8. HTTP switching protocol
9. XMPP/IM Connection
10. REGISTER/HTTP Connect https://openrainbow.com:443
11. HTTPS Connection http://openrainbow.com:443
12. HTTP switching protocol NATS
13. XMPP/IM Connection
14. Make Audio/Video call to Client1
15. Get ICE Server
16. STUN/TURN Configuration
17. Get ICE Server
18. STUN/TURN Configuration
19. HTTP Connect
20. Setting up TCP connection
21. HTTPS/HTTP Connection established
22. TURN/TCP connection
23. TURN Allocate Request
24. TURN Allocate Error
25. TURN Allocate Request
26. TURN Allocate Success
27. TURN Create/Permission Request
28. TURN Create/Permission Success
29. TURN/TCP connection
30. TURN Allocate Request
31. TURN Allocate Error
32. TURN Allocate Request
33. TURN Allocate Success
34. TURN Create/Permission Request
35. TURN Create/Permission Success
36. STUN Binding Request
37. TURN Send
38. STUN Binding Request
39. STUN Binding Request
40. TURN Send
41. TURN Binding Request
42. TURN Binding Request
43. TURN Binding Request
44. TURN Binding Request
45. TURN Binding Request
46. TURN Binding Request
47. TURN Binding Request
48. TURN Binding Request
49. TURN Binding Request
50. TURN Binding Request
51. TURN Binding Request
52. TURN Binding Request
53. TURN Binding Request
54. TURN Channel/bind Request
55. TURN Channel/bind Success
56. TURN Channel
57. DTLS Handshake
58. TURN Handshake
59. TURN Handshake
60. TURN Handshake
61. TURN Channel
62. TURN Channel
63. TURN Channel
64. TURN Channel
65. TURN Channel
66. TURN Channel
67. TURN Channel
• Steps 1-9 : Clients1, behind HTTP Proxy, establish HTTPS sockets and Secured WebSockets (For XMPP) through the HTTP Proxy.

• Steps 10-13 : Clients2, behind simple NAT, establish regular HTTPS sockets and Secured WebSockets (For XMPP) directly to Rainbow Cloud Services.

• Step 14 : Client1 make an Audio/Video call to Client2

• Steps 15-18 : Client1 and Client2 retrieves ICE configuration (list of TURN servers)

• Steps 19-28 : Client1 allocates TURN resources (through HTTP Proxy)

• Steps 29-35 : Client2 allocates TURN resources (direct connection to TURN)

• Steps 36-49 : Client1 and Client2 perform STUN connectivity check for various options (in this example, we illustrate the case where direct STUN connectivity check would failed)

• Steps 50-53 : Client1 and Client2 have found a network path through the TURN server. They start to initiate the DTLS-SRTP handshake.

• Steps 54-55 : Client1 ask TURN to switch to Channel mode to optimize network bandwidth (reduce TURN header overhead).

• Steps 56-57 : DTLS-SRTP is established, Audio/Video media starts to flow between Client1 and Client2
6 Limitations, Restrictions and workarounds

6.1 HTTP Proxy

If an HTTP Proxy is configured and/or selected at OS level (fixed configuration, auto-detect, script, ...), by design, Browsers and Rainbow desktop client as well will always rely on this HTTP Proxy to reach Rainbow cloud services (for all protocols used, including HTTPS/REST, XMPP over Secured WebSockets and TURN). It could append that the proxy in place in enterprise is not able or is not willing to pass-through some protocols (TURN for example). Capability and willingness of the HTTP Proxy must be checked by IS/IT team in case of trouble to start Rainbow clients or to establish Audio/Video call between Enterprise Lan and external users.

End of Document