URN Media Relays

GETTING STARTED GUIDE

ALCATEL-LUCENT RAINBOWTM

Network Requirements

GETTING STARTED GUIDE Ed 31

May 2024

Author: Operations - Cloud Services

Alcatel·Lucent Enterprise

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.

Should you use this document to configure firewalls and proxies, please subscribe to updates on the helpcenter. Indeed, as Rainbow is growing, we must add new IPs, URLs and protocols when adding new servers, location, or features. In any case of addition, we will update this document 7 days before activating new servers and services to let you time to configure your edge security equipment.

Copyright

Contents

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

Rainbow by Alcatel-Lucent Enterprise (ALE) is an overlay cloud service operated by ALE. Rainbow offers contact management, presence, persistent messaging, audio/video for peer-to-peer and multiparty real-time collaboration, screen and file sharing, telephony services on existing customers PBX or based on native cloud telephony capabilities, and API openness to integrate with customers processes, applications and machines.

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

This document describes the high level principles of network flows implemented by the solution, provides detailed information on Rainbow network connectivity requirements, allowing network and security administrators to identify needed firewall rules, verify bandwidth availability, and tune intermediate security elements such as proxies when applicable.

Section 3.2 gives a short summary of requirements for readers who do not have advanced security infrastructure or rules in place, and don't need to dive into the details

2 Document History

Modifications (see last edition's changes in green)	**Date**	**Edition**
Addition of new public IP addresses/servers in US/EMEA/DE	21/05/2024	Ed31
Removal of Load Balancers public IP Addresses in EMEA: 79.137.65.42 54.36.121.125 178.32.173.187 178.33.89.143 51.254.93.113 217.182.178.97 54.38.162.128 54.38.162.129 54.38.162.130 176.31.24.80 176.31.24.81 176.31.24.82	26/03/2024	Ed30
Addition of new public IP addresses/servers in US/NAR, EMEA and DE regions Update of TURN servers Addition of Rainbow HUB wildcard for US	23/02/2024	Ed29
Add restriction about DHCP options for Rainbow Hub devices. Addition of new public IP addresses/servers in EMEA, DE, US and LATAM regions Update of TURN server in Bahrain Add 2 ports for Apple Push	08/12/2023	Ed28

Add Rainbow HUB wildcard		
Addition of new public IP addresses/servers in EMEA, DE and US region Update of conference servers in Germany Fix IP flows between WebRTC Gw and PBX with SIPTLS (4.6.2)	07/06/2023	Ed27
Update WebRTC Gw to PBX IP flows: Fix missing TCP/5060 port, and add TCP/5061 for topologies involving end-to-end encryption with OXE (section 4.6.2)	08/03/2023	Ed26
Removal of deprecated IPs in France and Brazil Change of 2 conferences servers IP/fqdn in France Disclaimer completed: subscribe to updates Addition of bandwidth information for large grid and adjusted bandwidth info for screen sharing DPI section augmented with PKI	29/11/2022	Ed25
Addition of media ports for Rainbow applications used for Rainbow Hub (section 3.2.3) Addition of media ports for Rainbow desktop and web client for Rainbow Hub (section 4.1) Addition of media ports Rainbow Android and iOS clients and associated SDKs for Rainbow Hub (section 4.1) Addtion of Rainbow Hub public IP for Israel and addition of Rainbow Hub public IP for Transfer zone (dedicated zone for partners that have a private links toward Rainbow Hub) Addition of new IPs for callback proxy Change of 1 conference server IP in Germany Addition of 3 conference servers IP in Brasil Addition of new IP block in Germany	29/07/2022	Ed24
Addition of a summary paragraph for required flows for collaboration, Hybrid and Hub (section 3.2) Updated on WebRTC Gateway (section 4.6): • more relevant repartition of flows towards Rainbow Cloud and towards LAN side components • update on DMZ topology with dual interface capability Add note on TTL for NAT mappings for Android app connection to Google FCM service (section 4.2) Add new conference server IP in China	Xx/04/2022	Ed 23
Updated section 5 with FQDN and IP addresses changes related to: • add Webrtc and Turn located in Middle East/Bahrain • New external load balancers IP for Singapore	04/02/2022	Ed22

WebRTC gateway: Add details on NAT configuration for UDP, deployment in the DMZ specificities and configuration of a DNS server is mandatory		
Add new media relay servers IPs and names to whitelist Add new file sharing DNS entries Add webinar DNS entry Add connectors (teams…) IPs Precision of HTTP version supported by WRG (HTTP 1.1)	03/11/2021	Ed 21
Updated to notify removal of conference server number 4 in Brazil, turn server in Washington DC and Load Balancer in Washington DC Addition of information for Teams and Google connectors Some fixes in WebRTC Gateway port ranges Some precisions on proxy dimensioning aspects Streamline document paragraph numbering	28/09/2021	Ed 20
Updated section 5.4 with FQDN and IP addresses changes related to: • Removal of now deprecated TURN SBG1 configuration • Updated DNS/IP information on mail servers.	04/03/2021	Ed 19
Updated section 5.4 with PBX Agent bandwidth	19/11/2020	Ed 18
Updates to cover Rainbow Room, Rainbow Hub, and refined information on video bandwidth after introduction of simulcast video	27/09/2020	Ed 17
Updated section 5.4 with FQDN and IP addresses changes related to: • turn.sbg1.openrainbow.com removal	28/07/2020	Ed 16
Updated section 5.4 with FQDN and IP addresses changes related to: • New ANZ region and associated servers • New EMEA load balancers servers	30/06/2020	Ed 15
Updated section 5.Edition4 with FQDN and IP addresses changes related to: • New EMEA TURN and Media Conferencing servers • EMEA TURN and Media Conferencing servers removal • New South America Media Conferencing servers • New DE Media Conferencing servers • DE Media Conferencing servers removal	21/04/2020	Ed 14
Updated section 5.4 with FQDN and IP addresses changes related to: • South America Load Balancer, TURN and Media Conferencing servers • Germany Load Balancer servers	11/07/2019	Ed 13

• Europe and North America mail servers • UK TURN and Media Conferencing servers (removal)		
Updated section 5.4 with complete list of public IP addresses Section 5.3.4: WebRTC Gw now supports crossing web proxy for media flows.	15/03/2019	Ed 12
Improve and complete IP flows information presentation; some doc reorg; precisions on bandwidth for mobile devices; new TURN server	10/01/2019	Ed 11
Extended WebRTC TURN endpoints configuration	11/14/2018	Ed 10
Video Bandwidth requirements update, WebRTC GW requirements and SDK specificities	05/17/2018	Ed 09
TURN endpoints update, bandwidth requirements update	04/07/2017	Ed 08
HTTP vs. HTTPS cleanup	04/04/2017	Ed 05
Minor change (legacy PBX Agent removed)	31/03/2017	Ed 04
Information on bandwidth added (chapter 6)	08/03/2017	Ed 03
Chapter modified	05/01/2017	Ed 02
Creation of document	27/10/2016	Ed 01

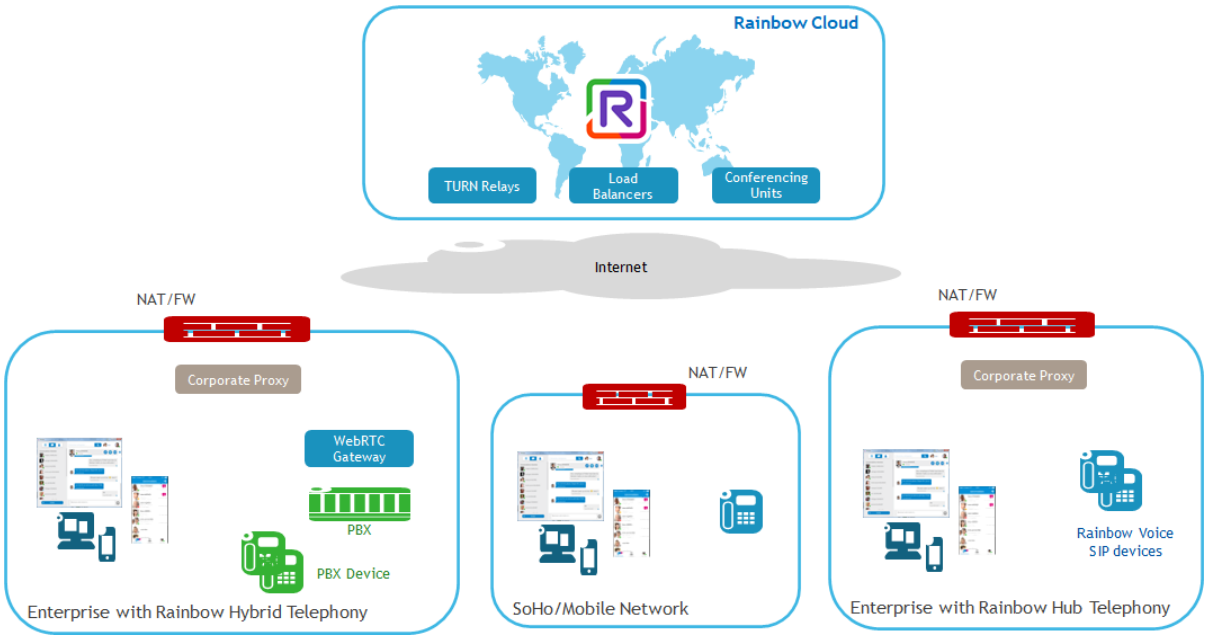
3 Solution Overview

3.1 Global Overview

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

- A Desktop application for Windows and OSX (Web-based, Electron-contained)
- A Web application for WebRTC compatible browsers
- An iOS native application
- An Android native application
- An Agent to connect customers' PBX for hybrid telephony (can be integrated with the PBX)
- A WebRTC Gateway to establish multimedia calls between customers' PBX and Rainbow
- Various SDKs allowing developers building client and server applications leveraging the Rainbow CPaaS capabilities (see https://developers.openrainbow.com)
- SIP devices are also supported in the context of the Rainbow Hub offer, in regions where it is available

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



3.2 Summary of ports/protocols requirements

This section provides the basic information on outgoing flows to enable for Rainbow to properly connect to Rainbow infrastructure. Details on the rationale and on the way the solution works are provided in further sections of the document.

1.1.1 Rainbow Collaboration

The table below gives minimum requirements for deployment of Rainbow as a collaboration solution, without telephony services.

Protocol	Port	Main use	Source	Destination [a]
TCP	443	Signaling, APIs Messaging, filesharing	All Rainbow clients and applications	*.openrainbow.com openrainbow.com openrainbow.io
UDP [b]	3478	Audio/video/desktop sharing media	All Rainbow clients	*.openrainbow.com
TCP [c]	5228-5229-5230	Android push notif	Pure wifi Android devices	Google FCM servers
TCP [d]	443, 5223, 2197	Apple push notif	Pure wifi iOS devices	Apple APNS servers

(a) details on FQDN and IP addresses of Rainbow servers are provided in section 5

(b) the solution can fall back on TCP/443 if the infrastructure does not allow UDP (UDP remains highly recommended for best quality of service for multi-media flows)

(c) Google requires that if the network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), a 30 minute or larger timeout is maintained for FCM connections over ports 5228-5230. Google Reference: https://firebase.google.com/docs/cloud-messaging/concept-options

(d) Apple reference: https://support.apple.com/en-ph/102266

1.1.2 Rainbow Hybrid Telephony

The table below gives minimum requirements for deployment of Rainbow on top of an existing customer PBX, providing telephony services and optionally advanced collaboration services.

Protocol	Port	Main use	Source	Destination [a]
TCP	443	Signaling, APIs Messaging, filesharing	All Rainbow clients and applications WebRTC Gateway PBX	*.openrainbow.com openrainbow.com openrainbow.io
UDP [b][c]	3478	Softphony with remote users	All Rainbow clients	*.openrainbow.com

		Audio/video/desktop sharing media for collaboration	WebRTC Gateway	
TCP [(d)]	5228-5229-5230	Android push notification	Rainbow on pure wifi Android devices	Google FCM servers
TCP [(e)]	443, 5223, 2197	Apple push notification	Rainbow on pure wifi ios devices	Apple APNS servers

(a) details on FQDN and IP addresses of Rainbow servers are provided in section 5

(b) the solution can fall back on TCP/443 if the infrastructure does not allow UDP (UDP remains highly recommended for best quality of service for multi-media flows)

(c) the NAT gateway implemented between the WebRTC Gateway and Rainbow must avoid too fast reuse of WAN ports. This can be achieved by implementing a 10mn timeout on NATed connection. See note of section 4.6.1 for details.

(d) Google requires that if the network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), a 30 minute or larger timeout is maintained by firewalls for FCM connections over ports 5228-5230. Google Reference: https://firebase.google.com/docs/cloud-messaging/concept-options

(e) Apple reference: https://support.apple.com/en-ph/102266

1.1.3 Rainbow Hub

The table below gives minimum requirements for deployment of the Rainbow Hub solution. The latter provides cloud telephony services and optionally advanced collaboration services.

Protocol	Destination Port	Main use	Source	Destination [(a)]
TCP	443	Signaling, APIs Messaging, filesharing	Rainbow applications	*.openrainbow.com openrainbow.com openrainbow.io
UDP	3478	Softphony Audio/video/desktop sharing media	Rainbow applications	*.openrainbow.com
TCP [(b)]	5228,5229,5230	Android push notif.	Rainbow on pure wifi Android devices	Google FCM servers
TCP [(c)]	443, 5223, 2197	Apple push notif.	Rainbow on pure wifi ios devices	Apple APNS servers

TCP	5061	SIP	SIP devices	*.openrainbow.com
TCP	443	Config and APIs	SIP devices	*.openrainbow.com
UDP	30000-44999	SRTP media	SIP devices Rainbow applications (softphony)	*.openrainbow.com
UDP	53	DNS	SIP devices	DNS server
UDP	123	NTP	SIP devices	pool.ntp.org

(a) details on FQDN and IP addresses of Rainbow servers are provided in section 5

(b) Google requires that if the network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), a 30 minute or larger timeout is maintained for FCM connections over ports 5228-5230. Google Reference: https://firebase.google.com/docs/cloud-messaging/concept-options

(c) Apple reference: https://support.apple.com/en-ph/102266

3.3 High-Level Principles and Flows

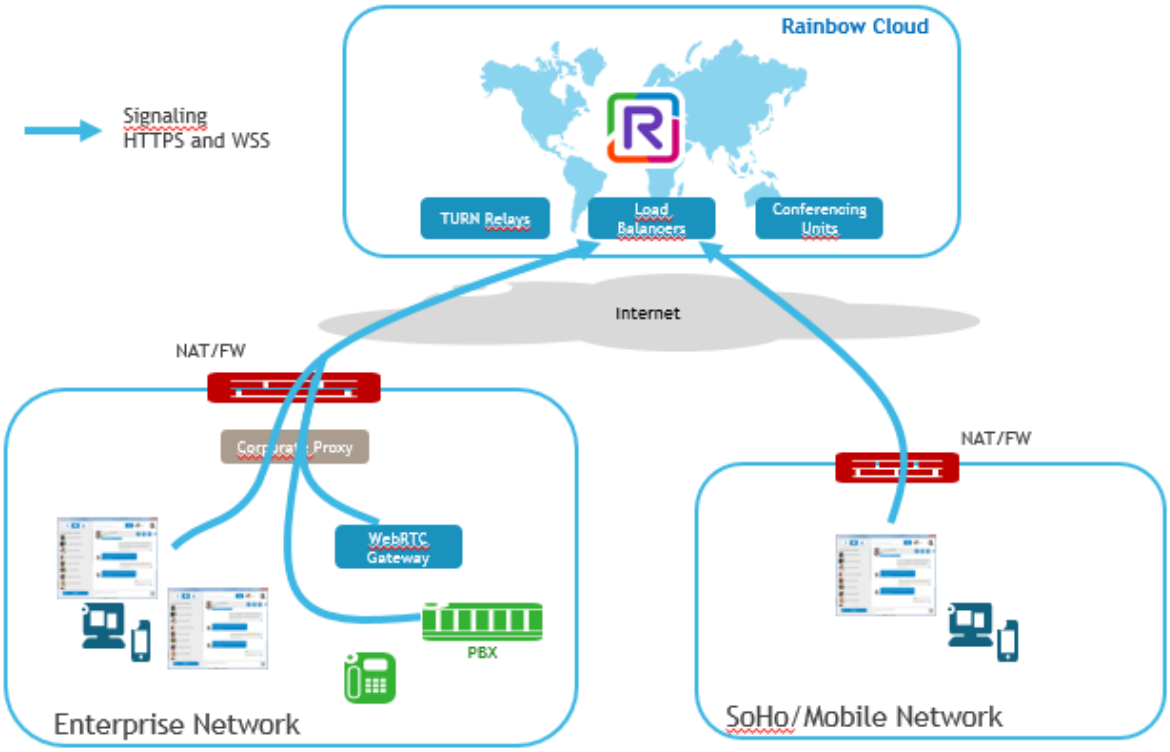
All applications aim at providing the same level of services and features and interact with server-side components for signaling and media. The basic principles are provided in this section, and a detailed list of protocols/ports in the following one.

3.3.1 Signaling for WebRTC calls

For signaling, HTTPS/REST and Secured Web Sockets protocols are used:

- HTTPS (443) for all REST API communications and resources loading.
- Secure Web Sockets (WSS, 443) for all XMPP messages and notifications.

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).



Full details on the involved ports are provided in the next sections.

3.3.2 WebRTC/Media

Media communications between two clients, or between client and server-side conferencing components, use the WebRTC technology with DTLS-SRTP protocol for encrypting audio, video and desktop sharing media. The solution leverages ICE mechanisms and Rainbow TURN relays to achieve connectivity thru NAT/Firewalls.

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:

- Each client gathers candidates addresses.
    - A candidate is a transport address, combination of IP address and port for a particular transport protocol, allocated on local interface (for example wired Ethernet interface or WiFi interface for a PC), and on TURN cloud relay server that are necessary to allow cross network communications. The Rainbow infrastructure ensures TURN servers are located in all regions for providing world-wide coverage, however for optimizing the number of candidates for a WebRTC communication, Rainbow clients are automatically using only the nearest two Rainbow TURN servers, based on their IP geo-localization.
- The client exchanges candidates with the distant peer (other client or conferencing unit),

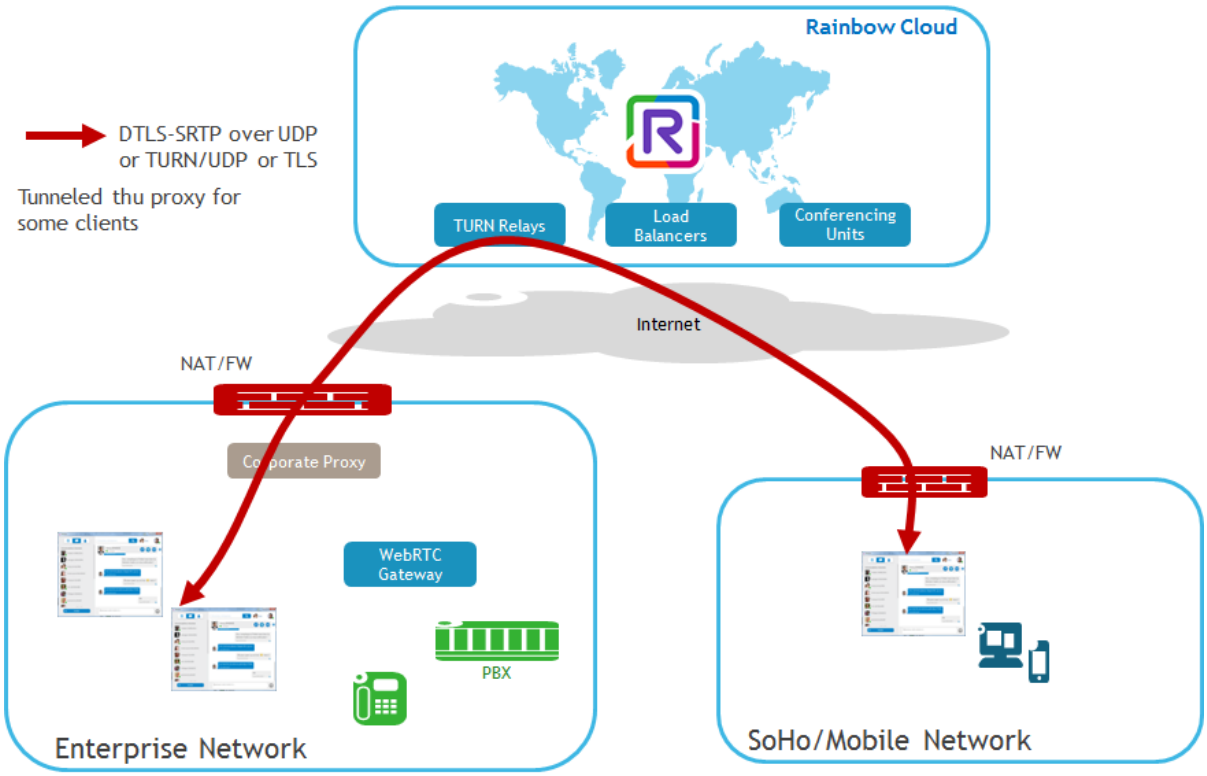
- Clients then check connectivity for candidates between both clients and select the most optimized working pair.

In case network conditions loss/change during an established communication, the network path for media is automatically renegotiated on-the-fly thru the above ICE mechanisms, allowing to keep communication active with only a small media interruption (no more than a few seconds max for device to change network connection and Rainbow WebRTC stack to perform re-negotiation). This typically happens in case of Wi-Fi/3G-4G handover for mobile devices, or network connectivity change on computer (wired to Wi-Fi connection).

Example1: P2P WebRTC between local client (Enterprise network) and Remote client (external to the Enterprise network)

In such a case, a direct connection is not possible and the communication is generally achieved by leveraging a TURN server, acting as a cloud relay for routing media. It is reminded here that TURN relays are simple traffic redirectors, and have no access to the relayed media that remains encrypted end-to-end between peers.

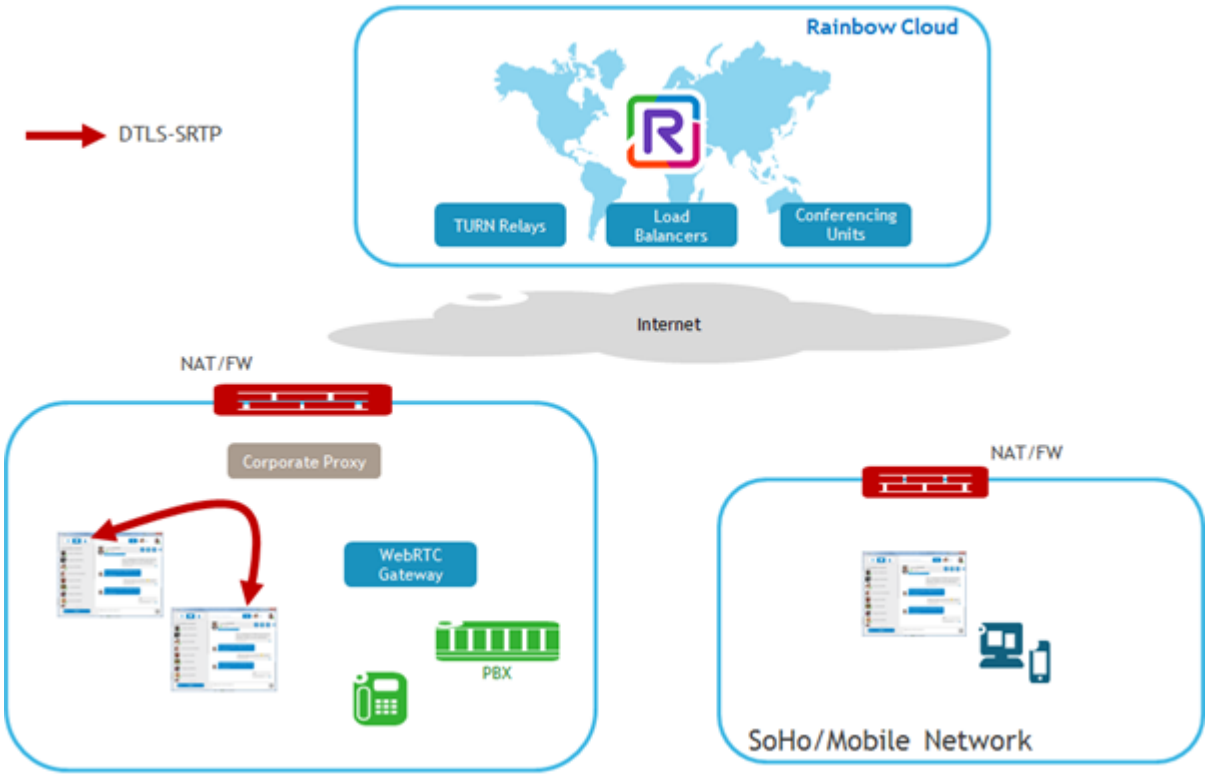
As illustrated below, in case a proxy is used on the enterprise network, the connection to the TURN servers, and consequently the media, can be tunneled thru the proxy for some Rainbow clients (see details in section 4).



Note: to simplify figures, only one TURN server is illustrated. For a P2P communication, depending on geography and network performance, up to two TURN servers could be used to establish a communication (a different one for each client).

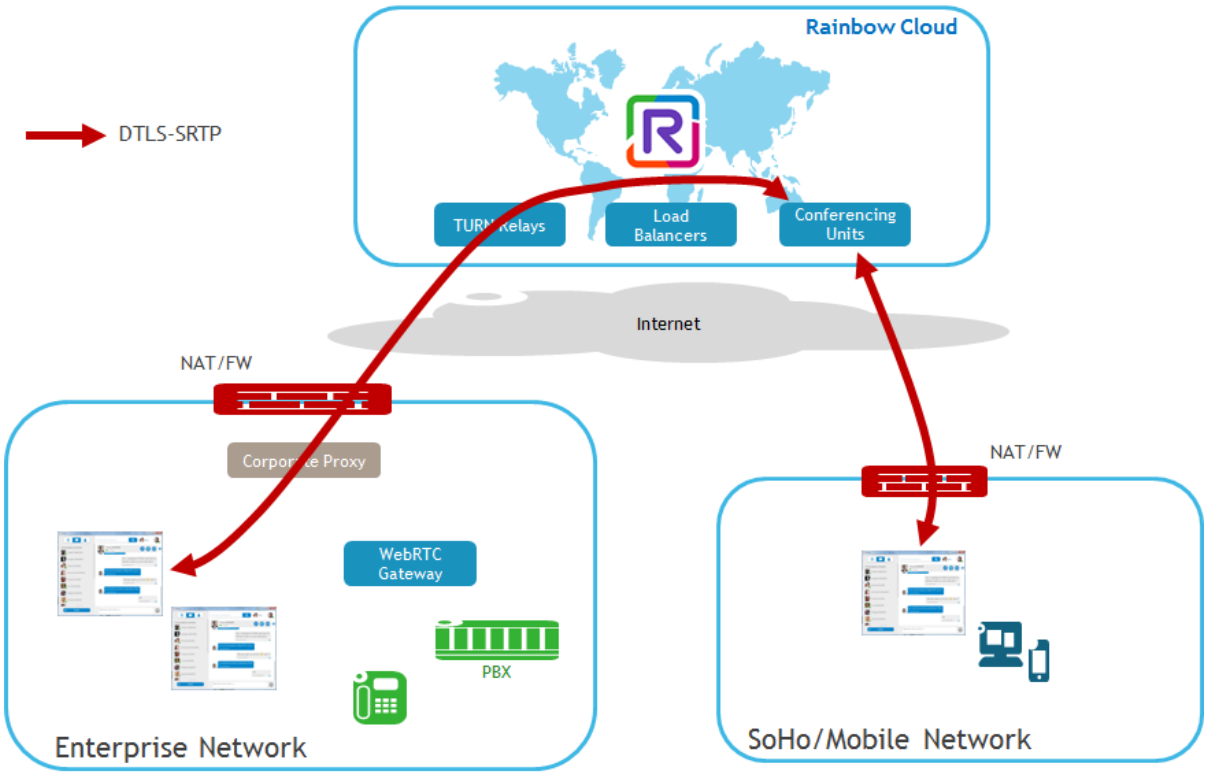
Example2: P2P WebRTC between two clients located on same LAN (Enterprise network)

In such a case, a direct connection is possible and the ICE negotiation results in clients choosing the direct path, as preferred path over the one going thru TURN.



Example3: Media with WebRTC Rainbow conference (Bubble)

When joining an Audio/Video Rainbow conference (bubble), clients connect to Rainbow cloud Conferencing Unit. Depending on the type of network infrastructure (Firewall/NAT type) on client side, clients either join the conferencing unit directly, or by getting relayed thru a TURN server, typically if UDP is not allowed directly between endpoints and the conferencing unit.

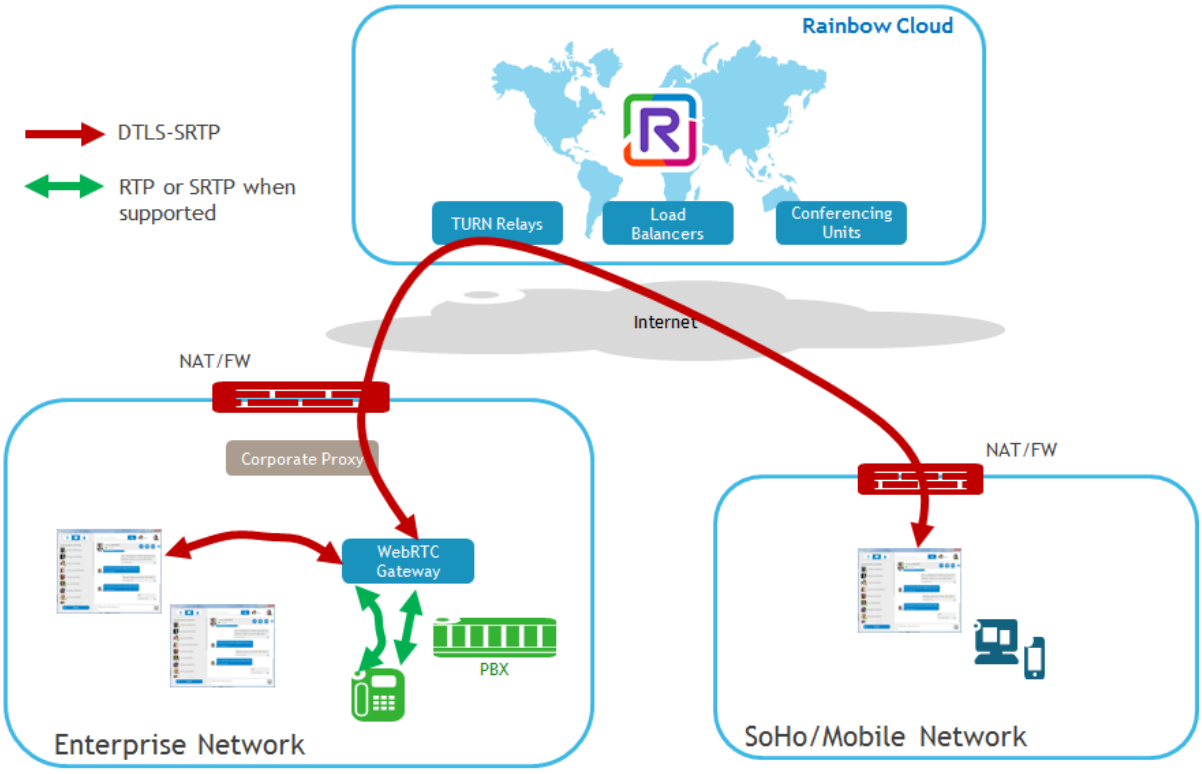


3.3.3 WebRTC for Hybrid Softphony calls

In hybrid mode, PBX telephony calls placed or taken with Rainbow clients also use the WebRTC technology and principles described in the above section, where one end of the WebRTC media call is the WebRTC Gateway. The latter acts as gateway between the Rainbow client used for the softphone call, WebRTC being used between Rainbow client and Gateway, whereas the gateway interfaces with the PBX in SIP and with PBX devices in RTP.

As for previous examples, the media path depends on whether the WebRTC Gateway and the Rainbow client are located on a same network and can therefore have a direct connection between each other. If this connection is possible, the call is direct between the WebRTC Gateway and the Rainbow application. If no direct connectivity exists, then the call is relayed thru a TURN server.

The two scenarios are depicted below.



3.3.4 Rainbow Hub

Rainbow Hub is a full cloud telephony and UC offer, rendering services on SIP devices connected directly to Rainbow cloud infrastructure, as well as on Rainbow clients, and applications built on top on Rainbow APIs. Traffic to/from the public network is enabled thanks to partner-provided SIP trunks, connected on the Rainbow backend.

Telephony services come in addition to other UCaaS and CPaaS services which network flows are already described in previous sections.

Specific flows are the ones involving SIP endpoints, that rely on the following secure protocols:

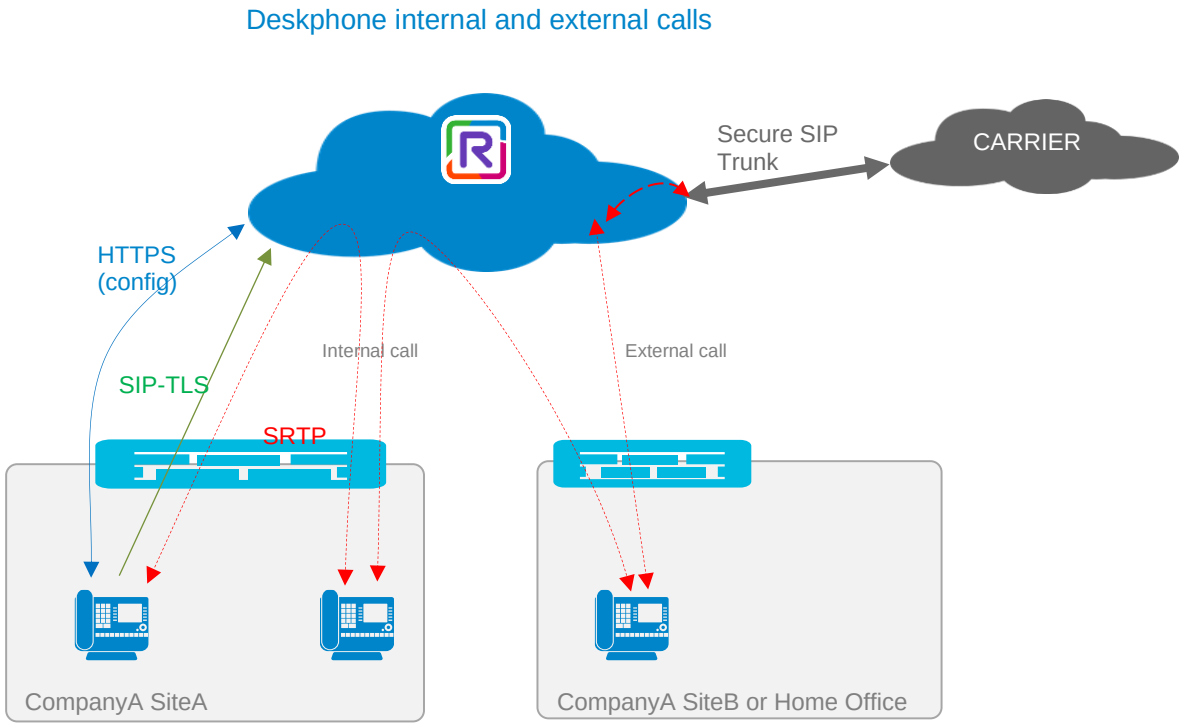
- HTTPS for automated configuration retrieval and firmware updates, for devices which are fully managed by Rainbow
- SIP-TLS for signaling towards Rainbow SIP cloud entry points
- SRTP for media

All flows are initiated from the devices towards Rainbow, removing the need to open any incoming port. All used protocols are compatible with NAT.

The main scenarios are illustrated hereafter.

Call scenarios with SIP devices

As depicted below, managed SIP devices automatically connect to Rainbow cloud to get their configuration and firmware updates from Rainbow, using HTTPS protocol. Phones are automatically recognized by Rainbow, after digital certificate and MAC address verification. All HTTPS requests are outgoing from SIP devices to Rainbow.



The configuration file contains the SIP parameters that then allow SIP devices to register to the platform through the nearest SIP entry point, and consequently establish the signaling link based on SIP-TLS. The SIP-TLS link is always to the initiative of the device and maintained permanently with the Rainbow back-end thanks to keepalive traffic sent over the SIP-TLS connection.

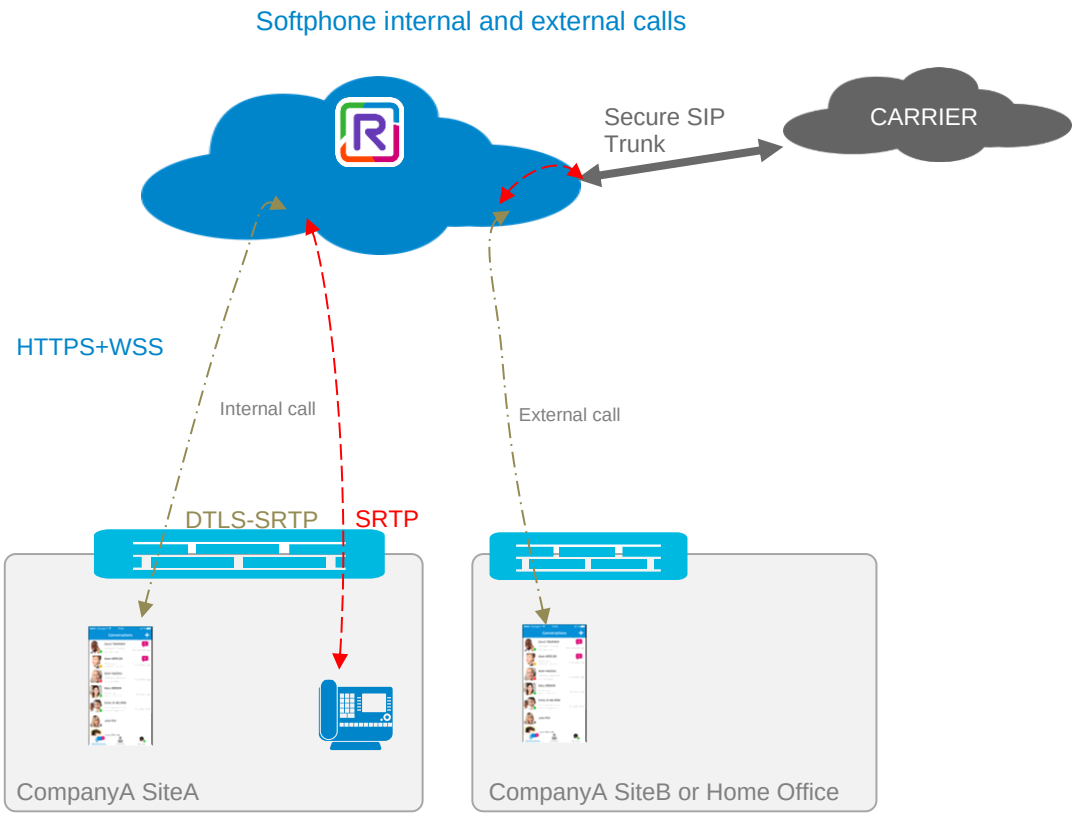
Calls are always established using SRTP protocol (RFC3711), relayed thru the Rainbow platform. The solution automatically adapts to NAT and uses the connection initiated by the device through the remote firewall/NAT component if any, to exchange media flows in both directions.

Call scenarios with Rainbow clients

Rainbow desktop/web and mobile clients can be used as softphone, to place and receive telephony calls to/from local or external extensions through the Rainbow Hub infrastructure.

Rainbow clients keep relying on WebRTC technology for these scenarios, and on the principles and protocols described in section 3.3.2.

When interacting with SIP devices or with an external extension through the SIP trunk, the mediation between WebRTC/DTLS-SRTP and SIP-TLS/SRTP is managed by the Rainbow infrastructure.



4 Detailed List of used Protocols and Ports

4.1 Rainbow Desktop and Web clients and Web SDK

Note that IP flows are always at the initiative of the clients, so no inbound firewalls rules from Internet to the enterprise network are needed.

The following connections take place between Rainbow client/Agent and Rainbow Cloud Services, possibly going thru a proxy if one is configured on the computer.

Protocols	Source	Destination	HTTP Proxy Compatibility
Signaling and APIs (mandatory)			
HTTPS **(Resources and REST API. Apps updates)**	**Rainbow client** OS dynamic port range (see 5.3.5)	**Rainbow servers,** TLS/443	**Yes**
Secure Web Sockets - WSS **(XMPP)**	**Rainbow client** OS dynamic port range	**Rainbow servers,** TLS/443	**Yes**
Pure WebRTC Audio/Video/ScreenSharing			
DTLS-SRTP for Peer-to-Peer WebRTC comm on same LAN **(Rainbow clients have direct connectivity between each-other)**	**Rainbow client** OS dynamic port range	**Peer Rainbow client** UDP OS dynamic port ranges	Not applicable (such flows remain on LAN)
DTLS-SRTP for Peer-to-Peer WebRTC comm thru Internet	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443 TCP/80 (see note1) (see note3)	**Yes**, requesting proxy to connect to TURN servers via ports TLS/443 and TCP/80 (see note1&2)
DTLS-SRTP to Rainbow WebRTC Conference servers	**Rainbow client** OS dynamic port range	**Rainbow conference servers** UDP port range UDP/49152-65535 As fallback if outgoing	**Yes**, requesting proxy to connect to TURN servers via ports TLS/443 and TCP/80 (see note1&2)

		UDP range is not opened: **Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443 TCP/80 (see note1)	
Hybrid Softphony (on ALE OXE/OXO/OTEC or supported 3d party PBX)			
DTLS-SRTP for Softphone call when the app is on LAN and can reach the WebRTC Gateway	**Rainbow client** OS dynamic port range	**WebRTC Gateway** UDP 20000-29999	Not applicable (such flows remain on LAN)
DTLS-SRTP for Softphone call when the app is not on same LAN as WebRTC Gateway	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443 TCP/80 (see note1) (see note3)	**Yes**, requesting proxy to connect to TURN servers via ports TLS/443 and TCP/80 (see note1&2)
Rainbow Hub Softphony			
DTLS-SRTP for Softphone call	**Rainbow client** OS dynamic port range	**Rainbow Cloud PBX** UDP 30000-44999	No, proxy case is addressed via use of TURN server (line below)
DTLS-SRTP for Softphone call	**Rainbow client** OS dynamic port range	*If above UDP range not opened or in case of proxy use* **Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	**Yes**, requesting proxy to connect to TURN servers via ports TLS/443 and TCP/80 (see note1&2)

Note1: Firefox does not correctly support TURN-TLS thru proxy at present time, ie version 64 for this document edition. TCP-80 is offered as a workaround, and port 80 must therefore be opened in firewalls for outgoing traffic when Firefox is being used thru a proxy. It is reminded that the usage of port TCP-80 does not imply clear media traffic. This port is only used as transport channel to the TURN server, and the applicative flow conveyed over it is encrypted end-to-end with DTLS-SRTP

Note2: DPI compatibility. The connection between a browser and the TURN Server, using TCP-80 or TCP-443 ports, are not using HTTP protocol beyond the HTTP CONNECT allowing the proxy to open the tunnel, but STUN/TURN and DTLS-SRTP protocols. In case Deep Packet Inspection is applied on the customer network and expects to examine HTTP traffic, exception rules must be applied for traffic to Rainbow TURN IP addresses, so the DPI gear allows this legitimate Rainbow TURN connections without attempt for intermediate decryption neither HTTP inspection.

Note3: The firewall will actually see tentative traffic to other destinations/ports, but the above table only lists the minimum required ports for ensuring correct functional behavior with less possible opened rules. Indeed, ICE connectivity checks, as described in 3.3.2, test all possible combinations of IP/ports between the local client and the remote peer candidates. As each peer generally provides candidates with local address (LAN), public relayed address (exposed at a TURN Server), and reflexive address (corresponding to their Internet access gateway), STUN connectivity checks are exchanged between all possible pairs, some being between the WebRTC Gateway and any possible remote IP address and port, which would be enabled by opening a firewall rule towards <any>/<any> IP/port tuple. Only allowing traffic to the TURN server avoids opening such a wide rule. It results in part of the connectivity checks to fail (the ones targeted at the peer reflexive address for example) but ensures that a media path is always found via a rainbow TURN server.

4.2 Rainbow Android and iOS clients and associated SDKs

The flows involved with mobile clients are similar to the ones used by computer apps, at the exception of proxy compatibility for media, and of the push notification channel required for users to properly receive incoming events (IM, call) when the app is not in foreground.

Proxy settings are inherited from device network configuration.

Protocols	Source	Destination(s)	HTTP Proxy Compatibility
Signaling and APIs (mandatory)			
HTTPS **(Resources and REST API)**	**Rainbow client** OS dynamic port range (see 5.3.5)	**Rainbow servers,** TLS/443	**Yes**
Secure Web Sockets - WSS **(XMPP)**	**Rainbow client** OS dynamic port range	**Rainbow servers,** TLS/443	**Yes**
Apple Push Notification **(iOS App)**	**Rainbow device** OS dynamic port range	**APNS** TCP/5223 TCP/2197 TCP/443 (*)	**No** If the ports are not opened on the firewall, the app automatically falls back to mobile data network if such connectivity is available For WiFi-only mobile devices, the IS/IT must open firewall rules to allow direct outgoing traffic to Push Notification ports
Google FCM Push Notification **(Android app)**	**Rainbow device** OS Dynamic port range	**Google FCM servers** TCP/5228-5229-5230 (**) TCP/443	
Pure WebRTC Audio/Video/ScreenSharing			
DTLS-SRTP for Peer-to-Peer WebRTC comm on same LAN (Rainbow clients have direct connectivity between each-other)	**Rainbow client** OS dynamic port range	**Peer Rainbow client** UDP OS dynamic port ranges	Not applicable (such flows remain on LAN)
DTLS-SRTP for Peer-to-Peer WebRTC comm	**Rainbow client** OS dynamic port	**Rainbow TURN Servers** using several connectivity alternatives:	**No**, proxy not supported for media If ports are blocked on

thru Internet	range	UDP/3478 TLS/443 (note3)	the firewall, the app automatically falls back to mobile data network if such connectivity is available For WiFi-only mobile devices, the IS/IT must open UDP/3478 and/or TLS/443 to Rainbow Servers
DTLS-SRTP to Rainbow WebRTC Conference servers	**Rainbow client** OS dynamic port range	**Rainbow conference servers** UDP port range UDP/49152-65535 As fallback if outgoing UDP range is not opened: **Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	
Hybrid Softphony (on ALE OXE/OXO/OTEC or supported 3d party PBX)			
DTLS-SRTP for WiFi Softphone call when the app is on LAN and can reach the WebRTC Gateway	**Rainbow client** OS dynamic port range	**WebRTC Gateway** UDP 20000-29999	Not applicable (such flows remain on LAN)
DTLS-SRTP for Softphone call when the app is not on LAN as WebRTC Gateway	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443 (note3)	**No**, proxy not supported for media If ports are blocked on the firewall, the app automatically falls back to mobile data network if such connectivity is available For WiFi-only mobile devices, the IS/IT must open UDP/3478 and/or TLS/443 to Rainbow Servers
Rainbow Hub Softphony			
DTLS-SRTP for Softphone call	**Rainbow client** OS dynamic port range	**Rainbow Cloud PBX** UDP 30000-44999	NA
DTLS-SRTP for Softphone call	**Rainbow client** OS dynamic port range	*If above UDP range not opened*	**No**, proxy not supported for media If ports are blocked on the firewall, the app

		Rainbow TURN Servers using several connectivity alternatives: UDP/3478 TLS/443	automatically falls back to mobile data network if such connectivity is available For WiFi-only mobile devices, the IS/IT must open UDP/3478 and/or TLS/443 to Rainbow Servers

(*) reference: https://support.apple.com/en-ph/HT203609

(**) reference: https://firebase.google.com/docs/cloud-messaging/concept-options

Note the important requirement from Google for push notification delivery:

"If your network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), implement a 30 minute or larger timeout for our connections over ports 5228-5230. This enables us [Google] to provide reliable connectivity while reducing the battery consumption of your users' mobile devices"

(note3): see note3 of 4.1

4.3 Rainbow Teams and Google Connectors

Teams and Google connectors rely on Rainbow Web SDK and allow leveraging Rainbow Hybrid and Cloud telephony capabilities from within Microsoft and Google software suites. The network flows involved are identical to the ones of the Rainbow desktop/web, please refer to section 4.1.

4.4 Rainbow Room

Rainbow rooms are Android clients and therefore rely on the same flows as Android smartphones applications.

Protocols	Source	Destination(s)	HTTP Proxy Compatibility
Signaling and APIs (mandatory)			
HTTPS **(Resources and REST API)**	**Rainbow client** OS dynamic port range (see 4.8)	**Rainbow servers,** TLS/443	**Yes**
Secure Web Sockets - WSS **(XMPP)**	**Rainbow client** OS dynamic port range	**Rainbow servers,** TLS/443	**Yes**

Google FCM Push Notification **(Android app)**	**Rainbow device** OS Dynamic port range	**Google FCM servers** TCP/5228-5229-5230 (**)	**No** The IS/IT must open firewall rules to allow direct outgoing traffic to Push Notification ports
Pure WebRTC Audio/Video/ScreenSharing			
DTLS-SRTP for Peer-to-Peer WebRTC comm on same LAN (Rainbow clients have direct connectivity between each-other)	**Rainbow client** OS dynamic port range	**Peer Rainbow client** UDP OS dynamic port ranges	Not applicable (such flows remain on LAN)
DTLS-SRTP for Peer-to-Peer WebRTC comm thru Internet	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	**No**, proxy not supported for media The IS/IT must open UDP/3478 and/or TLS/443 to Rainbow Servers
DTLS-SRTP to Rainbow WebRTC Conference servers	**Rainbow client** OS dynamic port range	**Rainbow conference servers** UDP port range UDP/49152-65535 As fallback if outgoing UDP range is not opened: **Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	

4.5 PBX Agents

PBX agents, embedded in ALE PBX or deployed as external component for third party PBX, require connecting to Rainbow Cloud to deliver hybrid telephony services. As for other Rainbow CPE components, all flows are initiated from PBX Agent to Rainbow cloud, avoiding opening any incoming firewall pinholes from Internet to the corporate network.

The following table details IP flows required for the agent to connect to Rainbow servers.

Protocols	Source	Destination(s)	HTTP Proxy Compatibility

Secure Web Sockets - WSS	**PBX Agent** PBX dynamic port range	**Rainbow servers,** TLS/443	**Yes**
DNS	**PBX Agent**	**DNS Server** (*) UDP/53	**No**

(*) The DNS server, generally located on corporate network, is required to resolve Rainbow server names.

4.6 WebRTC gateway

In hybrid softphony configurations with ALE PBX or supported 3d party PBX, the WebRTC Gateway acts as a bridge enabling media communications between Rainbow WebRTC clients and telephony extensions reached thru a PBX. It is deployed on the same network as the PBX.

Important: The configuration of a DNS server in the WebRTC Gateway is mandatory, even if only IP addresses are used. This limitation is linked to some internal components that will perform a reverse DNS query before the usage of the proxy.

4.6.1 WebRTC gateway to Rainbow Cloud

The following table details the flows involved between the WebRTC Gateway and other Rainbow components on Cloud side

Protocols	Source	Destination	HTTP Proxy Compatibility
HTTPS **(Resources and REST API)**	**WebRTC Gw** OS dynamic port range (see 4.8)	**Rainbow servers,** TLS/443	**Yes**
Secure Web Sockets - WSS **(XMPP)**	**WebRTC Gw** OS dynamic port range	**Rainbow servers,** TLS/443	**Yes**
ICE/TURN(s) **Media Connectivity Checks**	**WebRTC Gw** UDP 20000-29999	**Rainbow TURN Servers** UDP/3478***	**Yes*** Requesting proxy to connect to TURN servers via port TCP/80 by default, when mpmproxy command is used. Use of TLS/443 is possible for specific

			cases**
DTLS-SRTP for Peer-to-Peer WebRTC comm thru Internet	**WebRTC Gw** UDP 20000-29999	**Rainbow TURN Servers** UDP/3478***	**Yes*** Requesting proxy to connect to TURN servers via port TCP/80 by default, when mpmproxy command is used. Use of TLS/443 is possible for specific cases**

** the WebRTC Gateway supports HTTP proxy for media since version 1.71, by having the admin use the mpmproxy command so proxy is used instead of direct connection to TURN UDP/3478. Note that a direct connection to TURN servers, using UDP, remains the recommended way for Voice quality reasons, as it avoids TCP-related retransmissions if the network experiences packet loss. **Connection via proxy requires the proxy to implement HTTP version 1.1***

*** Using TCP/80 is the default because the channel to the TURN only conveys DTLS-SRTP encrypted media. Therefore TCP/80 avoids double encryption which impacts performances and may affect QoS. Proxying to TURN servers on TLS/443 is supported as a workaround for proxies or policies that may not allow proxying to TCP/80, but impacts the number of simultaneous communications the component can support*

**** The firewall will actually see tentative traffic to other destinations/ports, but the above table only lists the minimum required ports for ensuring correct functional behavior with less possible opened rules. Indeed, ICE connectivity checks, as described in 3.3.2, test all possible combinations of IP/ports between the local client and the remote peer candidates. As each peer generally provides candidates with local address (LAN), public relayed address (exposed at a TURN Server), and reflexive address (corresponding to their Internet access gateway). STUN connectivity checks are exchanged between all possible pairs, some being between the WebRTC Gateway and any possible remote IP address and port, which would be enabled by opening a firewall rule towards <any>/<any> IP/port tuple. Only allowing traffic to the TURN server avoids opening such a wide rule. It results in part of the connectivity checks to fail (the ones targeted at the peer reflexive address for example) but ensures that a media path is always found via a rainbow TURN server.*

Important : Concerning NAT configuration, the NAT gateway must be configured so the source port used at the WAN side is not reused too quickly for a subsequent call. This can be achieved either by implementing a static NAT/PAT logic (1 to 1 source port between WRG and NAT gateway) or by ensuring the port range of the NAT gateway is wide enough and with cyclic allocation, or that a TTL of at least 10 minutes is configured for traffic towards TURN servers UDP/3478.

4.6.2 WebRTC Gateway flows to PBX and local devices/clients

Besides these flows with the Rainbow ecosystem, the WebRTC Gateway communicates with the PBX ecosystem on the LAN. The flows are described hereafter in case firewalling is applied between WebRTC Gw and the LAN side.

Protocols	Source	Destination
SIP (when NO encryption is	**WebRTC Gw** UDP/5060	**PBX (main IP address)**

configured between PBX and WRG)	TCP/5060	UDP/5060 TCP/5060
SIP (when NO encryption is configured between PBX and WRG)	**PBX (main IP Address)** UDP/5060 TCP/5060	**WebRTC Gw** UDP/5060 TCP/5060
SIP-TLS (when encryption is configured between PBX and WRG)	**WebRTC Gw** TCP/dyn	**PBX (main IP Address)** TCP/5061
SIP-TLS (when encryption is configured between PBX and WRG)	**PBX (main IP Address)** TCP/dynamic	**WebRTC Gw** TCP/5061
(S)RTP Media **(SRTP if encryption is enabled on PBX ecosyst)**	**WebRTC Gw** UDP 30000-40000	**PBX Gateway and SIP Trunk SBC** UDP port range (*)
(S)RTP Media **(SRTP if encryption is enabled on PBX ecosyst)**	**PBX Gateway and SIP Trunk SBC** UDP port range (*)	**WebRTC Gw** UDP 30000-40000
(S)RTP Media **(SRTP if encryption is enabled on PBX ecosyst)**	**WebRTC Gw** UDP 30000-40000	**IP Phones** UDP port range (*)
(S)RTP Media **(SRTP if encryption is enabled on PBX ecosyst)**	**IP Phones** UDP port range (*)	**WebRTC Gw** UDP 30000-40000
WebRTC Media	**WebRTC Gw** UDP 20000-29999	**LAN side Rainbow clients** UDP OS dynamic port range (*)
WebRTC Media	**LAN side Rainbow clients** UDP OS dynamic port range (*)	**WebRTC Gw** UDP 20000-29999
DNS (**)	**WebRTC Gw** UDP/1024-65535	**DNS server** UDP/53
NTP	**WebRTC Gw** UDP/123	**NTP server** UDP/123

SSH ***If enabled***	**SSH client**	**WebRTC Gw** TCP/22

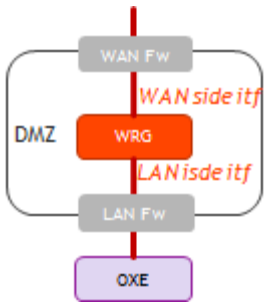
(*) please refer to IP Flows PBX documentation on BPWS, for precisions on gateway and devices port ranges.

(**) The configuration of a DNS server in the WebRTC Gateway is mandatory to resolve Rainbow servers FQDN, even in configurations relying on a proxy. This constraint is linked to some internal components that will perform a reverse DNS query before the usage of the proxy.

4.6.3 WebRTC gateway in the DMZ

The WebRTC Gateway supports being deployed in a DMZ. It is however not a security border element, and must therefore be protected by firewalls, and must not be directly exposed on the Internet.

To allow segmenting the flows from WAN and LAN side on different subnets within the DMZ, a second interface can be optionally activated on the WebRTC Gateway.



Should the WebRTC Gateway be deployed in a DMZ, make sure the following requirements are addressed:

- NAT is not supported between the WebRTC Gateway and the PBX or devices, so no NAT between the DMZ and the LAN
- Internal and external firewall must allow all necessary traffic as detailed in the above sections, more specifically
    - The WAN side firewall must enable all outgoing traffic as described in 4.6.1
    - The LAN side firewall must enable all flows detailed in 4.6.2

4.7 Rainbow Hub ALE SIP devices

This section lists the flows required for SIP devices to connect to Rainbow. It is only relevant in the context of the Rainbow Hub Offer.

Note: ALE SIP terminals do not support crossing HTTP proxy currently

Protocols	Source	Destination

SIP over TLS	**Desk phones** TCP/5061	**Rainbow Cloud PBX** TCP/5061
HTTPS	**Desk phones** OS Dynamic range	**Rainbow Device Discovery Service** TCP/443
SRTP Media	**Desk phones** UDP 30000-40000	**Rainbow Cloud PBX** UDP 30000-44999
DNS	**Desk phones** OS Dynamic range	**DNS server** UDP/53
NTP	**Desk phones** OS Dynamic range	**NTP server pool.ntp.org** UDP/123
SSH ***If enabled***	**SSH client**	**Desk phones** TCP/22
HTTPS	**HTTPS client**	**Desk phones** **TCP / 443**

Important note: The IP phone can obtain IPv4-related parameters in an IPv4 network via DHCP option. If the device receives a specific device management URL in option 43, 66 or 67, it will break the Rainbow Hub zero touch mechanism as the DHCP option will take precedence. It is recommended to disable these options in the DHCP server for Rainbow Hub deployments. If it is not possible to disable it, the device management given by the DHCP server must be https://rdd.openrainbow.com.

4.8 OS Dynamic port range

As complement to the info provided in the previous sections, the table below reminds the current default dynamic/ephemeral ports ranges used by the different operating systems Rainbow clients can run on. These ports are allocated by the OS and Rainbow apps have no control over this selection.

Supported Platforms	Dynamic Port Range (UDP and TCP)
Windows	49152-65535
MacOS	49152-65535
iOS	49152-65535
Android (>=7)	37000-50000
Linux WebRTC Gw	32768-60999

5 Rainbow Domains and IP addresses

This section lists the domains and IP addresses used for the Rainbow generic worldwide service.

For specific cases involving Rainbow Edge deployments, the principles described in the first part of the document apply, but domains and IP might differ. Please contact support if domains information is required for a specific Rainbow Edge.

To simply your firewall configuration, please consider allowing all subdomains of openrainbow.com and create a rule allowing any connection to *.openrainbow.com (wildcard). As alternative, you'll find below the current list of services and domains.

Used by	Purpose	Domains
Rainbow Clients	Resources (website, images, client package, Agent package, …)	web.openrainbow.com cdn.openrainbow.com meet.openrainbow.com webinar.openrainbow.com
Rainbow Clients/SDK	REST API	openrainbow.com
Rainbow Clients/SDK	XMPP over Secured WebSockets	openrainbow.com
Teams/Google and ITSM/CRM connectors	Resources and APIs *(in addition to all domains used by Rainbow clients/SDK)*	*.openrainbow.io (wildcard)
Developper Hub	Documentations and SDKs	hub.openrainbow.com

Used by	Purpose	Domains
Rainbow Clients/SDK	STUN/TURN	turn-*.openrainbow.com (wildcard) turn-bhs1.openrainbow.com (Canada) turn-cap1.openrainbow.com (South Africa) turn-bhr1.openrainbow.com (Bahrain) turn-bhr2.openrainbow.com (Bahrain) turn-che1.openrainbow.com (India) turn-dal1.openrainbow.com (US West) turn-lim1.openrainbow.com (Germany) turn-lim2.openrainbow.com (Germany) turn-lim3.openrainbow.com (Germany) turn-lim4.openrainbow.com (Germany) turn-rbx1.openrainbow.com (France) turn-rbx2.openrainbow.com (France) turn-sao1.openrainbow.com (Brazil) turn-sao2.openrainbow.com (Brazil) turn-sgp1.openrainbow.com (Singapore) turn-sjc1.openrainbow.com (US West) turn-syd1.openrainbow.com (Australia) turn-tok1.openrainbow.com (Japan) turn-vin1.openrainbow.com (US East) turn-vin2.openrainbow.com (US East) turn-vin3.openrainbow.com (US East) turn-dli2.myopenrainbow.cn.com (China)

Rainbow Clients/SDK	WebRTC conferences (for reverse DNS only)	rtc-*.openrainbow.com (wildcard) rtc-sbg1.openrainbow.com rtc-sbg2.openrainbow.com rtc-sbg3.openrainbow.com rtc-sbg4.openrainbow.com rtc-sbg5.openrainbow.com rtc-sbg6.openrainbow.com rtc-sbg7.openrainbow.com rtc-sbg8.openrainbow.com rtc-sbg9.openrainbow.com rtc-sbg10.openrainbow.com rtc-bhs1.openrainbow.com rtc-bhs2.openrainbow.com rtc-bhs3.openrainbow.com rtc-bhs4.openrainbow.com rtc-bhs5.openrainbow.com rtc-bhs6.openrainbow.com rtc-bhs7.openrainbow.com rtc-bhs8.openrainbow.com rtc-bhs9.openrainbow.com rtc-bhs10.openrainbow.com rtc-bhs11.openrainbow.com rtc-bhs12.openrainbow.com rtc-cap1.openrainbow.com rtc-bhr1.openrainbow.com rtc-gra2.openrainbow.com rtc-gra5.openrainbow.com rtc-gra6.openrainbow.com rtc-gra7.openrainbow.com rtc-gra8.openrainbow.com rtc-gra9.openrainbow.com rtc-gra10.openrainbow.com rtc-gra11.openrainbow.com rtc-gra12.openrainbow.com rtc-gra13.openrainbow.com rtc-gra14.openrainbow.com rtc-gra15.openrainbow.com rtc-gra16.openrainbow.com rtc-gra17.openrainbow.com rtc-gra18.openrainbow.com rtc-gra19.openrainbow.com rtc-gra20.openrainbow.com rtc-gra21.openrainbow.com rtc-gra22.openrainbow.com rtc-gra23.openrainbow.com rtc-gra24.openrainbow.com rtc-gra25.openrainbow.com rtc-gra26.openrainbow.com rtc-lim4.openrainbow.com rtc-lim5.openrainbow.com rtc-lim6.openrainbow.com rtc-lim7.openrainbow.com rtc-lim8.openrainbow.com rtc-lim9.openrainbow.com

		rtc-lim10.openrainbow.com rtc-lim11.openrainbow.com rtc-lim12.openrainbow.com rtc-lim13.openrainbow.com rtc-lim14.openrainbow.com rtc-lim15.openrainbow.com rtc-lim16.openrainbow.com rtc-lim17.openrainbow.com rtc-lim18.openrainbow.com rtc-lim19.openrainbow.com rtc-lim20.openrainbow.com rtc-lim21.openrainbow.com rtc-lim22.openrainbow.com rtc-lim23.openrainbow.com rtc-lim24.openrainbow.com rtc-lim25.openrainbow.com rtc-lim26.openrainbow.com rtc-lim27.openrainbow.com rtc-lim28.openrainbow.com rtc-lim29.openrainbow.com rtc-lim30.openrainbow.com rtc-lim31.openrainbow.com rtc-lim32.openrainbow.com rtc-rbx5.openrainbow.com rtc-rbx6.openrainbow.com rtc-rbx7.openrainbow.com rtc-rbx8.openrainbow.com rtc-rbx9.openrainbow.com rtc-rbx10.openrainbow.com rtc-rbx11.openrainbow.com rtc-rbx12.openrainbow.com rtc-rbx13.openrainbow.com rtc-rbx14.openrainbow.com rtc-rbx15.openrainbow.com rtc-rbx16.openrainbow.com rtc-rbx17.openrainbow.com rtc-rbx18.openrainbow.com rtc-rbx19.openrainbow.com rtc-rbx20.openrainbow.com rtc-rbx21.openrainbow.com rtc-rbx22.openrainbow.com rtc-rbx23.openrainbow.com rtc-rbx24.openrainbow.com rtc-rbx25.openrainbow.com rtc-rbx26.openrainbow.com rtc-rbx27.openrainbow.com rtc-rbx28.openrainbow.com rtc-rbx29.openrainbow.com rtc-rbx30.openrainbow.com rtc-rbx31.openrainbow.com rtc-rbx32.openrainbow.com rtc-rbx33.openrainbow.com rtc-rbx34.openrainbow.com rtc-rbx35.openrainbow.com

Used by	Purpose	Domains
		rtc-rbx36.openrainbow.com rtc-rbx37.openrainbow.com rtc-rbx38.openrainbow.com rtc-sao4.openrainbow.com rtc-sao5.openrainbow.com rtc-sao6.openrainbow.com rtc-sgp1.openrainbow.com rtc-syd1.openrainbow.com rtc-vin1.openrainbow.com rtc-vin2.openrainbow.com rtc-vin3.openrainbow.com rtc-vin4.openrainbow.com rtc-vin5.openrainbow.com rtc-vin6.openrainbow.com rtc-vin7.openrainbow.com rtc-vin8.openrainbow.com rtc-vin9.openrainbow.com rtc-vin10.openrainbow.com rtc-vin11.openrainbow.com rtc-vin12.openrainbow.com rtc-vin13.openrainbow.com rtc-vin14.openrainbow.com rtc-vin15.openrainbow.com rtc-vin16.openrainbow.com
Rainbow Clients/SDK	File sharing	files-*.openrainbow.com (wildcard) files-bhs.openrainbow.com files-lim.openrainbow.com files-sao.openrainbow.com files-sbg.openrainbow.com files-sgp.openrainbow.com files-syd.openrainbow.com files-us.openrainbow.com
PBX agent	PBX connection to Rainbow	agent.openrainbow.com
WebRTC GW	PBX media connection to Rainbow	As for Rainbow clients
Node Cli and SDKs in development mode	Sandbox connections for applications development tests	sandbox.openrainbow.com web-sandbox.openrainbow.com
Mail Server	For mails sent from Rainbow	smtp.openrainbow.com mail.openrainbow.com ms-*.openrainbow.com (wildcard) ms-sbg-2.openrainbow.com ms-bhs-2.openrainbow.com
SIP Desk phone for Rainbow Hub	Device discovery service used for firmware update, provisioning	rdd.openrainbow.com

Used by	Purpose	Domains
SIP Desk phone for Rainbow Hub	Signaling and media to establish calls	*.eu1.sip.openrainbow.com (wildcard) *.latam1.sip.openrainbow.com (wildcard) *.apac1.sip.openrainbow.com (wildcard) *.na1.sip.openrainbow.com (wildcard)

Nota: It is highly recommended that customers always use FQDNs, Rainbow servers IP addresses being subject to change. In the unfortunate event that using or whitelisting DNS entries is not an option, the table below references all public IP addresses used by the various Rainbow services. Please keep in mind that this map is subject to change and can be updated at any time without any further notice. Also keep in mind that due to the multiple high-availability and failover mechanisms in place, both at DNS and application levels, it is mandatory to whitelist all the IP addresses aforementioned, including those in regions and geographies that might not be explicitly those intended by end customer.

Services	Region / Country	Associated IP Addresses
Misc services *Those IPs can be dynamically associated to any below services, eg: load balancers, media relay, and decreases the number of changes needed on customer firewalls when Rainbow infrastructure changes*	North America / Canada	54.39.227.80/28
	North America / US	135.148.197.0/26
	South America / Brazil	
	Europe / France	5.135.82.192/28 51.75.103.64/27 51.178.224.224/27
	Europe / Germany	51.68.163.112/28 5.135.97.96/28 162.19.180.112/28
	Asia / Singapore	46.105.162.176/28
	Asia / China	
	Oceania / Australia	
Main Load Balancers	North America	142.4.216.72 167.114.175.31 167.114.135.97 149.56.179.10 144.217.123.252 169.44.201.2 144.217.133.89 51.81.53.158 51.81.59.212 144.217.125.221 144.217.129.224 144.217.129.233 144.217.139.14 144.217.139.32 144.217.139.44
	South America	169.57.207.27
	Europe	178.32.125.32 178.32.125.46 178.32.125.56 178.32.125.107 178.32.125.135 178.32.125.149 178.32.125.161 178.32.125.168 178.32.125.241 178.32.126.16 178.32.126.70 178.32.126.94 178.32.126.97 178.32.126.147 178.32.126.196 178.32.126.210 178.32.126.211

		178.32.126.251 178.32.127.14 178.32.127.42 178.32.127.143 178.32.127.144 178.32.127.183 178.33.40.217
	Germany	54.36.108.169 51.38.111.143 51.89.55.153e 54.37.95.41 51.195.21.111
	Asia	139.99.122.102 139.99.122.99 139.99.2.105 139.99.4.245 139.99.4.244 139.99.83.81 139.99.83.82 169.38.94.246 169.56.128.9 169.56.36.238
	Oceania	139.99.148.135 139.99.161.35 139.99.177.193 139.99.212.212 139.99.212.213 139.99.212.214
TURN Media Relays	North America / US West	169.44.201.11
	North America / US Central	169.46.173.182
	North America / US East	135.148.197.1
	North America / Canada	149.56.18.31
	South America / Brazil	169.57.174.104
	Europe / France	5.135.139.27 87.98.130.28
	Europe / Germany	162.19.180.114 162.19.180.113 51.195.68.2 51.195.1.23
	Asia / India	42.202.135.10
	Asia / Singapore	139.99.120.111
	Asia / China	54.153.56.183

	Asia / Japan	169.56.36.231
	Oceania / Australia	139.99.148.99
	Africa / South Africa	13.244.169.230
	Middle East / Bahrain	15.184.158.216 157.175.244.247
Conferencing Media Servers	North America / Canada	144.217.75.16 66.70.164.123 66.70.170.25 66.70.170.34 66.70.170.35 66.70.170.205 66.70.207.235 66.70.164.2 144.217.179.168 66.70.164.84 66.70.170.28 66.70.207.209
	North America / US East	51.81.70.131 51.81.61.47 135.148.199.92 135.148.199.93 135.148.199.90 135.148.199.91 135.148.199.94 135.148.199.95 135.148.199.96 135.148.199.97 135.148.199.98 135.148.199.99 15.204.13.228 51.81.232.190 51.81.224.231
	South America / Brazil	169.57.174.108 169.57.174.105 169.57.174.110
	Europe / France	51.178.179.102 51.178.178.88 51.178.89.220 51.178.89.227 178.33.41.97 178.33.41.118 178.32.113.41 87.98.190.141 188.165.40.236 188.165.32.173 87.98.184.126 87.98.188.47 188.165.32.179 188.165.40.199

		188.165.36.82 188.165.38.22 87.98.186.100 213.251.163.116 178.33.151.75 178.33.151.72 178.32.160.73 188.165.187.83 178.33.151.74 178.33.43.5 178.33.252.101 176.31.78.57 178.32.181.14 178.33.129.119 94.23.104.132 188.165.124.66 46.105.164.41 94.23.188.26 178.33.134.107 188.165.124.64 188.165.124.67 178.32.13.1 178.32.13.2 178.32.113.157 178.32.106.141 178.32.116.183 178.32.117.70 178.32.111.240 178.32.115.136 178.32.113.191 178.32.116.101 178.32.108.79 178.32.114.250 178.32.104.245 178.32.114.56 178.32.107.241 178.32.113.83 178.32.106.248 178.32.116.5 178.32.116.254 178.32.116.147 87.98.184.126 178.32.114.241 178.32.113.111
	Europe / Germany	158.177.103.120 158.177.103.124 54.37.207.198 54.37.95.19 54.37.95.21 54.38.152.232 54.38.220.89 54.38.221.163 51.38.107.53

		51.38.107.47 51.38.120.122 54.37.206.227 51.75.84.235 51.75.157.38 54.38.220.221 54.37.95.17 54.37.95.18 54.37.95.16 54.37.95.20 51.89.1.152 51.38.121.160 51.89.124.29 51.89.124.22 51.89.95.97 51.38.117.99 51.75.84.169 51.75.84.149 51.89.121.223 51.38.104.132 54.37.194.109 51.89.95.80 51.195.67.96 51.195.32.12 51.195.68.28
	Asia / Singapore	139.99.122.114
	Asia / China	42.202.135.11 42.202.135.29
	Oceania / Australia	139.99.247.11
	Africa / South Africa	13.244.170.205
	Middle East / Bahrain	15.184.244.239
Mail	North America / Canada	54.39.227.85
	Europe / France	51.178.224.244
Cloud PBX (Rainbow Hub)	Europe / Germany	5.135.97.100
	Europe / Germany (sip trunk over private link)	217.182.180.193
	EMEA / Israel	109.226.50.177
	South America / Brazil	169.55.63.254
	Asia / Singapore	51.79.245.155
	North America / Canada	144.217.133.90
Device discovery service	Europe / France	51.254.93.113 217.182.178.97 178.32.125.241

(Rainbow Hub SIP devices)		178.32.126.196 178.32.125.56 178.32.125.149 54.38.162.130 176.31.24.82 162.19.180.120
	Europe / Germany	51.195.55.209
	Oceania / Australia	139.99.177.193 139.99.212.214
	Asia / Singapore	139.99.2.105 139.99.83.81
	North America / Canada	135.148.197.19 135.148.197.17
Connectors endpoints	World Wide	141.94.145.96/28
Rainbow callback proxy	World Wide	178.33.41.118

6 Bandwidth requirement

6.1 WebRTC for Rainbow peer-to-peer calls and multiparty conferences

Rainbow WebRTC communication currently rely on the following codecs:

WebRTC P2P:

- OPUS for audio
- VP8 or H.264 for Video and Screen Sharing

WebRTC Conference:

- OPUS for audio
- VP8 for Video and Screen Sharing

These WebRTC codecs are able to dynamically throttle both their resolution and bitrates, depending on network performance observed.

Peer to peer (P2P) WebRTC communications video resolution is 720p.

For Rainbow video conferences, Rainbow clients allows users to decide the way they want to see other participants video, ending up with different possible views:

- Active talker only: 1 high resolution 720p video displayed (if bandwidth permits). If screensharing is done in parallel, the active talker video is displayed in lower resolution
- Active talker with additional thumbnails: 1 high resolution 720p video (if bandwidth permits), and 180p videos for thumbnails[(1)]. If screensharing is done in parallel, the active talker video is also displayed in lower resolution. Web/Desktop application supports up to 5 thumbnails, 7 for Rainbow Room. This mode is not supported on mobile/tablet apps.

- Grid view with up to 12 videos for Web/Desktop or Room, and up to 6 for mobile applications): lower resolution (360p or 180p)[(1)] video streams (depending on network conditions)
- Large grid: 1 high resolution 720p video stream displaying up to 49 participants (the video composition is built on Rainbow server side for large grid)

The logic to manage different video resolutions relies on a simulcast technique. In upstream direction, depending on the available bandwidth and on server-side instructions, clients send up to 3 different video streams in different resolutions, enabling remote applications to subscribe to the most appropriate and optimized stream according to the selected view (active talker full screen, thumbnails or grid). Sending simulcast streams is currently only supported by Web/Desktop application, but all applications implement the selection of the appropriate stream on receiver end.

The following table provides maximum bandwidth requirement per media, from the perspective of a Rainbow application. Note that Rainbow sets an upper limit to the bandwidth consumed for video in 720p, 360p and 180p to respectively 800 kbps, 300 kbps and 100 kbps, except for large grid and sharing where the upper limit is set to 2Mbps

Media Type	Maximal Bandwidth	Average Bandwidth	Lowest Bandwidth	Comment
Audio (bi-directional)	100 kbps	40kbps	15kbps	
Screen Sharing (upstream for person who shares, downstream for others)	2 Mbps (1080p)			Depends on screen motion figures here are max
Video p2p (bi-directional assuming the two person show their video)	P2P all Clients: 800 Kbps (720p)			actual bandwidth depends on network conditions, figures here are max
Video Conference Downstream direction	**Active talker-only view**: 800 Kbps (720p) **Act talk + thumbnails**: 800Kbps (720p) + N*100kbps (180p)[(1)] *(max N = 5 for web/desk, 7 for Room, N/A mobiles)* **Grid view**: 12 * 100 kbps (180p)[(1)] **Large Grid**: 2Mbps			actual bandwidth depends on network conditions, figures here are max
Video Conference	Video upstream for Web/Desktop: 1.2 Mbps (720p+360p+180p)			actual bandwidth depends on

Upstream direction	Video upstream for Mobile/Room: 800 Kbps (720p)(2) Sharing upstream: 2Mbps (1080p)	network conditions, figures here are max

(1) if video is originated from an app that does not support simulcast, max video thumbnail is 720p rather than 180p

(2) to allow users to limit the used bandwidth on mobile devices where data plans are expensive, a parameter can be set to limit the video bandwidth (480p instead of 720p for upstream video, and downstream video throttled to 500 kbps)

6.2 Hybrid softphony calls

Business calls made or taken from CPE PBX and through the WebRTC gateway use G711 or G722 codecs for audio.

These codecs run at 64 kbps rate, which with addition of UDP and IP headers leads to 87.5kps.

It is reminded that real-time voice media is sensitive to the network quality, and that a good quality communication with G711 requires:

- One-way latency to be maximum 150ms
- Jitter to be maximum 30ms
- Packet loss to be maximum 1%

6.3 Rainbow Hub Softphony calls

Telephony calls placed or received with the Rainbow application to a SIP device or to PSTN, currently use G711 for media.

This codec runs at 64 kbps rate, leading to 87.5 kbps with UDP and IP headers.

It is reminded that real-time voice media is sensitive to the network quality, and that a good quality communication with G711 requires:

- One-way latency to be maximum 150ms
- Jitter to be maximum 30ms
- Packet loss to be maximum 1%

6.4 PBX Agent traffic

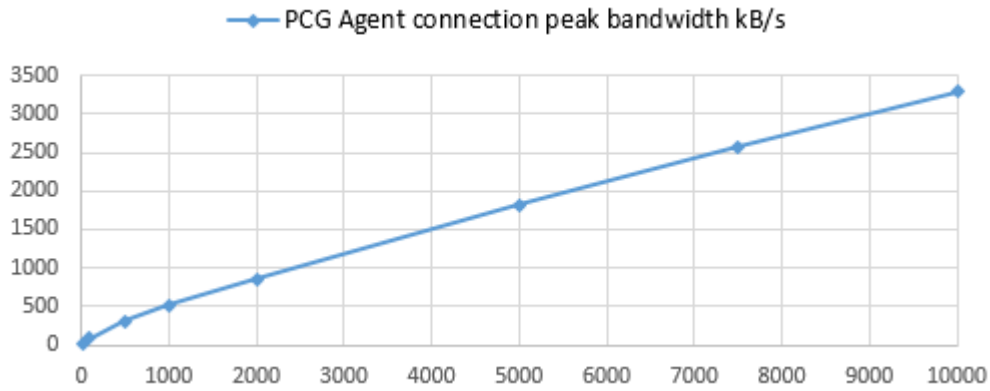
The PBX Agent acts as a CTI gateway between a local CPE PBX and the Rainbow Cloud, handling the following exchanges:

Connection to Rainbow Cloud

involving phonebook synchronization, as well as CTI monitoring initiation and phone state synchronization. This exchange takes place when the PBX Agent is started as well as when reconnecting following a broken connection due to an issue along the path.

The connection incurs a substantial burst of messages lasting anywhere from less than 1 second to 10 seconds depending on the number of PBX subscribers subject to Rainbow monitoring, whose rate is characterized in the following table:

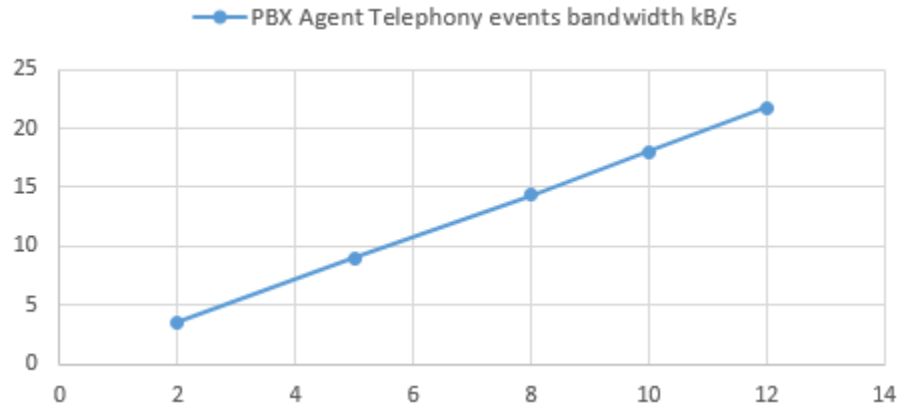
# subscribers	20	100	500	1000	2000	5000	7500	10000
Connection Peak bandwidth kB/s	26	80	304	510	850	1818	2696	3294



Telephony events

Once connected, CSTA telephony events flowing in both directions in 1pcc or 3pcc contexts. The level of traffic here is directly proportional to call activity initiated on PBX side from endpoints or external inbound calls, or initiated from a Rainbow client in 3pcc mode. As such, this bandwidth is much lower than connection bursts, characterized as a function of the overall number of calls per second in busy hour rather than number of subscribers alone.

Calls / second	2	5	8	10	12
BHCA	7200	18000	28800	36000	43200
Bandwidth kB/s	3.5	9	14.4	18	21.7



Notes:

- The figures above are given in kilobytes per second, not kbps.
- The peak bandwidth is based on measurements conducted in real conditions from an enterprise site benefiting from an enterprise-grade WAN connection to the Rainbow Cloud with low latency, high bandwidth capacity. Actual WAN connections and/or local concurrent traffic may restrict the bandwidth available to the PBX Agent connection without consequence except for a longer time to connect.
- The peak bandwidth indicated here only accounts for the burst mostly induced by the phonebook synchronization. This burst is followed by a lower rate of CSTA exchanges to initiate the monitoring of devices, which for large PBXs can take several minutes for the connection to be fully operationnal.
- The simultaneous connection or reconnection of several PBX Agents cumulates the overall bandwidth requirements indicated here, possibly up to the common link capacity. If only one or some PBX Agents are to reconnect at the same time while others remain connected, the peak bandwidth requirement must be cumulated with the current telephony events traffic generated by already connected PBX Agents.
- The figures may be linearly interpolated to the actual number of subscribers.

7 Configuration of border elements in enterprise

7.1 DNS, Firewall, Proxy configuration

To allow Rainbow to operate properly, border elements like DNS, HTTP Proxy or Firewall must be configured to allow resolving accessing domains and protocols listed in the table of chapter 4 and 5.

7.2 HTTP Proxy and DPI

If an HTTP Proxy is configured on the device where Rainbow applications are running, Rainbow Web and Desktop clients always rely on this HTTP Proxy to reach Rainbow cloud services (for all protocols used, including HTTPS/REST, XMPP over Secured Web Sockets and TURN). Mobile application use the proxy for signaling, but media has to be enabled directly or by fallback on mobile data network (see chapter 4.2).

In case Deep Packet Inspection is implemented by proxy/firewall, some exceptions have to be configured for Rainbow, according to the Note of 4.1:

> *The connection between Rainbow clients or WebRTC Gateway and the TURN Servers, using TCP-80 or TCP-443 ports, are not using HTTP protocol beyond the HTTP CONNECT allowing the proxy to open the tunnel, but STUN/TURN and DTLS-SRTP protocols.*
>
> *In case Deep Packet Inspection is applied on the customer network and expects to examine HTTP traffic, exception rules must be applied for traffic to Rainbow TURN Servers, so the DPI policy allows this legitimate Rainbow TURN connections without attempt for intermediate decryption neither HTTP inspection.*

DPI exception can be applied on *.openrainbow.com.

In case the DPI solution also scrutinizes PKI authorities for SSL connections, it must be noted that the connection between the PBX and Rainbow uses a dedicated PKI based on an ALE certification authority. This CA is used solely for the connection of the PBX to the domain agent.openrainbow.com. This method allows optimizing the serviceability for PBX connection to Rainbow and is based on a

fully secured PKI management practice by ALE. However, this authority won't be authorized by default by the DPI element. The solution is therefore to either whitelist agent.openrainbow.com so the CA is not checked by the DPI, or to install the ALE CA on the DPI gear. In the latter case please contact Rainbow support.

If must also be verified that the proxy is properly dimensioned, so it supports the number of simultaneous ports inferred by Rainbow usage:

- For signaling and APIs, each Rainbow client uses a permanent WSS towards Rainbow servers, and can perform parallel HTTPS requests for resources and APIs calls
- In addition to this, each WebRTC call via the proxy (ie involving a remote user) consumes additional ports for audio and video and sharing (one each in conference). Calls can be generated from Rainbow clients, and from the WebRTC gateway (possibly several hundred of simultaneous audio calls, refer to WebRTC Gateway capacity in TBE067 available on business partner web site)

Note finally that HTTP version 1.1 must be supported and used by the proxy, typically for the WebRTC Gateway to properly allow connecting to TURN server when a proxy is used.

End of Document