Business Talk IP for Alcatel-Lucent Enterprise OXO Connect & OXO Connect Evolution

versions addressed in this guide : 6.x

Information included in this document is dedicated to customer equipment (IPBX, TOIP ecosystems) connection to Business Talk & BTIP service : it shall not be used for other goals or in another context.

Latest edition: 02/04/2024

Table of contents

1. Goal of this document

The aim of this document is to list technical requirements to ensure the interoperability between Alcatel-Lucent Enterprise OXO Connect IPBX with Business Talk IP services from Orange Business, hereafter so-called “BTIP”.

2. Certified architectures

2.1. Introduction to architecture components and features

This document describes “only” the main supported architectures either strictly used by our customers or that are used as reference to add specific usages often required in enterprise context (specific ecosystems, multi-codec and/or transcoding, recording…)

Concerning fax communications, Orange supports the following usage :

- fax servers connected to the IPBX -and sharing same dial plan-, or as sperate ecosystems -and separate dial plan-
- analog fax machines, usually connected on specific gateways* (seen as IPBX ecosystem or not)

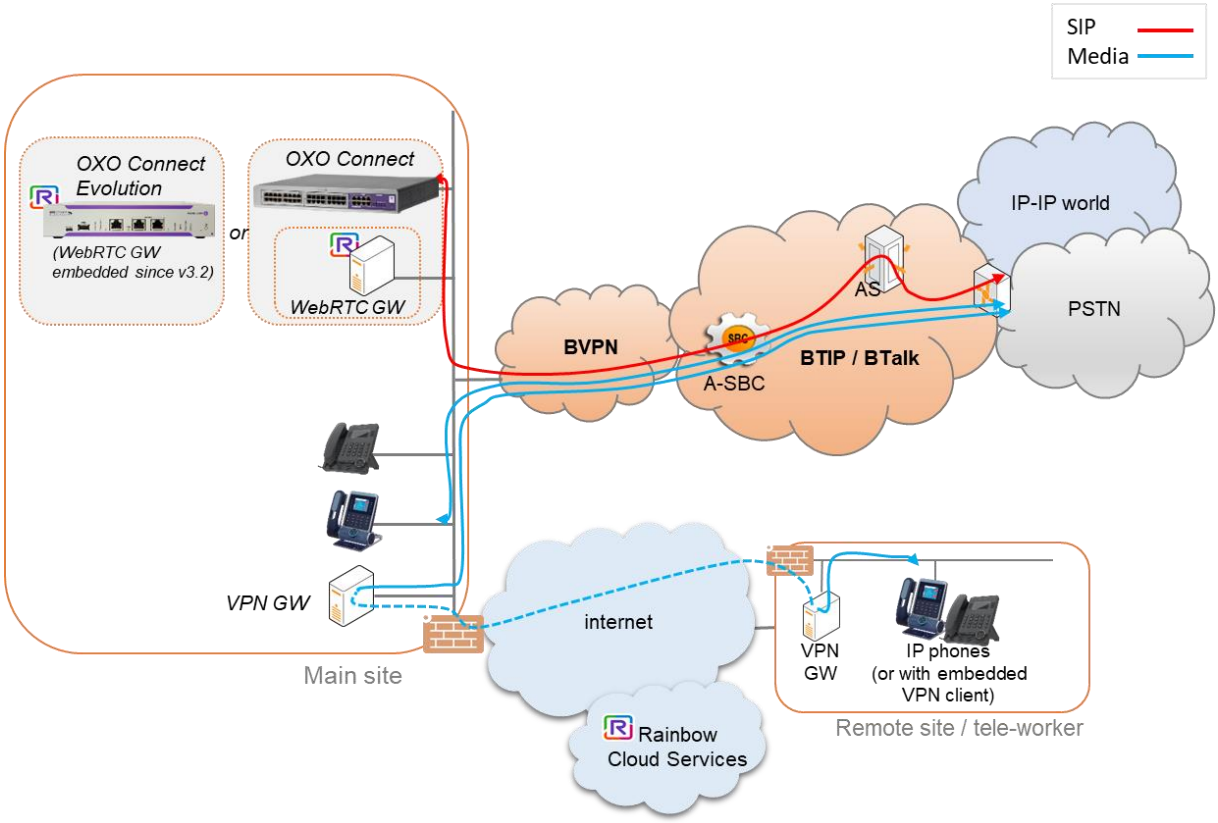
Fax flows are handled through BTIP via T.38 transport only.

Concerning the Quality of Service, Business VPN and BTIP networks trust the DSCP (Differenciated Services Code Point) values sent by customer voice equipment. That’s why Orange strongly recommends to set the IPBX, IP phones and other voice applications with a DiffServ/TOS value = 46 (or PHB value = EF) at least for media.

‘BTIP DROM’ architectures are now supported. Dedicated BTIP aSBC pairs have been installed in Caribbean and Indian Ocean zones for local calls. For a trunking point of view, the mechanism is similar to ‘Business Talk French customers’, the IPBX must support international dial plans and route local calls to the dedicated aSBC pair.

*T38 relay mode is not supported by OXO Connect PowerCPU and IPBox, that’s why **only faxes directly connected to analog ports of PowerCPU version are supported** with BTIP.

2.2. Architecture over BVPN



Notes :
In the diagram above, an offnet call from/to main site and an offnet call from/to a remote site or remote are displayed as example. Proprietary and Rainbow internal flows are hidden.

In this architecture :

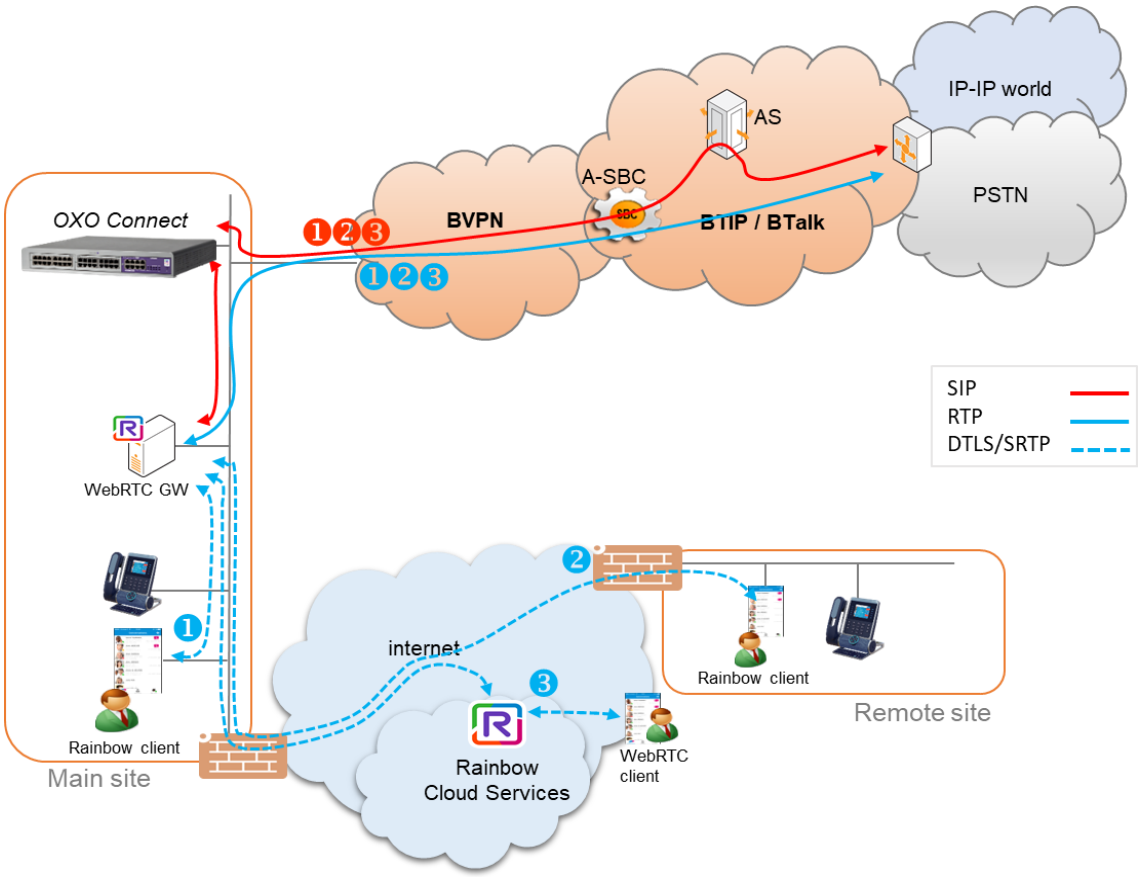
- all SIP signaling flows are carried by the OXO Connect and routed on the main BVPN connection.
- Media flows are direct between endpoints and BTIP but IP routing differs from one site to another:
  - For the main site site, media flows are routed to the BVPN router,
  - For remote sites, media flows are routed through the main site and a secured link (VPN or IPSEC over internet).

Here below a table with a few examples about sizing elements :

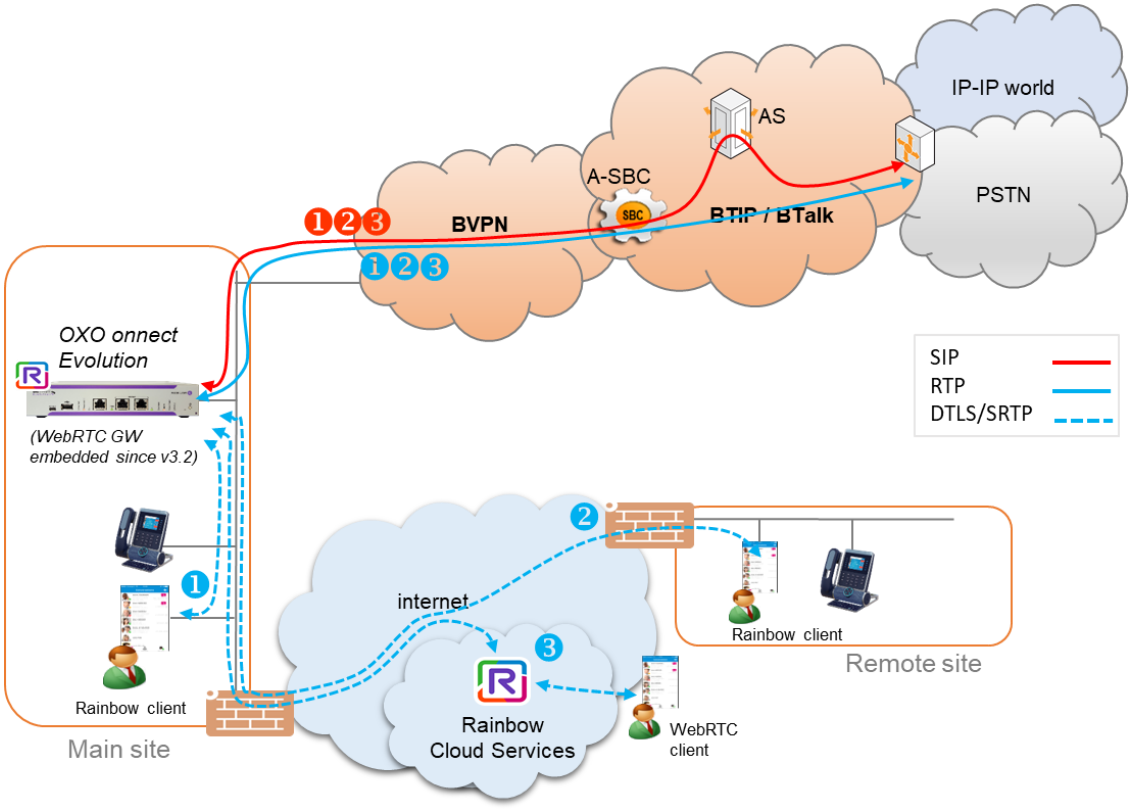
Call scenario	nb of voice channels/media resources used		
	IPBX*	WAN router**	BTIP
1 offnet call from/to the head quarter (HQ)	**1**	**1** in HQ	**1** in HQ
1 offnet call from/to a remote site (RS)	**1**	0 in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site **with put on hold**	**2**	**1** in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site **after transfer/forward to BTIP**	0	0 in HQ **0** in RS	0 in HQ **2** in RS
1 **forced onnet** call **from head quarter to a remote site** (= through Business Talk infrastructure)	**2**	**1** in HQ **1** in RS	**0** in HQ **0** in RS

*global CAC for the BTIP SIP trunk **on the WAN router, 1 voice channel = 80Kb/s

2.3. Architecture over BVPN with Rainbow



OXO Connect PowerCPU with a FrontEnd or a dedicated Rainbow WebRTC gateway on the LAN



OXO Connect Evolution with the embedded Rainbow WebRTC gateway

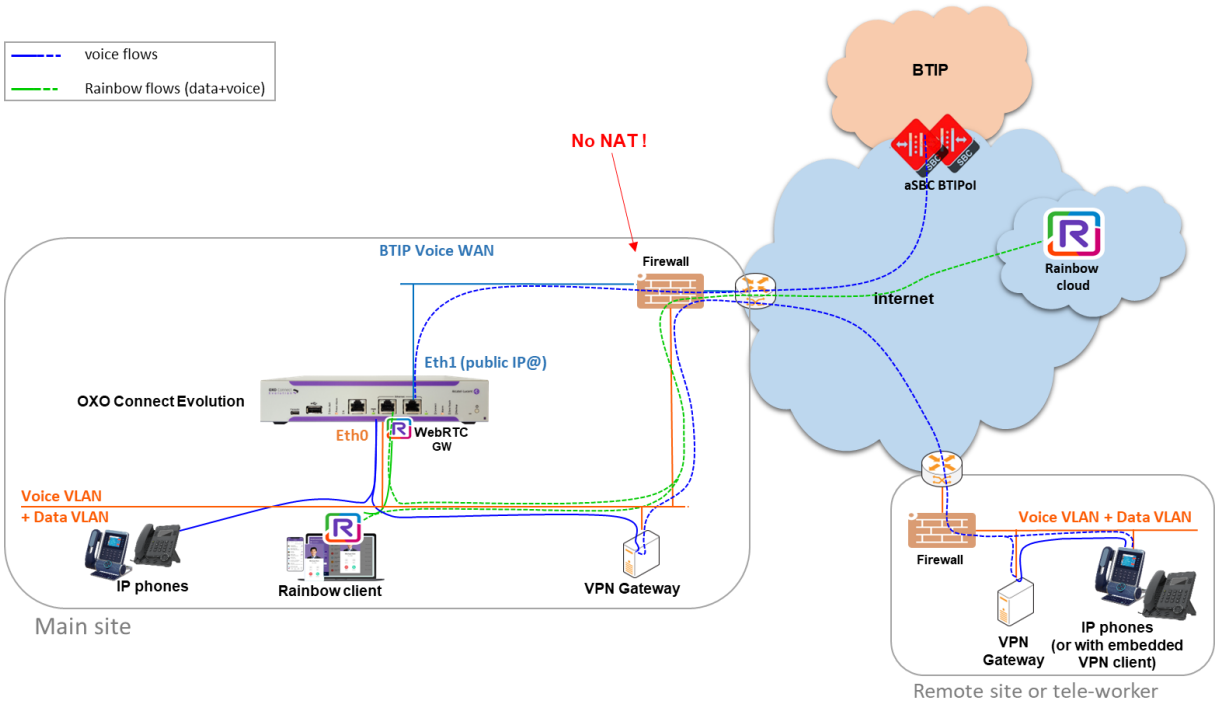
Notes :

In the diagrams above, data flows (HTTPS/XMPP/Jingle/REST) between the clients, OXO Connect or OCE, WebRTC Gateway and Rainbow services on the internet are hidden.

❶ call from/to main site
❷ call from/to remote site or worker
❸ call from/to internet client

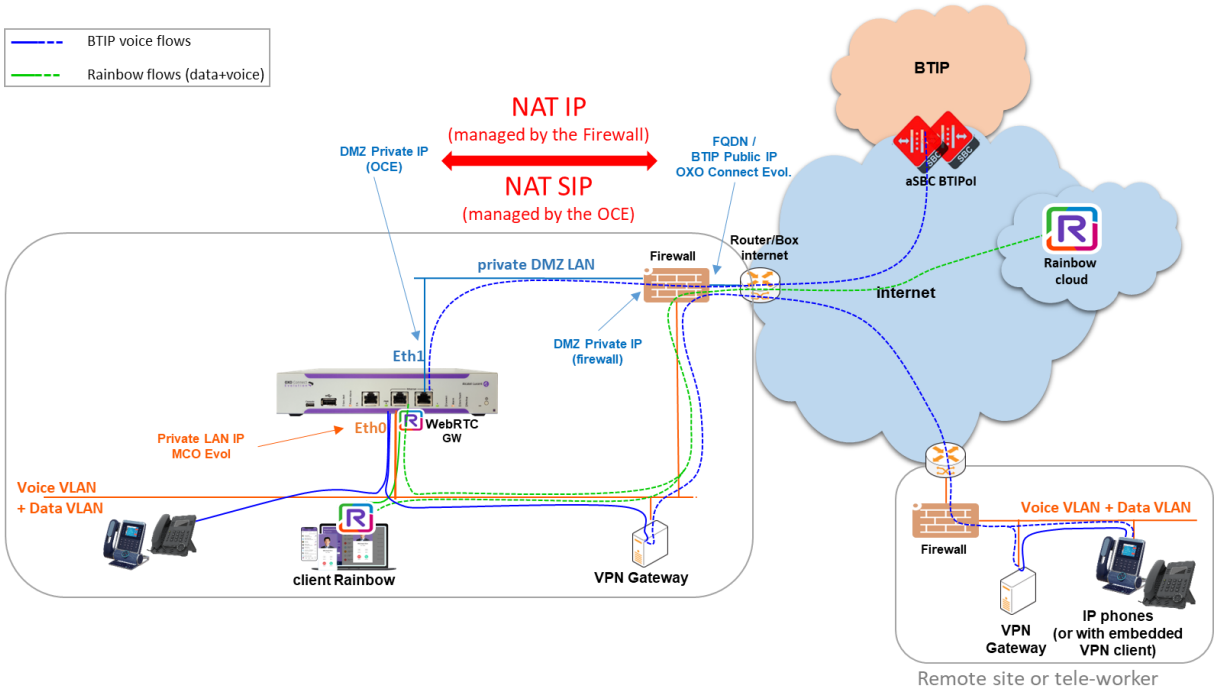
2.4. Architecture over internet (OXO Connect Evolution only)

A. Recommended topology: No NAT on the firewall, Public IP carried by the IPBX



In this topology, the **public IP is carried by the OCE** on Eth1 interface. There is **No NAT on the firewall** (transparent / bridge mode).

B. Alternative topology: Public IP + IP NAT on the firewall, SIP NAT on the IPBX



In this topology, the **public IP is carried by the firewall with layer 3 NAT** (router mode). Private IP is set up on OCE Eth1 interface. **SIP NAT is managed by the OCE** ('static NAT' feature on the 'SIP gateway').

Both SIP signalization and media flows between endpoints and BTIP are anchored and encrypted in SIP TLS and SRTP by the OCE IPBX :

- for the main site, voice flows are routed through the OCE towards the BTIP over the internet access
- for remote sites -either on Internet-, voice flows transit **through the OCE** for using the same BTIP over the internet access. A VPN or IPSEC tunnel has to bet set up between the main site and the remote site. The VPN client embedded in the newest Alcatel phones can be used also.

Reminder: only the OCE "stand alone" supports natively encrypted voice flows. **Architectures with OCE "Front End" and/or OXO PowerCPU are not supported with BTIP over internet.**

2.4.1. BTIP over Internet technical requirements

In order to establish the connection with public interface of BTIP access SBC (a-SBC), several preliminary steps have to be performed or ordered. These involve the following:

- Public IP address assignment
- Public DNS record (FQDN)
- SSL Certificate (**signed by a public CA** – Certificate Authorithy)
- Firewall rules update (to allow TLS, SRTP, DNS ports)
- TLS v1.2 cipher suites compliancy
- TLS mutual authentication
- SRTP media encryption

Refer to the 'Business Talk IP over Internet pre-requesites' and 'Technical Specifications to Access to the Service" documents provided by your sales team for more details about the encrypted architecture, the certificate management, the firewall rules, etc…

2.4.2. Public IP address assignment

The certified solution is using a public IP address directly configured on the OXO Connect Evolution interface (Eth1) placed within a DMZ in case of topology A (recommended architecture), or a public IP address with IP NAT configured on the firewall in case of topology B (alternative architecture).

2.4.3. Public DNS record

Orange a-SBC can be reached via a Fully Qualified Domain Name (FQDN) type SRV or type A deployed on public DNS. Customer premise requires a record on public DNS that enables to reach it using FQDN via public internet. BTIP over Internet can be reached using FQDN only.

2.4.4. Firewall updates

Firewalls in the way of voice traffic between the OCE and BTIP have to be updated to open required ports:

Service	Protocole	Source	Source Port	Destination	Destination Port
Voice Sig TLS	permit tcp	@IP / FQDN IPBX OCE	ALL TCP	@IP / FQDN SBC BTIPoI Nominal (1)	TPC 5061
Voice Sig TLS	permit tcp	@IP / FQDN IPBX OCE	ALL TCP	@IP / FQDN SBC BTIPoI Backup (2)	TPC 5061
Voice secured RTP	permit udp	@IP / FQDN IPBX OCE	ALL UDP *	@IP / FQDN SBC BTIPoI Nominal (3)	UDP 6000 to 38000*
Voice secured RTP	Permit udp	@IP / FQDN IPBX OCE	ALL UDP *	@IP / FQDN SBC BTIPoI Backup (4)	UDP 6000 to 38000*
Voice Sig TLS	permit tcp	@IP / FQDN SBC BTIPoI Nominal	ALL TCP	@IP / FQDN IPBX OCE	TPC 5061
Voice Sig TLS	permit tcp	@IP / FQDN SBC BTIPoI Backup	ALL TCP	@IP / FQDN IPBX OCE	TPC 5061
Voice secured RTP	permit udp	@IP / FQDN SBC BTIPoI Nominal	ALL UDP	@IP / FQDN IPBX OCE	UDP 6000 to 38000*
Voice secured RTP	Permit udp	@IP / FQDN SBC BTIPoI Backup	ALL UDP	@IP / FQDN IPBX OCE	UDP 6000 to 38000*
Public DNS resolution	Permit udp	@IP / FQDN IPBX OCE	ALL	@IP / DNS servers	UDP 53

(1) nominal BTIP SBC for TLS : sbc1.business-talk-ip.orange-business.com (194.250.129.194)
(2) backup BTIP SBC for TLS : sbc2.business-talk-ip.orange-business.com (194.250.129.196)
(3) nominal BTIP SBC for SRTP : 194.250.129.193
(4) backup BTIP SBC for SRTP : 194.250.129.195

2.4.5. Certificate updates

In order to ensure the security of traffic, public root & intermediate certificates need to be exchanged between OCE and Orange a-SBC. OCE would require an identity certificate signed by a public root CA certificate (including any intermediate certificates in the path). The OCE should send public Root & Intermediate certificates which signed OCE certificate to Orange.

In case of different public Root & intermediate certificates used by Orange (provided by Digicert), customer should retrieve ours which signed Orange a-SBC's certificates and upload them to OCE. This is described in following chapters of OCE with BTIP over internet configuration.

2.4.6. TLS v1.2 cipher suites compliance

The following cipher suites are supported by Orange SBC for TLS 1.2:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 *(preferred cipher suite)*
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

2.4.7. SRTP encryption through BTIP over internet

Media encryption preferred format: **AES_CM_128_HMAC_SHA1_80**

2.4.8. Supported codecs through BTIP over internet

Supported codec is **G.711A (20ms)** for BTIPol.

2.4.9. Fax

Fax T38 protocol -in transit- is not supported by the OXO Connect Evolution. So, **fax service is not supported** with BTIP over Internet + OCE.

3. Parameters to be provided by customers to access to the service

IP addresses marked in red have to be indicated by the Customer, depending on Customer architecture scenario

Architecture over BVPN	Level of Service	@IP used by service
Main site - single OXO Connect or OXO Connect Evolution	No trunk redundancy	OXO Connect or OCE @IP
Remote site without survivability (IP Phones only)	No trunk redundancy	N/A

Architecture over Internet	Level of Service	@IP used by service
Main site - single OXO Connect Evolution	No trunk redundancy	OCE public FQDN(1) DNS type A
Remote site without survivability (IP Phones only)	No trunk redundancy	N/A

(1) FQDN is mandatory for BTIP over Internet (France)

4. Business Talk & BTIP certified versions

4.1. Global Release Policy

Orange supports the last 2 major IPBX versions only and will ensure BTIP infrastructure evolutions will rightly interwork with the related architectures. Orange will assist customers running supported IPBX versions and facing issues.

Please refer to the latest Alcatel-Lucent '**ComSuiteSMB_ReleasePolicyInfo_Oct2023_ed7.1.pdf**' for more details about the supported versions.

4.2. Alcatel-Lucent Entreprise IPBX

ALE IPBX – software versions			
Reference product	Software version	Certification	Certified "Loads"
OXO Connect / OXO Connect Evolution	6.0	✓	OXO060/026.001 min

4.3. Alcatel-Lucent Entreprise endpoints and applications

ALE IPBX - endpoints and applications					
Reference product		Software version	Certification	OXO versions	Comments
Alcatel-Lucent endpoints	80x8, 80x8s series 80x9 series Pleaides Essential & Business series	NA	✓	all all ≧ 6.0	
	4135, 4135S	NA	✓	all	
	82x2 series 82x4 series xBS8378 IP-DECT	NA	✓	all ≧ 6.0 all	
	Rainbow WebRTC GW		✓	all	Embedded in OCE Stand-alone for OXO Connect
Third-party endpoints					
	Others		*On demand*		
Fax	Analog fax on PowerCPU (Z-x, SLI-x, MIX-x)	NA	✓	all	OXO Connect PowerCPU only
	Analog fax via Mediatrix 4102		×		*not supported*
	Analog fax via AudioCodes MP11x		×		*not supported*
enterprise SBC			*On demand*		Third party SBC

5. OXO Connect SIP trunking configuration checklist

5.1. Global settings

The OXO Connect configuration guides and profiles for BTIP are provided by ALE (Refer to the Alcatel-Luccent Enterprise Busines Portal) :

OXO Connect	Technical Bulletin	TC and SIP Trunk Profile references
4.0 to 6.0	TC1284	- TC1284en-Ed129_OmniPCX_Office_Public_SIP_Trunking_Interoperability_and_Technical_SupportProcedure.pdf
4.0 to 6.0	TC3027	- TC3027_SIP_Trunk_Solution_OBS-BTIP_(FR)_Configuration_Guideline_ONE040.pdf - TC1994_SIP_Easy_Connect_SIP_Trunk_Profile_Import-Export.pdf - FR_Orange-BTIP_ONE040_SIP.spf

Notes :

- *OXO Connect R4.0 to R6.0 share the same configuration guide and the same sip profile (refer to TC3027)
- an internet acces *–independent of BTIP-* is fully recommended to connect the IPBX to the ALE Cloud Connect (ports 500/tcp and 4500/udp towards internet to be opened on the customer firewall)

5.2. Additional and specific settings for BTIP over internet

5.2.1. Public IP/FQDN – Topology A

This section deals with architecture topology A only (= No NAT on the firewall). For the alternative topology B (= IP NAT on the firewall + SIP NAT on the IPBX) please refer to the next section 5.2.2.

First of all, you need to configure your firewall to be transparent (= without NAT) between BTIP and the OCE eth1 interface.

Then configure the CN (Common Name) / SAN (Subject Alt Name) correctly on the OCE's **eth0** interface, although the eth1 interface is used for the BTIP SIP trunk.:

Go to **OMC > Hardware and limits > LAN/IP Configuration -> eth0 -> Router IP address/Domain name** - and place here the **public FQDN** of the OCE.

The eth1 interface is configured with the **OCE public IP** address in the field “Router IP address/Domain name”:

Go to **OMC > Hardware and limits > LAN/IP Configuration -> eth1 -> Router IP address/Domain name** - and place here the **public IP address** of the OCE

Go to **OMC > Hardware and limits > DNS** - and add here **public DNS IP addresses**

Please reboot the system.

5.2.2. Public IP/FQDN – Topology B

This section deals with the architecture topology B only (= IP NAT on the firewall + SIP NAT on the IPBX). For the topology A (= No NAT on the firewall) please refer to the previous section 5.2.1.

First of all, you need to configure your firewall to manage IP NAT only (= layer 3 router mode) between BTIP and the OCE eth1 interface.

Then configure the CN (Common Name) / SAN (Subject Alt Name) correctly on the OCE's **eth0** interface, although the eth1 interface is used for the BTIP SIP trunk.:

Go to **OMC > Hardware and limits > LAN/IP Configuration -> eth0 -> Router IP address/Domain name** - and place here the **public FQDN** of the OCE.

The **eth1** interface is configured with the **OCE private IP** address in the field "Router IP address/Domain name":

Go to **OMC > Hardware and limits > LAN/IP Configuration -> eth1 -> Router IP address/Domain name** - and place here the **private IP address** of the OCE (private DMZ LAN).

Update the routing table if required by the system.

Enable the '**Static NAT feature**' to manage the 'SIP NAT' only by the OCE:

Go to **OMC > External Lines > SIP > SIP Gateways > Topology** and enable the **Static NAT** parameter, fill-in the **IP address** field by the **public IP address** of the OCE (the one declared on the firewall for the IP NAT), and modify the **SIP/SIP TLS port** to **5061**.

Go to **OMC > Hardware and limits > DNS** - and add here **public DNS IP addresses**

Please reboot the system.

5.2.3. Certificate management

Then from the **Web monitor**, generate the CSR (Certificate Signing Request) file needed to acquire identity certificate from the Certificate Authority of your choice (e.g. Digicert, GlobalSign, Comodo, Entrust, Gandi…).

The CSR generation has a format with fixed values that cannot be modified and dynamic values out of the system configuration.

The fixed ones are L = Generic, O = OmniPCX Office, OU = OmniPCX Office, Public Key Algorithm: rsaEncryption, Public-Key: (2048 bit).

The dynamic values are CN and SAN which have the same value that can be modified via OMC.

Go to **Web Monitor > Certificates > Public Server Certificates** - and click on **Generate CSR and Key**. Download the CSR file to make it certified by your public CA.

When you will receive the identity certificate signed by your CA upload it on the OCE:

Go to **Web Monitor > Certificates > Public Server Certificates > Certificate Container/File.** Select the certificate from your computer and click on **Install.** The OCE will ask to reboot to take into account the new certificate.

As mutual authentication is used between both parties, you must check and import the Root and the Intermediate Orange CA (included in the DigiCert CA). From your browser connect to the Digicert site : https://www.digicert.com/digicert-root-certificates.htm then download the certificates below (in pem format):

- the Root CA: DigiCert Global Root CA *(already pre-installed in the OCE)*
- the Intermediate CA: DigiCert TLS RSA SHA256 2020 CA1

Repeat this step to import the root and intermediate certificates of your own CA if necessary.

To import them into the OCE Trust Store go to **Web Monitor > Certificates > Root Certificates Trust Store > Certificate File**. Select the certificate(s) from your computer and click on **Install**. The OCE will reboot automatically to take into account the new certificate(s).

5.2.4. SIP trunk encryption

Go to **OMC > Security** menu and enable "DTLS Encryption". It is mandatory to activate encryption feature on the system.

Go to **OMC > Voice Over IP > VoIP Parameters > eth1.** SIP TLS trunk Signal Port must be set to **5061** and UDP to TCP swiching must be **enabled**.

Go to **OMC > External Lines > SIP > SIP Gateways > DNS** menu, select **DNS A** and enter your DNS servers IP adresses. These DNS servers must be able to resolve public FQDNs.

Go to **OMC > External Lines > SIP > SIP Gateways > Security** menu, check that **SIP TLS** is enabled and activate **Mutual Authentication.** Check that **SRTP** is enabled and add at least the AES-CM_128_HMAC_SHA1_80 cryprographic suite in the selected suites list.

And finally go to **OMC > External Lines > SIP > SIP Gateways > Domain Proxy** menu to add the **Target Domain Name** and the **Realm** and **Outbound Proxy** with the BTIPoI aSBC FQDN (should be sbc1.business-talk-ip.orange-business.com for the first SIP Gateway and : sbc2.business-talk-ip.orange-business.com for the second SIP Gateway).

Glossary

- OXO : OmniPCX Office
- OCE : OXO Connect Evolution (“ IP box ”)
- A-SBC : access Session Border Controller (Orange Business)
- C-SBC : customer or enterprise Session Border Controller (on customer side)
- BTIP : Business Talk IP (Orange Business – French market)
- BTalk : Business Talk (Orange Business – International market)
- BTIPoI : BTIP over Internet
- BToI : BTalk over Internet
- MCO : Multi Connect Office
- AS : Application Server Business Talk / BTIP
- TP WAN : Third Party WAN (on customer side)
- BVPN : Business Virtual Private Network (Orange Business MPLS)
- CAC : Call Admission Control
- WebRTC GW : Rainbow WebRTC gateway
- CA : Certificate Authority