Cloud Voice SIP Trunking

LAN and Firewall Guide

Introduction

This document provides supporting information for the configuration of a customer firewall and LAN to support a successful implementation of a Cloud Voice SIP Trunking service.

When placing an order for Cloud Voice SIP, customers are requested to acknowledge that;

1. The content has been read and understood, and

2. Where applicable implementation of any changes to customer owned network configuration will be undertaken before BT implement the service.

Once configured, your Cloud Voice SIP service enables you to make and receive calls via your PBX utilising a BT internet access service thus providing a consolidated voice and data service.

It is important that the service has connectivity across your internal data network so that your PBX can communicate with our Cloud Voice SIP platform to ensure consistent quality.

Firewalls

There is a wide range of firewalls available from a variety of manufacturers and as a result there is no single method of configuration to achieve support of a given application.

The information in this document states the requirements of the Cloud Voice SIP service, however you will need to determine the most appropriate method of configuration in-conjunction with your IT/Firewall provider or maintainer.

Cloud Voice SIP is a registering SIP service. Connectivity is established using outbound SIP REGISTER messages and therefore in some instances you may find that the service will be available without the need for any additional configuration.

If you are experiencing connectivity issues, then changes may need to be implemented on your firewall to ensure Cloud Voice SIP Trunking service can be accessed from your network.

Recommendations

We recommend that you consult your firewall provider before you make any changes so you can be sure that you don't inadvertently expose your network to any security risks. or contravene any local IT policies.

Network Routing

Our Cloud Voice SIP service has the following requirements:

- The IP-PBX or SIP Gateway will need LAN connectivity, access to the internet, and appear on the outside of the firewall with a public IP address.
- This can be achieved by using address translation. SIP will only work with NAT and not PAT.
- The IP-PBX or SIP Gateway requires access to the Cloud Voice SIP platform on IP address 217.32.186.185 and 217.32.186.121 using port numbers 5060 to 5075.
- **SIP ALG must be disabled**

IMPORTANT NOTE:

If your router and/or firewall is "SIP Aware" / has a SIP ALG enabled, then this functionality must be turned OFF so that the device does not interfere with any signalling.

Not all firewall configurations need ports to be opened. If your firewall is running inside to outside rules, then ports should be opened to allow access to the BT Cloud Voice SIP service.

There should be no reason to open ports inbound on the firewall.

Prioritisation

If you are using BT Business internet access this service prioritises your SIP signalling and VoIP traffic over other traffic. However, if using a non-BT Business access provider please ensure that voice traffic is prioritised in order to ensure highest quality of service.

To ensure end to end voice quality is maintained your LAN should also prioritise this traffic.

Our BT Cloud Voice platform has the following IP addresses:

Signalling - 217.32.186.185 and 217.32.186.121

Media - 217.32.186.178 and 217.32.186.114

These addresses should be used to build the policies to support prioritisation i.e. traffic to and from these addresses should be prioritised over other competing traffic in your LAN infrastructure.

In particular:

1. The incoming and outgoing BT Cloud Voice SIP and VoIP (RTP) traffic should be prioritised over other traffic though the firewall.

2. If the SIP signalling and VoIP traffic traverses your LAN (e.g. between IP phones and PBX or between the PBX and the firewall) and competes with other traffic then it will need to be prioritised over that other traffic.

Important Note: The SIP and VoIP (RTP) packets are not re-marked in terms of CoS, ToS, DSCP or any other Quality of Service markings. Any received DSCP markings should be regarded as un-trusted and not used for QoS.

Ports

This section identifies all the required TCP/UDP ports for correct operation.

Device	Protocol	Outbound Destination	Destination Port
IP PBX / SIP Gateway (Signaling)	SIP	Primary 217.32.186.185/27 Secondary 217.32.186.121/27	UDP/TCP 5060 to 5075
IP PBX / SIP Gateway (Media)	RTP	Primary 217.32.186.178 Secondary 217.32.186.114	UDP 32766 to 65535
IP PBX / SIP Gateway	NTP	Supplied Locally* or europe.pool.ntp.org	UDP/TCP 123
IP PBX / SIP Gateway	DNS	Supplied Locally* (customer DNS server) or BT DNS Servers	UDP/TCP 53

* Customer to provide the installation engineer with IP address or FQDN of any locally delivered services.

DNS SRV Record

SRV Record

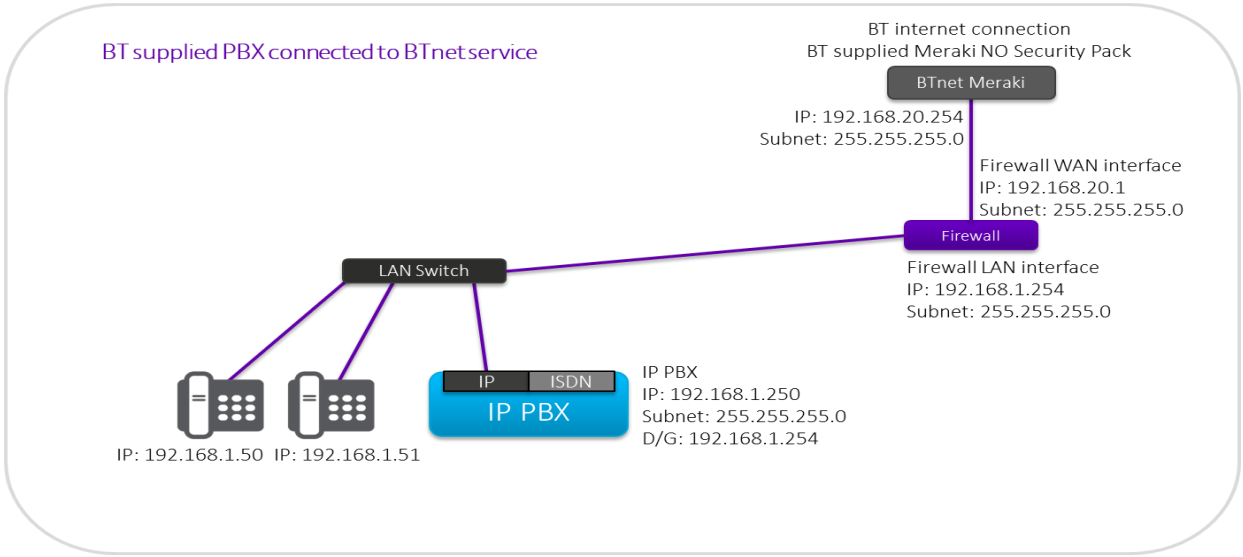
ipcomms-btb-sipt-dynamic-wv24lnws24.bt.com

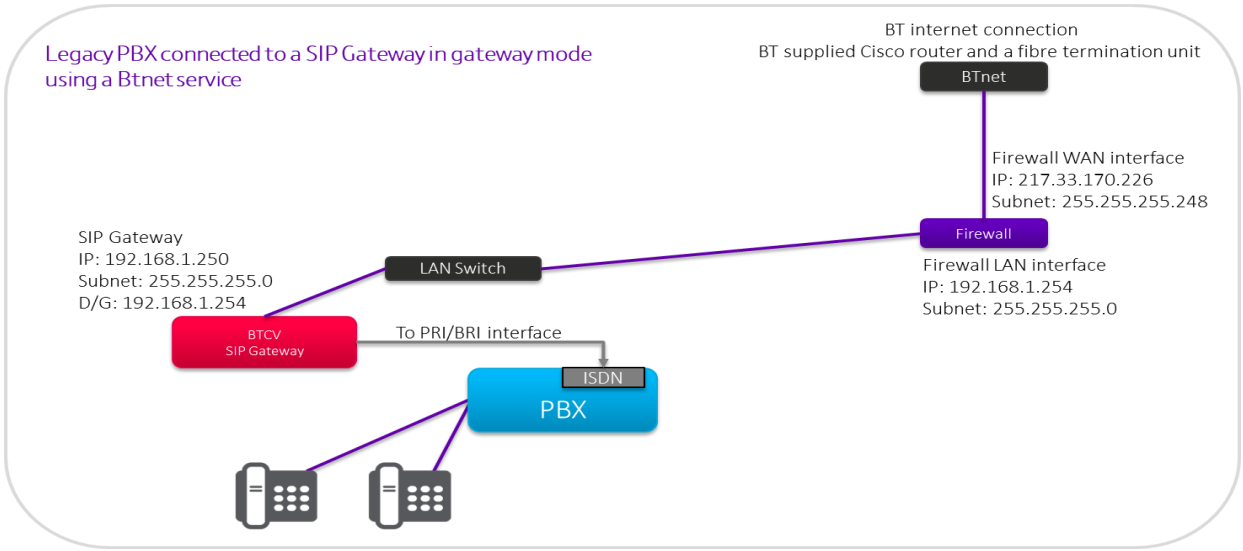
A Record

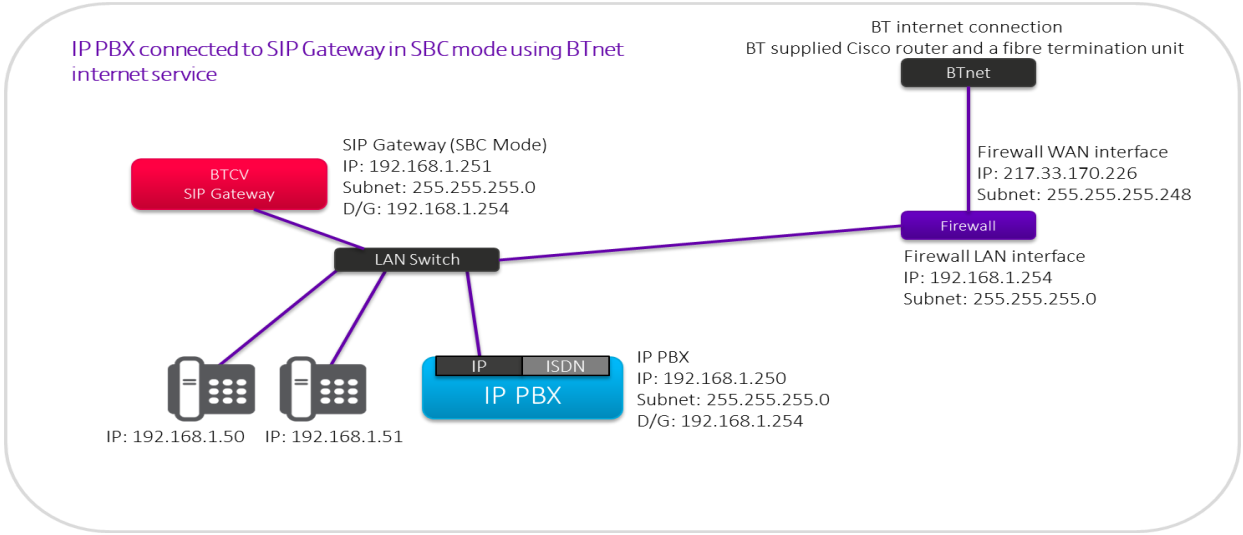
Primary - ipcomms-btb-sipt-dynamic-wv24.bt.com

Secondary - ipcomms-btb-sipt-dynamic-lnws24.bt.com

Example Deployments







Glossary of terms

CoS – Class of Service

DNS – Domain Name Service

DSCP - Differentiated Services Code Point

FQDN – Fully Qualified Domain Name

LAN – Local Area Network

NAT – Network Address Translation

NTP – Network Time Protocol

PAT – Port Address Translation

QoS – Quality of Service

RTP – Real Time Protocol

SRV – Service Record

ToS – Type of Service

Important Stuff

You should be able to use your BT Cloud Voice service to make and receive good quality phone calls. However, you'll only be able to do that if your internal network is properly set up. If it isn't, your call quality won't be top-notch. If you report a fault to us and we find that the fault is down to a problem with equipment that you own or due to non-BT access you are using, then charges will be raised related to the issue.

The information in this document is provided for general guidance only. It is recommended that your firewall maintainer, switch maintainer or IT consultant is consulted on all matters relating to your communications network including, but not limited to, PBX configuration, LAN and firewall configuration. This is particularly important in connection with any issues which may impact on your network security or local IT policies.