myPortal@work

1. Introduction:

   There are several homeworking solutions available on OpenScape Business. The most common ones are device@home (HFA or SIP) or myPortal@work with the integrated VoIP client. In both cases connections towards the system can be made directly via Internet without the usage of VPN gateways.

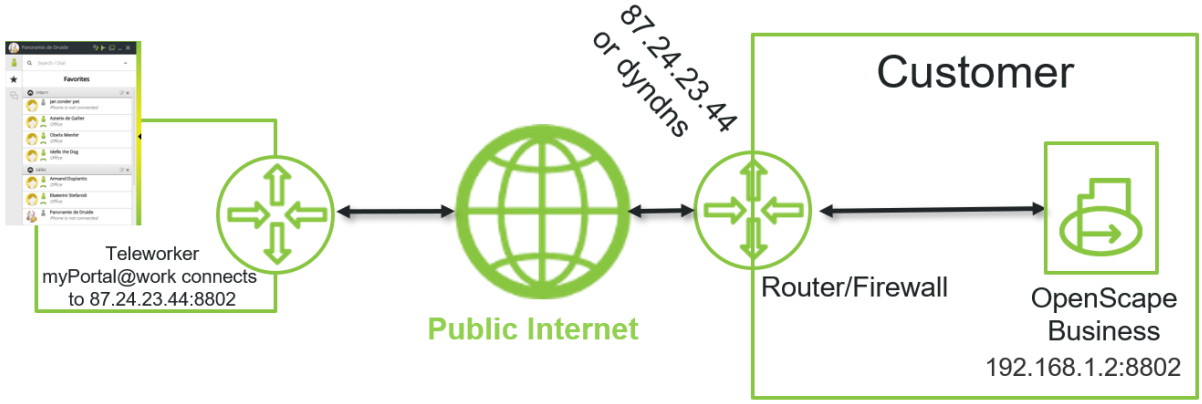
   When using device@home, the user will use a desk phone, or he can also decide to use myPortal to Go with the integrated HFA VoIP client. For this last case, the integrated VoIP client can only be used if the Android or IoS device is connected via WiFi (WLAN mode). In case of 4G the system will switch back to GSM mode, and the mobile device will be called on the mobile number. For more information about device@home, ports, tips and tricks please check:

   With myPortal@work, the user has a soft client on his PC (Windows or Mac) and can use, besides the UC functionalities of the client also the integrated VoIP client in combination with a headset and this from any location where internet is available. Of course, there are some configuration rules that need to be taken in to account. If you follow those rules, there should not be any issue in the use of all the functionalities this client has to offer.

2. Connectivity options with myPortal@work client
   a. myPortal@work has 2 functions.
      i. The client can be used as a pure UC client to control a normal desk phone.
      ii. The client can be used as a UC client with an integrated soft phone based on the WEBRTC protocol.
   b. myPortal@work can be connected to the system via:
      i. the Local LAN at the customer's site
      ii. Via a VPN connection between his location and the location where the OSBiz is located
      iii. Via public internet. This is done via port forwarding on the ISP router via which the OSBiz has connection to the internet.
3. What can go wrong when connecting myPorta@work via Public internet?

   In case myPortal@work is connected via the public internet, there are some rules and network configurations that can influence the behaviour of the VoIP client. If these rules and configurations are not correct payload issues might occur in several scenarios.

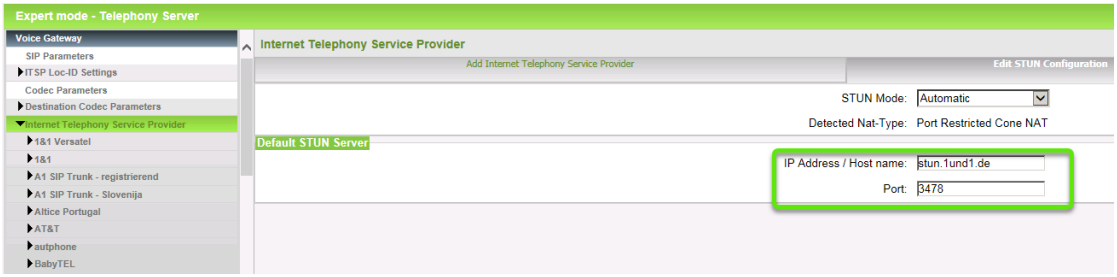
   1. What is needed to connect myPortal@work with integrated VoIP client via the public internet:



Firewall rule or Router forwarding from Internet:
Source Internet TCP Port 8802 ➔ Destination IP 192.168.1.2 TCP Port 8802
In the system, a STUN server must de defined. The system needs to reach the STUN server via the normal internet access.

a. Port forwarding on the router. Port 8802 needs to be open from external to the internal IP address of the system/booster port 8802.
b. STUN server needs to be configured.
    i. If the connected ITSP uses an own STUN server, this will be used.
    ii. If the connected ITSP has no own STUN configuration or calls are made via ISDN, then a STUN server needs to be configured via Expert mode ➔ Telephony server ➔ Voice gateway ➔ Internet Telephony Service Provider ➔ Edit STUN configuration
c. The flag “use internal SBC” which is used for device@home MUST NOT be activated.

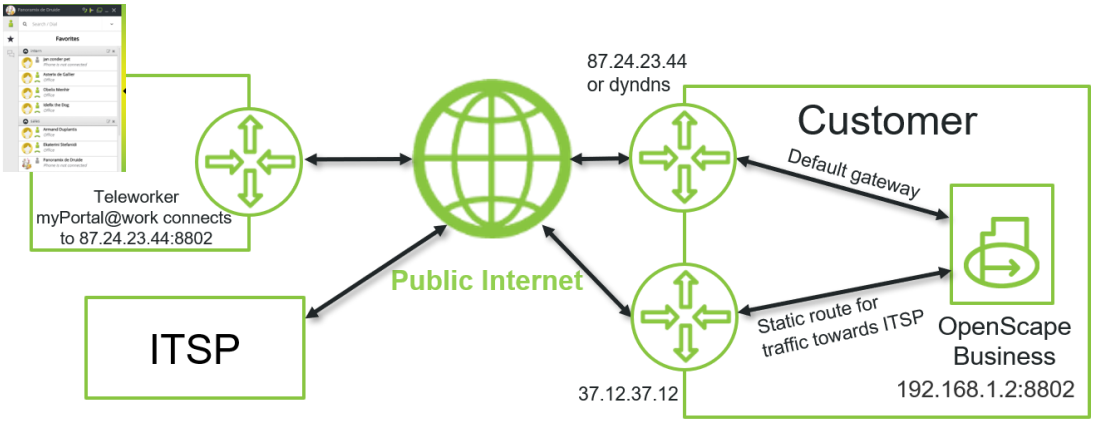
2. What needs to be kept in mind:
    a. Make a small network plan of the environment.
    b. myPortal@work can only be connected via the LAN port of the system.
    c. Only TCP port 8802 needs to be forwarded towards the LAN IP address of the OSBiz. for incoming Internet traffic, on the Firewall/router. All other ports will be auto negotiated between the client and the OSBiz.
    d. A STUN server needs to be configured in the system. If in the connected ITSP a STUN address is entered, this is sufficient. Otherwise, STUN configuration needs to be entered manually. Expert mode ➔ Telephony server ➔ Voice Gateway ➔ Internet telephony server provider ➔ Edit STUN configuration
    e. The route towards the STUN server needs to be via same the router (public IP address) that is used for the incoming traffic on port 8802. If STUN requests are sent via another router, the public IP address will be wrong and payload issues will occur.



f. In case of a firewall please be sure the STUN server on the correct port can be reached.
g. If the system detects a Symmetric NAT router, payload will not be possible. Depending on the type of firewall, settings can be made to change the NAT type.
    i. On more complex firewalls the option could be to change the setting of the firewall. The UDP source ports 1024 until 65535 should not be changed for outgoing traffic. When the original source port is changed you have symmetric NAT.
h. SIP alg should be deactivated in all cases on the routers. This is needed on the home office routers as well as on the router that is located on the side where the OSBiz is located.

i. The WAN interface should not be used when connecting myPortal@work via public internet. If this is done our internal SBC will detect the Public IP address of the WAN interface and will use this in the communication between the client and the OSBiz. This will lead to payload issues.

Possible solution: Connect the ITSP also via the LAN interface. This can be done via the normal ISP router or via a second router and static routes.



Firewall rule or Router forwarding from Internet:
Source Internet TCP Port 8802 ➔ Destination IP 192.168.1.2 TCP Port 8802
In the system, a STUN server must de defined. The system needs to reach the STUN server via the normal internet access.

This solution via a second router will not work if the ITSP uses an own STUN, since the internal SBC will again use the wrong Public IP address in the messaging between the system and the client.

Be careful, if you need to change the setup form WAN to LAN the complete system needs a restart, this is something that most of the times is not allowed during business hours.

j. A homeworker could also be using his myPortal@work behind a symmetric Nat router and this could also lead to Payload issue. There are 2 things to analyse this problem:
   i. Check the connection via an already tested internet access. Try to be sure that your own office or home environment is a working environment. If there are issues with users of an end customer, you can always test from your location with their credentials. This test is not only applicable for this issue, but can also be appliable for issues with PC's, headsets, sound card drivers etc.
   ii. You can make a small test to check the Nat of the end user's router. Use the following link to make a test: https://webrtc.github.io/samples/src/content/peerconnection/trickle-ice/

   The outcome of the test could be one of the 3 following results:

   1. there is only one srflx candidate --> no sym. NAT

   2. there are two srflx candidates with different port --> sym.NAT

3. there is no srflx candidate at all --> UDP seems to be blocked completely

To make the test you need to enter at least 2 STUN addresses. E.g.:

stun:stun1.l.google.com:19302

stun:stun2.l.google.com:19302

k. In some particular cases you need to use a Mulap/Team configuration. This is mainly the case if the user uses a TDM phone or a DECT handset as extra phone. In case the users is using an IP phone in the office it is much better to use a desk hare configuration;
    i. Create the IP-phone as a desk share user in the system.
    ii. Use this data for connecting the phone directly to the system. This means you do not need to use *9419 to log on or log of the desk share user every time.
    iii. When the desk share user starts his myPortal@work with VoIP activated, the desk phone will be logged out automatically. On the display the following message is shown: Cancel mobility.
    iv. When the user wants to start his desk phone, he selects “cancel mobility” and the phone starts up again with the correct number.
l. In case of payload issues, please also check the headset or sound card:
    i. An easy test can be to use as a test the speakers and microphone of the PC.
    ii. In some cases, we have seen that the sound card of a PC on which no headset is connected also lead to the fact that a call cannot be set up. So always be sure you have a headset with you to test.
    iii. It also can help to deactivate the headset integration flags as a first test. This will help to define if there is an issue with the headset/PC or other elements of the scenario. When headset integration is deactivated, a call cannot be answered via the headset and the LED on the headset will not light up when the user is in a call. As a test this should not be a problem.