TELAVOX

FAQ - Network

All calls from Desktop/Webapp and your fixed phones are done through an internet connection, because of this you need to confirm that the traffic to and from our servers is getting through properly. We highly recommend that you make a few test calls before you start using our service. The best way to test this is to connect a phone and attempt to recieve a call, then make an outgoing call.

We recommend that the first incoming call test is made 15 minutes after the phone has been connected. This test cannot be performed if you are moving a phone number from another service provider to us, we need to move the number first. Please contact us to perform the test.

If the call is not being connected, you most likely have a firewall that is causing the problem. We recommend that you make the following adjustments to your firewall.

CONFIGURING YOUR FIREWALL

For outgoing traffic:
Create a rule for all UDP- and TCP ports to Telavox net 80.83.208.0/20.

This rule should have a Timeout (TTL) of at least 3720 seconds, since our phones synchronize with us every 3600 seconds.

Complete information about our network:
Address: 80.83.208.0
Netmask: 255.255.240.0 = 20
Wildcard: 0.0.15.255
Network: 80.83.208.0/20
Broadcast: 80.83.223.255
HostMin: 80.83.208.1
HostMax: 80.83.223.254
Hosts/Net: 4094

For incoming traffic:
This does not require any rules because the session is initiated from the inside of the network.

Inactivate all ALG/SIP-functions and Application Control on the traffic to Telavox if this is in the firewall, it often does more harm than good.

TELAVOX

BANDWIDTH

A call requires 0,1mb/s download and upload speed. Since your calls run through an internet connection along with all other traffic within your network, it's important to have enough capacity for this. We highly recommend a fiber connection.

To ensure that there is enough bandwidth for the phone service, we recommend that you set the rules for Traffic Shaping in your firewall to prioritize traffic to and from Telavox. An alternative to this is to set the Quality of Service to prioritize tagged packets. We tag all packets with the following:

- For RTP (sound/media) Expedited Forwarding (EF) DSCP46 = TOS184/0XB8
- For SIP (signalling) Assured Forwarding (AF31) DSCP26 = TOS104/0X68.

Only hardware purchased from us including our softphone have these tags.

sip.telavox.se

To reach higher accessibility and a simplified flow of communication between a SIP-terminal and Telavox platform, it's possible for the terminal to take advantage of DNS SRV posts to locate Telavoxs servers. Normally, DNS A posts are used to see what IP-address a server has. All terminals that are provisioned by Telavox use DNS SRV posts to set the name service to sip.telavox.se.

A terminal that is configured to use DNS SRV posts for SIP over UDP, therefore it makes a suggestion to the address _sip._udp.sip.telavox.se.

In Windows CMD/Powershell
nslookup -type=SRV _sip._udp.sip.telavox.se

Bash Terminal UNIX/OSX
dig SRV _sip._udp.sip.telavox.se

If you are using a physical PBX with a SIP-trunk. the traffic will go to siptrunk. telavox.se. Press here to read more.

PROTOCOL

Below you will find the protocols used by hardware delivered by Telavox together with a description of their functions. Different types of terminals use different protocols. As an example, HTTPS is preferred for retrieval of software instead of TFTP and HTTP. In cases where the terminal does not support HTTPS, one of the other is used. Telavox does not recommend that you block traffic to and from terminals based on ports and/or protocols, we instead recommend that you trust all traffic to and from the Telavox network. Telavox does not pledge to only use the protocols below. Please observe that the

specified ports are receiving ports, as a rule rather than an exception, our hardware uses randomly chosen sending ports.

FTP

File Transfer Protocol, RFC959, TCP port 21 and 20. Used to retrieve terminal configuration and software.

DNS

Domain Name Server, RFC1035, TCP/UDP port 53. DNS functionality is a part of a working IT network and the terminals delivered by Telavox don't work if they don't have access to a working DNS.
In the case where the DNS is placed outside the firewall, the firewall must allow the terminals to suggest the DNS.
Our provisioned phones are configured with Googles DNS:s 8.8.8.8 and 8.8.4.4.

HTTP

Hyper Text Transfer Protocol, RFC2616, TCP port 80. Used to retrieve terminal configuration and software. Normally, no special configuration is required for HTTP to work well.

HTTPS

Hyper Text Transfer Protocol over Secure Socket Layer, RFC2818, TCP port 443. Used to retrieve terminal configuration and software.

TFTP

Trivial File Transfer Protocol, RFC1350, UDP port 69 and dynimically allocated ports for data transfer. Used to retrieve terminal configuration and software.

SNTP/NTP

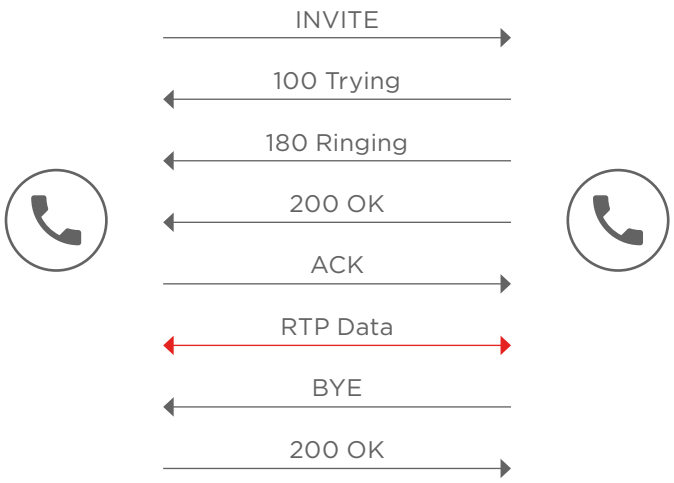
Simple Network Time Protocol, RFC1305/RFC1361, UDP port 123.
Used to set the date/time in the terminal.

TELAVOX

SIP

Session Initiation Protocol, RFC3261, UDP port 5060. Used to connect and disconnect calls. The SIP-traffic runs between our SIP-servers and the phone. This is the most important protocol for the phone service to work.

The picture below show the SIP-traffic between two phones.



RTP

Real Time Transfer Protocol, RFC1889, UDP port 1024-65535 (Telavox uses UDP port 10 000-20 00) The sound during a conversation runs via RTP. The port used for the call is randomized when the call is initiated. All of Telavox delievered terminals use symmetrical RPT which means that the recieving and sending port for the RTP-stream are the same for both outgoing and incoming sound. This means that the soundstream that goes from the terminal to us opens up a session in the firewall to allow even incoming soundstreams over the same session.

RTCP

Real Time Control Protocol, RFC3550, UDP port 1024-65535. Some terminals generate RTCP-packets used in the communication between RTP-endpoints to convey local statistics and conversation data aswell as information about jitter and eventual packetloss.