Topology requirements

Network Topology without NAT

As long as you have no NATs between the sipXcom server and all the phones and gateways there should be no challenges from a network topology perspective. As long as all the hosts are reachable a routed network works fine and also network segments reachable via VPN are not a problem.

Network Topology with NAT

NAT traversal at the near-end or far-end represents a significant challenge for the SIP protocol as both signalling (SIP) and media (RTP) needs to be mapped to traverse NATs successfully. Up to and including sipXcom release 3.10 an external Session Border Controller (SBC) is required for NAT traversal.

As of release 4.0 sipXcom includes native support for both remote worker configurations as well as SIP trunking. There are two services utilized for this sipXrelay for NAT traversal and sipXbridge for trunking support. Use of these services is only encouraged for Lab purposes only. These services do not scale properly and do not support a HA configuration. The user should utilize a session border controller for this functionality.

External Session Border Controllers

For releases earlier than 4.0, an external SBC is needed for operation behind NATs. In newer releases a SBC is still recommended. This gets external SIP signalling and media off of the server allowing the server to scale better and provide a more reliable connection for Trunks and Remote workers.

Remote worker configurations require both near-end and far-end NAT traversal assistance. Some products, such as the Sangoma SBC or Ingate SIParator provide support for both. Therefore, at the far-end there is no special equipment required and phones connected behind a traditional firewall /router will work fine. Other products might require NAT traversal assistance at the far-end as well.

SIP Trunking requires both near-end NAT traversal as well as interoperability with the ITSP providing the SIP trunking service. An SBC is required and we have typically used Acme Packet (now Oracle), Sangoma or Ingate SIParators for this purpose.

Network Services

sipXcom does not work unless DNS and DHCP services are properly configured. It is possible to use the sipXcom server for such network services. The single CD ISO installation disk provides for automated installation and configuration of such services. However, more often you already have DNS and DHCP services deployed on your network. Please consult the respective information on how to configure such services to work with sipXcom. sipXcom uses DNS SRV records, which requires proper setup. If you deploy sipXcom in a high-availability configuration the complexity of the DNS SRV configuration increases dramatically.

The sipXcom administration portal (sipXconfig) provides automated tests that allow the verification of proper configuration of all such network services. Make sure the tests pass immediately after installation and before you file a trouble ticket.