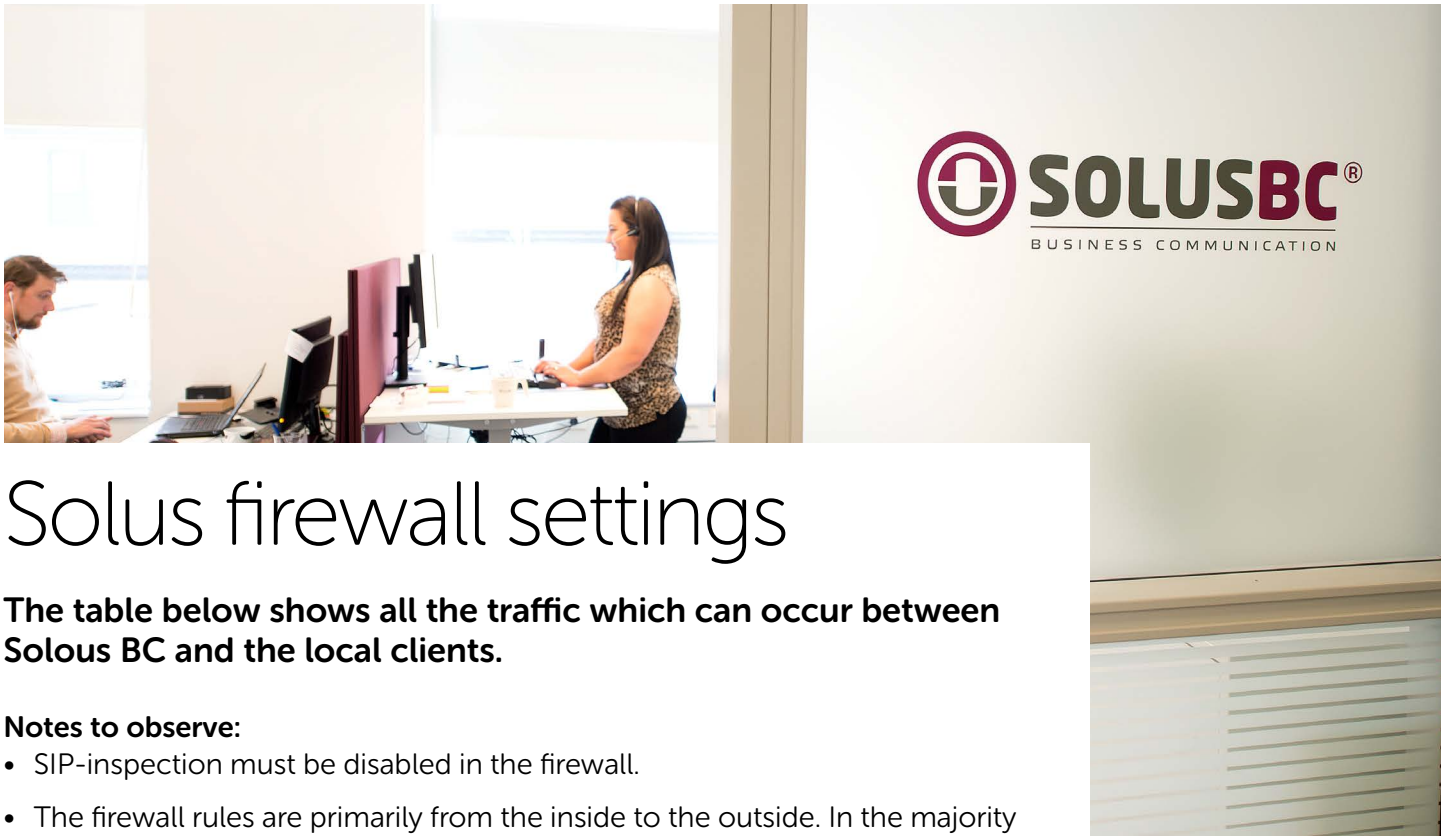
SOLUSBC®
BUSINESS COMMUNICATIONS

"It's not just a system, it's a new way of work."



Solus firewall settings

The table below shows all the traffic which can occur between Solous BC and the local clients.

Notes to observe:

- SIP-inspection must be disabled in the firewall.
- The firewall rules are primarily from the inside to the outside. In the majority of cases no port openings are necessary since most firewall configurations allow traffic from the inside.
- Some firewalls and firewall configurations may demand that port openings are made, not only from the inside, but also from the outside. If the telephony isn't working as expected, try opening the ports bot from the inside and from the outside.
- Media, namely speech traffic is dynamically negotiated between the SolusBC platform and the local clients for each separate call. Hence, traffic can emerge on the whole port span 49152–65534.

FROM THE INSIDE TO THE OUTSIDE

TO

Destination port – IP (s)	Protocol	Transport	Firewall rule	Comment
212.247.59.2-29	80	HTTP	TCP	Allow
212.247.59.2-29	443	HTTPS	TCP	Allow
212.247.59.2-29 SIP Inspection must be disabled in the firewall.	5060 & 5061	SIP/UDP	TCP	Allow
212.247.59.2-29 Media- (speech traffic).	49152–65534	RTP/RTCP	UDP	Allow
212.247.59.2-29	123	NTP	UDP	Allow
212.247.59.2-29	514	SYSLOG	UDP	Allow

Solus Business Communications AB | Fabriksgatan 7, 412 50 Göteborg
Office Phone: +46 31 352 40 00 | **Support Phone:** +46 771 720 720 | info@solus.se
Orgnr 556377-2317 | Innehar F-skattsedel | www.solus.se