Tele365
powered by Mitel

The table below shows all traffic which can occur between Tele365 and the local clients

Tele365 Firewall Settings

Notes to observe:

* SIP-inspection should be disabled in the local firewall.

* Firewall rules primarily apply for traffic from the outside of the local firewall, since most firewalls automatically allow traffic from the inside.

* If services aren´t working as expected, please allow the rules from the inside of the local firewall as well.

* Media/Speech is negotiated dynamically in the SDP for every call. Therefore it is necessary to allow the whole port span.

To	Destination port	Protocol	Transport	Rule	Comments
Tele365 telephony system					
185.39.124.0-31	80/443	HTTP(S)	TCP	Allow	
212.247.59.2-29	80/443	HTTP(S)	TCP	Allow	
Tele365 telephony system					
185.39.124.0-31	5060/5061	SIP	TCP/UDP	Allow	SIP inspection in the firewall should be turned off.
212.247.59.2-29	5060/5061	SIP	TCP/UDP	Allow	SIP inspection in the firewall should be turned off.
Tele365 telephony system					
185.39.124.0-31	49152-655534	RTP/SRTP	UDP	Allow	Media/Speech
212.247.59.2-29	49152-655534	RTP/SRTP	UDP	Allow	Media/Speech
Tele365 telephony system					
185.39.124.0-31	514	Syslog	UDP	Allow	
212.247.59.2-29	514	Syslog	UDP	Allow	
Mitel Phone Firmware					
185.39.124.0-31	80/443	HTTP(S)	TCP	Allow	Firmware for Mitel Phones.
Mitel Phone RCS					
rcs.aastra.com	80/443	HTTP(S)	TCP		Used for Mitel phone settings distribution via the suppliers redirection system.
Snom Phones					
185.39.124.30	9443		TCP	Allow	Used for provisioning of Snom phones
185.39.124.0-31	123	NTP	UDP	Allow	
212.247.59.2-29	123	NTP	UDP	Allow	
SPF records					
83.140.103.4					All emails related to Tele365 is sent from this address

Version 1.2