

If the Firewall is a **General** Type:

\* **WAN To LAN** - Open ports in range 5060 - 35000 (If possible, open ANY & ANY) in protocols TCP & UDP to all addresses or domains (If possible) :

<u>Addresses</u>	<u>Domains</u>
108.61.199.115	fs3a.amst.omnitelecom.com
45.32.239.114	fs3b.amst.omnitelecom.com
94.188.160.180	fs3c.tlv.omnitelecom.com
45.63.119.234	fs3d.fra.omnitelecom.com
95.179.244.94	fs3f.fra.omnitelecom.com
108.61.210.160	fs3q.fra.omnitelecom.com
95.179.149.139	fs3h.amst.omnitelecom.com
95.179.182.13	fs3i.amst.omnitelecom.com
78.141.219.220	fs3j.amst.omnitelecom.com

\* **LAN To WAN** - ANY > ANY

\* Disable - "SIP ALG"

If the firewall is a **Checkpoint** type:

Open all the addresses listed above and also follow these steps:

\*you should mark "V" in "Deep Inpaction"

\* Keep Alive Time Out : Users&Objects > Services > SIP > Sip\_UDP > Advanced > Session Timed out > **Set to 200**

• **Set OQS:** Device > Internet > ISP Dialup > Advanced > Qos Settings > **Enable** Qos (upload) > ISP upload bandwidth (בהתאם לחבילת גלישה)

• Access Policiy > QOS > Blade Control > **ON**

• Access Policiy > QOS > Policy > Sorec & Destenation > **ANY ANY SIP 20% / 25%**