1 General requirements

The customer firewall and all other network infrastructure components involved (LAN switches, routers, WLAN components, etc.) should transfer all IP traffic for telephony (UDP + TCP and all protocols) from the internal customer network (LAN) to VoIP infrastructure of Telecom Liechtenstein (WAN).

The IP subnet (C-Class) of Telecom Liechtenstein is: **80.66.238.0/24 (TCP + UDP on all protocols/ports)**.

This IP subnet is used by Telecom Liechtenstein for all current and future VoIP services. By releasing the entire IP subnet, the customer infrastructure is prepared for future expansions and it is also ensured that all IP addresses of the geo-redundant VoIP infrastructure of Telecom Liechtenstein can be reached.

If security restrictions on the customer side do not allow the activation of all IP protocols/ports, the protocols and ports used are listed below. However, if any impairments occur, the Telecom Liechtenstein rule listed above must install in order to exclude problems on the firewall or other components.

It is mandatory that the firewall does not manipulate the SIP and HTTP protocols in any way by deep inspection or other mechanisms (application layer gateway). It means, the following (or other similar) mechanisms must be disabled:

- Deep Inspection
- UDP Port Hopping
- SIP Awareness / SIP NAT Support / SIP ALG
- HTTP Content Filtering

1.1 Multiple LAN-side network segments

If the customer has several LAN segments (e.g. a separate segment for the WLAN infrastructure) connected via a router/firewall/Layer 3 switch, it must be ensured that all ports (especially the RTP/sRTP ports) are also between the LAN segments are switched through to each other.

1.2 Quality of Service (QoS) functions on the LAN

There are two methods for ensuring the required quality on the LAN:

- Sufficient bandwidth: If the complete infrastructure of the customer site is building with Gigabit LAN throughput, no further QoS support is required, but it is still strongly recommended.
- QoS support and clean configuration of the PC clients: The LAN infrastructure and the Layer 3 switches used must trust DiffServ Code Points (DSCP) of end devices (DSCP trusted) and accept them in Class-of-Service (COS).

1.3 DNS-server and NTP-server Addresses

If the Internet connection comes from Telecom Liechtenstein, the following IP addresses and ports must be enabled for the DNS and NTP services.

DNS name (URL)	IP address	Protocoll:Port	Description
	217.173.235.71 217.173.235.72 217.173.235.73	UDP:53 (DNS)	DNS-server
ntp1.telecom.li ntp2.telecom.li	80.66.224.2 80.66.224.10	UDP:123 (NTP)	NTP-server

FL +423 237 74 00 | www.FL1.li | **CH** 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

2 Restrictions on individual protocols/ports (LAN ➔ WAN)

The restrictions on individual IP protocols/ports should be make only if the corresponding security guidelines require this. In order to be able to activate new services in the future, Telecom Liechtenstein may require additional IP protocols/ports. However, these will always be within the C-Class listed above.

2.1 For product FL1 CommPlus (vPBX)

IP address / net mask	Protokoll:Port	Description
80.66.238.0/24	UDP:5082 (SIP) TCP:5061 (SIPs, TLS) UDP:10000-65535 (RTP, sRTP)	SIP-Outbound-Proxy (SIP signalling) SIP-Outbound-Proxy (SIP signalling secure) SIP-Outbound-Proxy (SIP media-ports)
	TCP:5075 (SIP) TCP:5076 (SIPs)	CSTA-server for CTI-clients CSTA-server secure for CTI-clients
	TCP:5244 (XMPP) TCP:9091 (XMPP-Data)	instant-messaging server instant-messaging server file-transfer (secure)
	TLS:636 (LDAPs) TCP:389 (LDAP)	LDAP-server for central phone book *(TCP:389 only, if Gigaset N510/N720)*
	TCP:80 (HTTP) TCP:443 (HTTPS) TCP:18443 (HTTPS)	configuration-server for auto-provisioning of IP devices configuration-server for auto-provisioning of Softphone-client access to CommPlus administration GUI

2.2 For product FL1 Trunk

IP address / net mask	Protokoll:Port	Description
80.66.238.0/24	UDP:5083 (SIP) TCP:5063 (SIPs, TLS) UDP:10000-65535 (RTP und sRTP)	SIP-Outbound-Proxy (SIP signalling) SIP-Outbound-Proxy (SIP signalling secure) SIP-Outbound-Proxy (SIP media-ports)
	TCP:443 (HTTPS)	access to Trunk administration GUI (planned)

2.3 For products FL1 SIP-Line (combi-products with VoIP und Convoip Line CH)

IP address / net mask	Protokoll:Port	Description
80.66.238.0/24	UDP:5082 (SIP) TCP:5061 (SIPs, TLS) UDP:10000-65535 (RTP und sRTP)	SIP-Outbound-Proxy (SIP signalling) SIP-Outbound-Proxy (SIP signalling secure) SIP-Outbound-Proxy (SIP media-ports)

Notes for all products:

- The SIP UDP session timeout should be set to 90s (seconds).
- The URL for the customer domain (SIP server domain) is visible on the customer data sheet, which the customer has received in writing from Telecom Liechtenstein.

FL +423 237 74 00 | www.FL1.li | **CH** 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6