1 Allgemein gültige Anforderungen

Die Kundenfirewall und alle weiteren, beteiligten Netzwerk-Infrastrukturkomponenten (LAN-Switches, Router, WLAN-Komponenten, etc.) sollen den gesamten IP-Verkehr für Telefonie (UDP + TCP und alle Protokolle) vom internen Kunden-Netzwerk (LAN) zur VoIP-Infrastruktur der Telecom Liechtenstein (WAN) erlauben.

Das IP-Subnetz (C-Klasse) der Telecom Liechtenstein lautet: **80.66.238.0/24 (TCP + UDP auf alle Protokolle/Ports)**

Dieses IP-Subnetz wird seitens Telecom Liechtenstein für alle aktuellen, aber auch zukünftigen VoIP-Dienste verwendet. Durch die gesamtheitliche Freigabe des ganzen IP-Subnetzes ist die Kunden-Infrastruktur für zukünftige Erweiterungen vorbereitet und es ist zudem sichergestellt, dass alle IP-Adressen der geo-redundanten VoIP-Infrastruktur der Telecom Liechtenstein erreichbar sind.

Sollten kundenseitig vorhandene Security-Einschränkungen die Freischaltung aller IP-Protokolle/Ports nicht erlauben, sind die verwendeten Protokolle und Ports nachfolgend aufgeführt. Beim Auftreten allfälliger Beeinträchtigungen ist jedoch die oben aufgeführte Regel von Telecom Liechtenstein zu installieren, um Probleme auf der Firewall oder weiteren Komponenten auszuschliessen.

Es ist zwingend erforderlich, dass die Firewall keine wie auch immer gearteten Manipulationen durch Deep Inspection oder andere Mechanismen (Application Layer Gateway) an den Protokollen SIP und HTTP vornimmt. D.h. es sind die nachstehenden (oder andere ähnliche) Mechanismen zu deaktivieren:

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

1.1 Mehrere LAN-seitige Netzwerksegmente

Sind kundenseitig mehrere LAN-Segmente (z.B. ein separates Segment für WLAN-Infrastruktur) über Router / Firewall / Layer-3 Switch zusammen geschalten, ist darauf zu achten, dass alle Ports (insbesondere die RTP/sRTP-Ports) auch zwischen den LAN-Segmenten gegenseitig durchgeschalten werden.

1.2 Quality of Service (QoS) Funktionen im LAN

Um die erforderliche Qualität im LAN sicherzustellen, gibt es zwei Methoden:

- Ausreichende Bandbreite: Wird die komplette Infrastruktur des Kundenstandortes durchgängig mit Gigabit LAN umgesetzt, ist keine weitere QoS Unterstützung gefordert, aber dennoch dringend empfohlen.
- QoS Unterstützung und saubere Konfiguration der PC Clients: Die LAN Infrastruktur und die eingesetzten Layer 3 Switches müssen DiffServ Code Points (DSCP) von Endgeräten vertrauen (DSCP trusted) und diese in Class-of-Service (COS) übernehmen.

1.3 DNS-Server und NTP-Server Adressen

Wenn der Internetanschluss von Telecom Liechtenstein zur Verfügung gestellt wird, sind zusätzlich folgende IP-Adressen und Ports für die DNS- und NTP-Services freizuschalten.

DNS Name (URL)	IP-Adresse	Protokoll/Port	Beschreibung
	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 Einschränkungen auf einzelne Protokolle/Ports (LAN ➔ WAN)

Die Einschränkungen auf einzelne IP-Protokolle/Ports sollten nur gemacht werden, wenn entsprechende Security Richtlinien dies erfordern. Um zukünftig neue Dienste freischalten zu können kann es sein, dass seitens Telecom Liechtenstein zusätzliche IP-Protokolle/Ports notwendig werden. Diese werden jedoch stets innerhalb der oben aufgeführten C-Klasse liegen.

2.1 Für Produkt FL1 CommPlus (vPBX)

IP-Adresse/Netz	Protokoll:Port	Beschreibung
80.66.238.0/24	UDP:5082 (SIP) TCP:5061 (SIPs, TLS) UDP:10000-65535 (RTP, sRTP)	SIP-Outbound-Proxy (SIP Signalisierung) SIP-Outbound-Proxy (SIP Signalisierung secure) SIP-Outbound-Proxy (SIP Media-Ports)
	TCP:5075 (SIP) TCP:5076 (SIPs)	CSTA-Server für CTI-Clients CSTA-Server Secure für 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 für zentrales Telefonbuch *(TCP:389 nur, wenn Gigaset N510/N720)*
	TCP:80 (HTTP) TCP:443 (HTTPS) TCP:18443 (HTTPS)	Konfigurations-Server für Auto-Provisioning der IP-Endgeräte Konfigurations-Server für Provisioning der Softphone-Client Zugang zum CommPlus Kundenportal

2.2 Für Produkt FL1 Trunk

IP-Adresse/Netz	Protokoll:Port	Beschreibung
80.66.238.0/24	UDP:5083 (SIP) TCP:5063 (SIPs, TLS) UDP:10000-65535 (RTP und sRTP)	SIP-Outbound-Proxy (SIP Signalisierung) SIP-Outbound-Proxy (SIP Signalisierung secure) SIP-Outbound-Proxy (SIP Media-Ports)
	TCP:443 (HTTPS)	Zugang zum Trunk Kundenportal (in Planung)

2.3 Für Produkte FL1 SIP-Line (Kombi-Produkte mit VoIP und Convoip Line CH)

IP-Adresse/Netz	Protokoll:Port	Beschreibung
80.66.238.0/24	UDP:5082 (SIP) TCP:5061 (SIPs, TLS) UDP:10000-65535 (RTP und sRTP)	SIP-Outbound-Proxy (SIP Signalisierung) SIP-Outbound-Proxy (SIP Signalisierung secure) SIP-Outbound-Proxy (SIP Media-Ports)

Hinweise für alle Produkte:

- Die SIP UDP Session Timeout sollte auf 90s (Sekunden) eingestellt werden.
- Die URL für die Kundendomäne (SIP-Server Domain) ist auf dem Kundendatenblatt ersichtlich, welches der Kunde von Telecom Liechtenstein schriftlich erhalten hat.

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