

Firewall readiness

Application	Protocol	Destination port(s) ¹	Direction	IP range	QoS tag ²	Notes
Signalling (SIP)	TCP	5060	Outbound*	192.47.253.0/24	DSCP 46 COS 5	VoIP protocol
	UDP	5060				
	TCP/TLS	5061 ⁵				
Media (RTP)	UDP	10000-27999 ⁶	Outbound*	192.47.253.0/24	DSCP 46 COS 5	VoIP protocol
Reserved	TCP	9002	Outbound	192.47.253.0/24		For future expansion
HTTP	TCP	80	Outbound	Any ³		For portal access and phone provisioning
HTTPS		443				
HTTPS	TCP	8001	Outbound	192.47.253.0/24		Websocket for portal live updates
Network Time	UDP	123	Outbound	*.pool.ntp.org		Required for CPE and for displaying correct date/time on phones not behind a CPE. ⁴
IPSec IKE	UDP/TCP	500	Outbound*	192.47.253.0/24		Only needed if you use CPEs
IPSec ESP	IP UDP	Proto 50 4500		206.47.197.112/29		
				206.47.197.120/29 75.98.142.222 173.231.98.246		
DNS	UDP/TCP	53	Outbound	8.8.8.8 8.8.4.4		Only needed if you use CPEs

*It is assumed that you have a stateful firewall that will automatically allow the reverse flow. If not, you will need to allow all high ports inbound from our IP addresses, as the destination ports on your end will be random.

1. Source ports are assumed to be random high ports
2. When applicable, QoS tags should be supplied to the phones by your switches via an LLDP-MED network policy, and your network elements must be configured to enforce these tags with priority queuing.
3. If you do not allow direct internet access to all web addresses, we can supply the specific URLs that must be allowed. Note that the IPs used will be subject to change, so filtering by destination IP is not recommended.
4. If you don't use our CPEs and prefer to use your NTP this can be arranged.
5. SIP-TLS is optional. It will not work out of the box on most phones.
6. IMPORTANT- If you have a reliable SIP ALG in your firewall, opening SIP might be sufficient and these ports will open dynamically. If you have audio issues (One-Way sound or no sound at all), then we suggest you allow this range in your firewall. OR DEACTIVATE SIP ALG.