jtel Container Stack - Networking OnPrem

Introduction

The following page explains the networking information and requirements that must be considered if the jtel Container Stack is located OnPrem.

General Information

During the basic installation of a jtel Container Stack, a firewall is configured locally. This firewall blocks all incoming traffic unless specifically instructed otherwise.

To connect SBCs, PBXs or SIP-Trunks. the IP-Address must be specifically allowed in the firewall rules.

Outgoing traffic is generally not blocked.

Glossary

Hostname (Alias)	Function
acd-stack	The jtel Container Stack
SBC	The SBC/s Session Border Controller
PBX	The PBX/s
SIP-Trunk	SIP Trunk/s
FW	The Firewall/s
FQDN	Fully Qualified Domain Name **Example**: jtelacd.jtel.online
VSCode	VS Code Server Provides Fileshare access to maintenance staff

DNS Requirements

The customer must provide a Fully Qualified Domain Name (FQDN) for the stack, as well as

- DNS A record pointing FQDN to the VM's IP address
- DNS must be resolvable from both internal network and internet (if external access required)
- Wildcard or additional DNS records for subdomains:
  - `vscode.<FQDN>` (VS Code Server)
  - `<FQDN>` (main web interface)

Firewall - Required Inbound Ports

The customer's network firewall must allow the following inbound traffic to the VM:

Administrative Access

Port	Protocol	Purpose	Source
22	TCP	SSH (system administration)	JTEL support IPs or customer admin network

Web Interface

Port	Protocol	Purpose	Source
80	TCP	HTTP (redirects to HTTPS)	End users (agents, supervisors)
443	TCP	HTTPS (main web interface)	End users (agents, supervisors)

SIP Telephony (Primary FreeSWITCH)

Port	Protocol	Purpose	Source
5060	TCP/UDP	SIP signaling (unencrypted)	SIP trunks, PBX, softphones
5061	TCP	SIP over TLS (encrypted signaling)	SIP trunks, PBX, softphones
30000-34999	UDP	RTP media streams (voice/audio)	SIP endpoints, media gateways

Note: RTP port range (30000-34999) = 5000 ports = supports up to ~2500 concurrent calls

Firewall - Required Outbound Access

The VM requires unrestricted outbound internet access for the following:

Container Registry Access

Destination	Port	Protocol	Purpose
`dockerhub.jtel.de` or `jtelacr.azurecr.io`	443	HTTPS	Pull Docker container images

Critical: Without registry access, the stack cannot start or update.

Git Repository Access

Destination	Port	Protocol	Purpose
`bitbucket.org`	22	SSH	Fetch configuration updates, GitOps workflow

Note: Used during initial provisioning and for configuration management.

Let's Encrypt (SSL Certificates)

Destination	Port	Protocol	Purpose
`acme-v02.api.letsencrypt.org`	443	HTTPS	Automatic SSL certificate issuance and renewal

Operating System Updates

Destination	Port	Protocol	Purpose
`deb.debian.org`, `security.debian.org`	80, 443	HTTP/HTTPS	Security updates, package installation

Azure OAuth2 (Optional)

Destination	Port	Protocol	Purpose
`login.microsoftonline.com`	443	HTTPS	Azure AD authentication for VS Code Server

AI Services

Destination	Port	Protocol	Purpose
`api.openai.com`	443	HTTPS	GPT-based summarization, RAG chatbot (if enabled)
`api.mistral.ai`	443	HTTPS	Alternative LLM provider (if enabled)

Note: AI services are disabled by default.

Legacy

Windows Machines

In some cases, for example TAPI Monitoring services, a windows machine might still be installed. In this case, the following ports must be opened to enable the jtel service to access this machine

Description	Protocol	Source	Port(s)	Destination	Port(s)	Description
Remote Access	TCP + UDP	jtel Support	Any	All Windows	3389	RDP remote Access to Windows Systems.