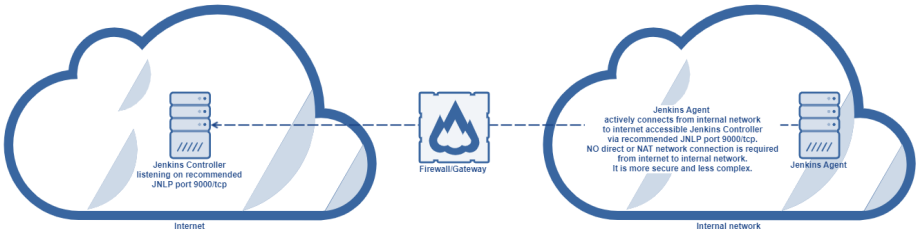
Executing Jenkins jobs when only one way network connection exists

Introduction

Usually, Jenkins controller and Jenkins agent are located in the same network, therefore it is quite easy to adopt Jenkins agents using SSH. This time we will talk about the situation when Jenkins controller and bunch of other DevOps tools are running in "network A" and Jenkins agents are running in "network B". Quite often connections from A to B are rejected, however, connections from B to A are accepted. There might be various reasons, in general, network B has elevated security expectations. The typical setup is Jenkins controller located in public cloud and Jenkins agent(s) located in a private customer network. Private customer network might be needed in such because some sort of higher data privacy requirements must be matched or some specialised hardware is present in customer premises and it cannot be accessible directly from the public internet.

Solution

The recommended solution is controller/agent setup, when the controller runs in a public environment and agent is running on a server located in a private network. The agent is also called "on-premise executor" (OPE). Jobs are then performing jobs/tasks on such agent in internal/private networks. Jenkins Agent has an active connection from the internal network to internet accessible Jenkins Master via recommended JNLP port tcp/9000 and keeps listening to builds/jobs. Port can be changed, but we will keep talking about 9000. NO direct or NAT network connection is required from the internet to internal network. It is a secure and simple solution.



Steps to setup

Detailed steps are described in following article:

Jenkins agent setup#DeploymentofJenkinsagentandconnectingtocontroller