Model Context Protocol (MCP) by Anthropic

A mini-project to teach myself about MCP, an open-source protocol to give AI models access to various external systems & services. For the project itself, I'll be using Docker MCP servers, to test giving a locally-hosted model access to a sandbox environment. The objective of the project will be to give the model enough autonomy to ssh into a sandbox environment and install tailscale, a VPN client.

Environment Set-Up

For this project, I'll primarily be using Docker containers running on isolated network (configured with OPNsense - see "Network Projects"). A high level of the containers, are as follows:

1. File Server with random test files (Ubuntu container)
2. MCP Server
3. Portainer (Container Admin GUI)
4. RHEL 8 server to host model