In the initial set-up, the SHIPS server is sand-boxed for security. It is separated from the in-house running programs and systems, essentially to prevent system failures, software vulnerabilities, network problems, power outages or malicious attacks from spreading.

A sandbox typically provides a tightly controlled set of resources for SHIPS programs to run in. Sand-boxing implies separation. The requirement of a fixed and free IP (sub-net) address already provides some detachment. Moreover, the SHIPS server should not be connected to the in-house LAN directly. Access shall be only over the internet at first, to provide adequate protective sand-boxing.

Typically a sandbox is implemented by executing software in a restricted operating system environment strictly controlling the resources that “emerging” processes may use. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted. By isolating, the risk of harming host machines or operating systems is minimized. It thus allows the running of programs without allowing the software to harm host devices. In the sense of providing a highly controlled environment, sandboxes may be seen as a specific example of virtualization.