Policies Provided in the GUI Blueprint:

- **SSH (Secure Shell)**: It's a network protocol and cryptographic security technology used for secure remote communication and data transfer over a potentially unsecured network, such as the internet. It provides a secure way to access and manage remote systems, execute commands, transfer files, and perform various network-related tasks.
- **Firewall**: A firewall in the context of an Ubuntu Server operating system (OS) is a network security system that helps protect the server from unauthorized access and network-based threats. It acts as a barrier between the server and the network or the internet, controlling incoming and outgoing network traffic based on a set of predefined rules or policies. (Important) **Ubuntu Server typically uses the Uncomplicated Firewall (UFW) as its default firewall management tool.**
- **SELinux (Security-Enhanced Linux)**: It's a mandatory access control (MAC) security framework that is integrated into the Linux kernel. It provides a powerful and fine-grained mechanism for controlling and enforcing access policies for various system resources, such as files, processes, network sockets, and devices
- **Fail2Ban**: It's a popular open-source intrusion prevention tool used on Linux-based servers, including Ubuntu Server, to enhance security by protecting against brute-force attacks and other malicious activities. Its primary purpose is to monitor log files for suspicious or repeated failed login attempts, and then take action to block or ban the IP addresses from which those attempts originate.
- **Intrusion Detection System** : An Intrusion Detection System (IDS) is a critical component of security infrastructure that helps monitor and safeguard computer systems and networks, including Ubuntu Server OS. Its primary purpose is to detect and respond to unauthorized or malicious activities, security policy violations, and potential threats.
- **TOR (The Onion Router)**: It's a privacy-focused network technology and software designed to enable anonymous communication over the internet. It was initially developed by the U.S. Navy for secure and anonymous online communication and later became a free and open-source project used by people around the world for various privacy and security purposes.

Some other policies:

- **File Permissions**: File permission hardening in Ubuntu Server OS refers to the process of enhancing and tightening the security of file permissions on the system to minimize the risk of unauthorized access and data breaches. This is a critical aspect of system security, as improper file permissions can lead to security vulnerabilities.
- **Password Policies**: Password policy hardening in Ubuntu Server OS involves implementing and enforcing stricter rules and practices related to user passwords. The goal is to enhance security by making it more difficult for unauthorized users to guess or crack passwords.

- **Backup and Recovery**: Backup and recovery hardening in Ubuntu Server OS involves implementing robust backup and recovery strategies to ensure the availability and integrity of your data, as well as to mitigate the impact of unexpected events such as data loss, hardware failures, or security breaches.
  Example: Develop comprehensive backup policies and procedures that define what data to back up, how frequently to perform backups, and where to store backup copies.