Secure Apache Web Server Deployment – CentOS Stream 9

Overview

This project documents the deployment and validation of an Apache HTTP Server on a CentOS Stream 9 staging system using enterprise-aligned Linux administration practices. The objective was to install and enable a web service while applying controlled network access and verifying system state through standard service and firewall management tools.

The process includes installing the httpd package, confirming the service is running and managed by systemd, and configuring firewalld to allow only required web traffic. Firewall rules are made persistent and validated to ensure consistency across reboots. Administrative access is handled separately from public services to reflect real-world production security expectations.

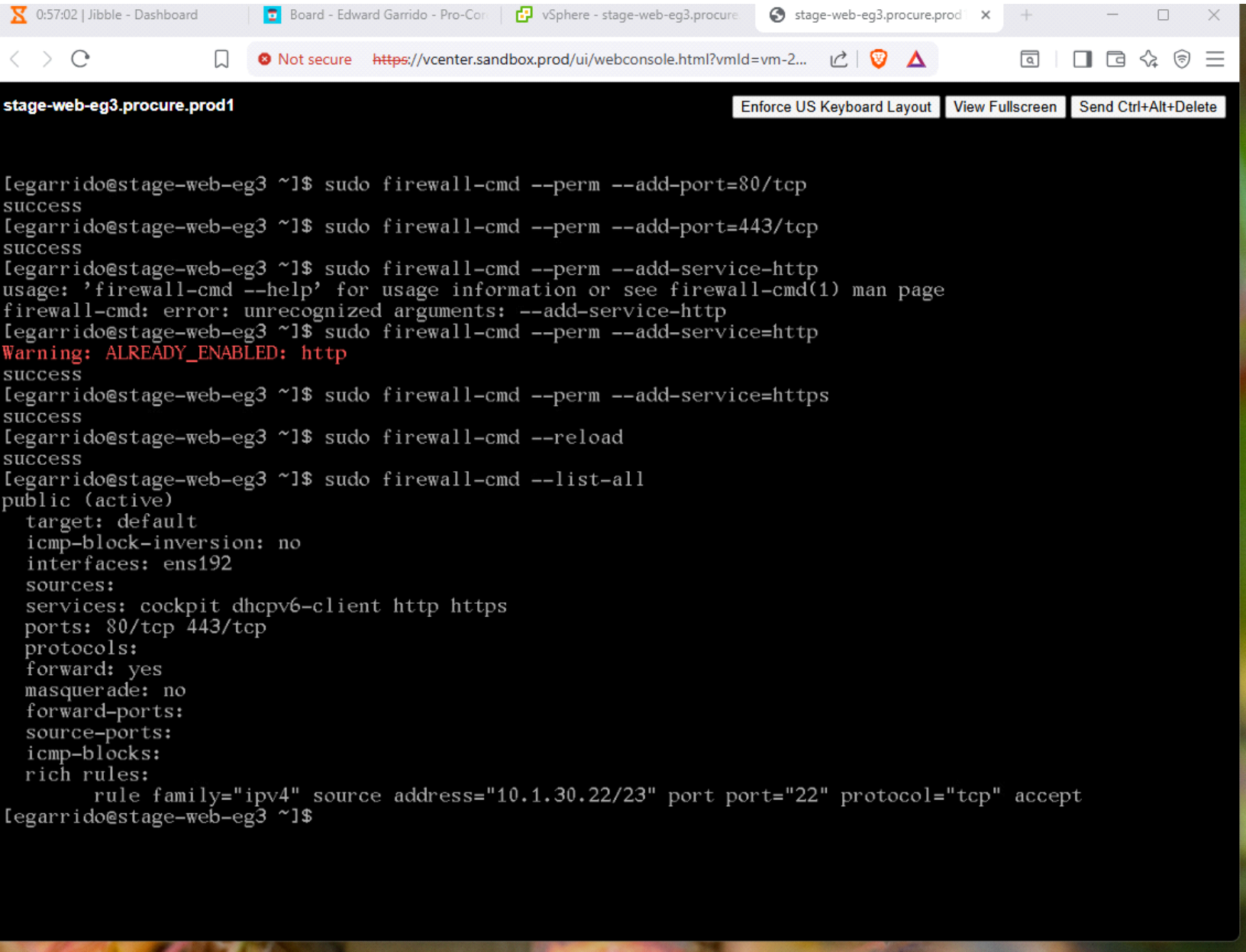
Result

The Apache HTTP Server was successfully installed, started, and verified as running. HTTP (port 80) and HTTPS (port 443) access were explicitly enabled through the firewall, and the active firewall configuration was reviewed to confirm only approved services and ports were exposed. SSH access remained restricted via a source-based rule, maintaining a reduced attack surface.

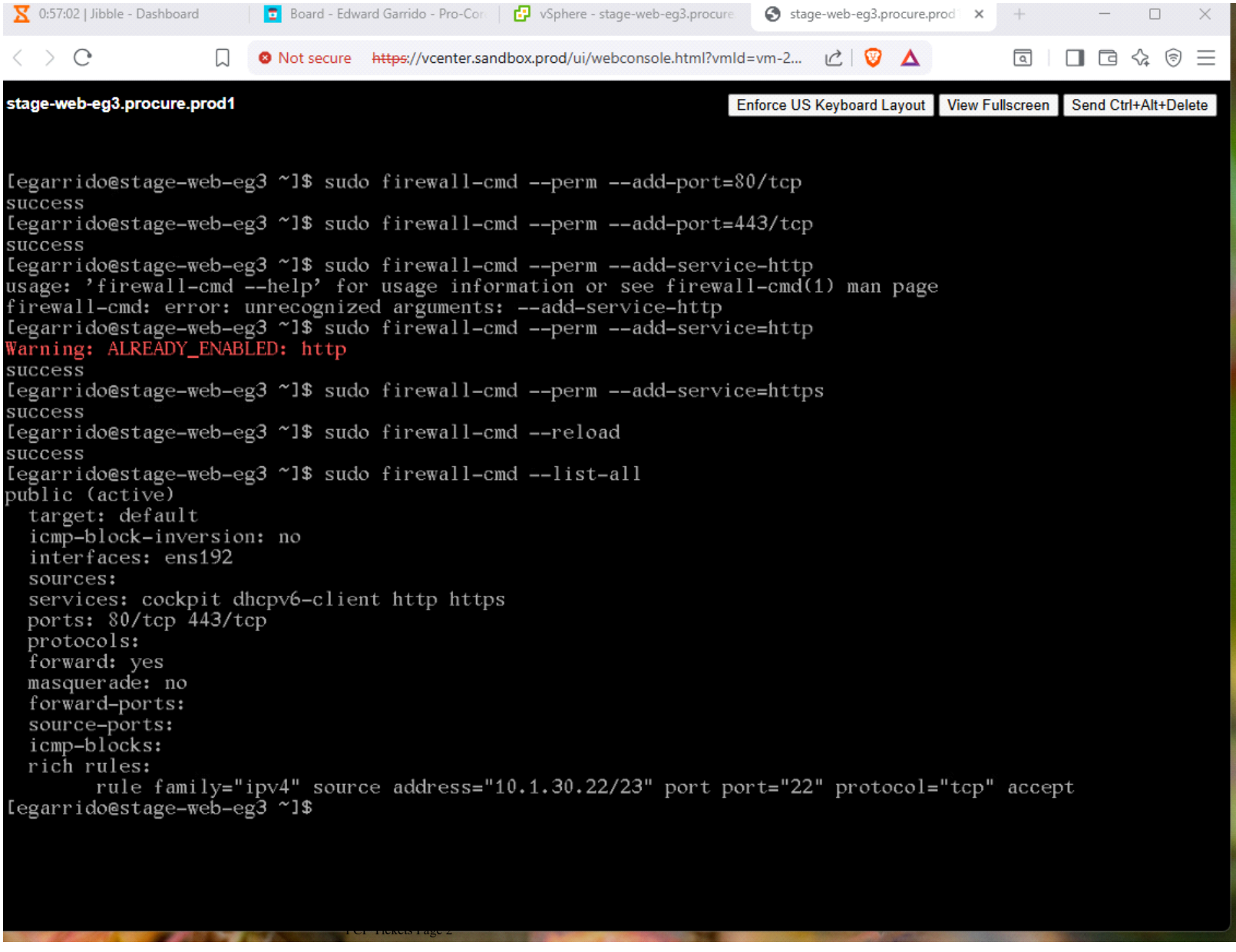
The final system state reflects a functional and secure staging web server with clear evidence of service availability, firewall enforcement, and configuration persistence.

At the end of the process, all screenshots were sanitized to remove or obscure sensitive information such as internal IP addresses, hostnames, and environment-specific identifiers.

This screenshot shows firewall configuration and verification on the stage-web-eg3 server. HTTP (port 80) and HTTPS (port 443) are enabled permanently using firewall-cmd, followed by a firewall reload. The final --list-all output confirms the active public zone, allowed services (http, https, cockpit), open ports (80/tcp, 443/tcp), and an existing rich rule restricting SSH (port 22) access to a specific source subnet. This validates that the web server is accessible while SSH access remains scoped for security.



This screenshot documents firewall configuration on the stage-web-eg3 server. HTTP (80/tcp) and HTTPS (443/tcp) are added permanently, the firewall is reloaded, and the active configuration is verified with firewall-cmd --list-all. The output confirms the public zone is active, web services (http, https) are enabled, required ports are open, and SSH (22/tcp) remains restricted via a scoped rich rule to an approved source subnet.



Summary

The screenshots confirm the completed firewall configuration on the staging web server. HTTP (80/tcp) and HTTPS (443/tcp) are permanently enabled and validated using firewall-cmd --list-all, showing that the web services are accessible as intended. At the same time, SSH access remains restricted through a scoped rich rule, ensuring administrative access is limited to an approved source. Together, these screenshots verify that the server is securely exposed for web traffic while maintaining controlled management access.