SSH Firewall Hardening Across Environments

This work documents the implementation and validation of strict, network-based SSH access controls using firewalld rich rules across multiple Linux environments. The configuration focuses on minimizing SSH exposure by explicitly allowing access only from trusted internal networks while blocking known or unauthorized external sources.

Permanent firewall rules are applied to reject SSH connections from a specific external IPv4 address and to permit SSH access on TCP port 22 solely from an approved internal subnet. Firewall changes are safely reloaded and verified to ensure rules are active, persistent, and correctly enforced without disrupting system availability.

The rule sets are consistently validated to confirm that allow and deny policies are functioning as intended, demonstrating a repeatable and environment-agnostic approach to SSH security hardening.

Result:

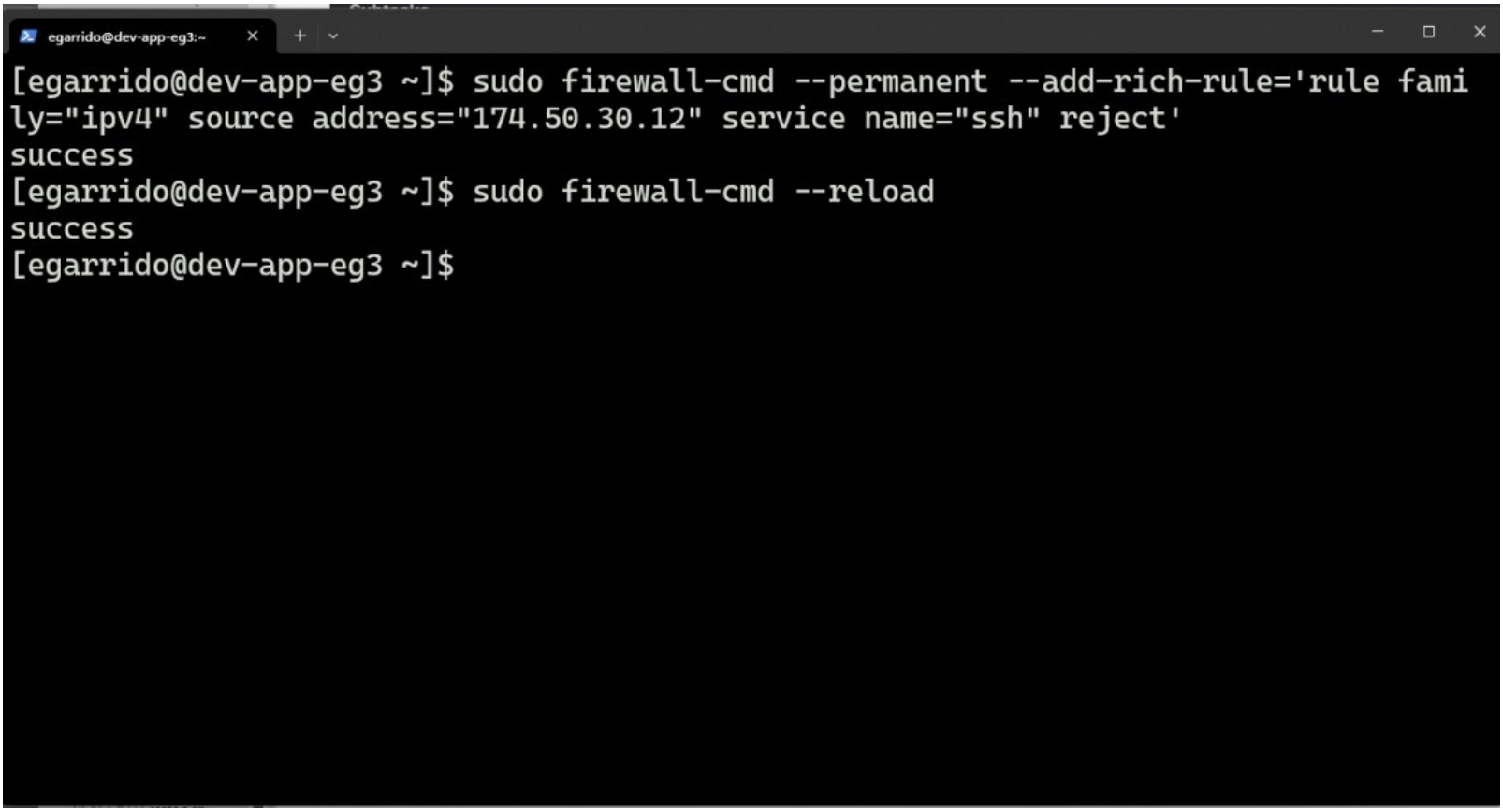
A consistently secured SSH configuration that reduces attack surface, enforces network-based access control, and demonstrates disciplined firewall management across development, staging, and performance environments.

Firewall Rich Rule to Block SSH from Specific Source

This step applies a permanent firewalld rich rule to explicitly reject SSH connections originating from a specified IPv4 source address. The rule targets the SSH service and enforces a deny action, adding an additional layer of access control beyond default firewall rules. The firewall configuration is then reloaded to activate the change immediately without disrupting other services.

Result:

SSH access from the specified source IP is blocked while normal SSH access remains available for authorized hosts, demonstrating fine-grained firewall control using firewalld rich rules.

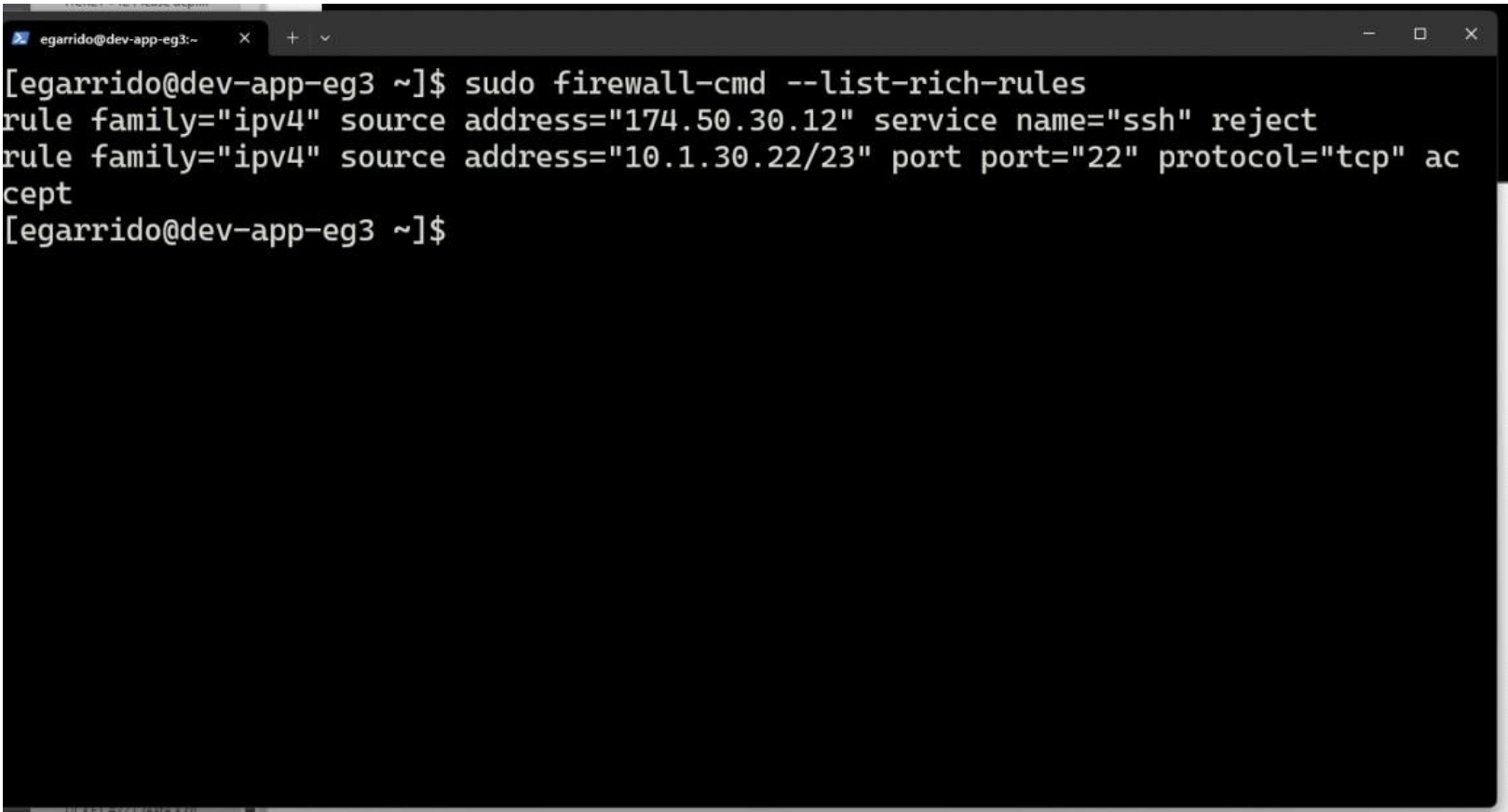


Firewall Rich Rule Verification for SSH Access Control

This output verifies the active firewalld rich rules applied to the system. One rule explicitly rejects SSH connections originating from a specific external IPv4 address, while another rule allows SSH access on TCP port 22 from an approved internal network range. Listing the rules confirms that both deny and allow policies are correctly enforced and ordered as intended.

Result:

Fine-grained SSH access control is in place, restricting unauthorized sources while permitting trusted network access through explicitly defined firewall rules.

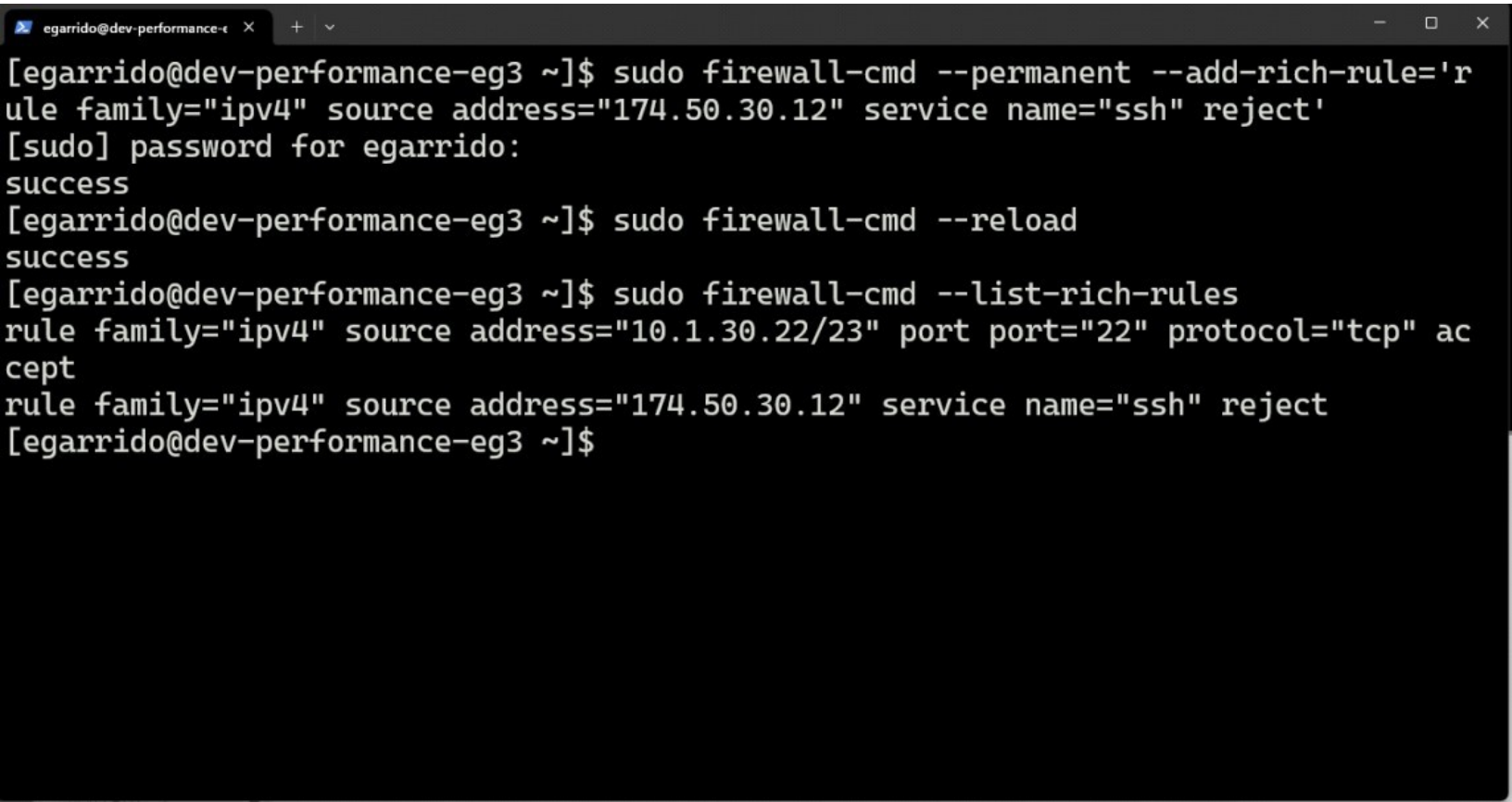


SSH Access Control via firewalld Rich Rules (Validation)

This sequence demonstrates the application and verification of firewalld rich rules to control SSH access on the system. A permanent rule is added to explicitly reject SSH connections from a specified external IPv4 address, followed by a firewall reload to apply the configuration. The active rule set is then listed to confirm both the deny rule for the external source and the allow rule permitting SSH access from an approved internal network range on TCP port 22.

Result:

SSH access is restricted to trusted internal networks while explicitly blocking unauthorized external sources, illustrating precise, policy-based firewall enforcement using firewalld rich rules.

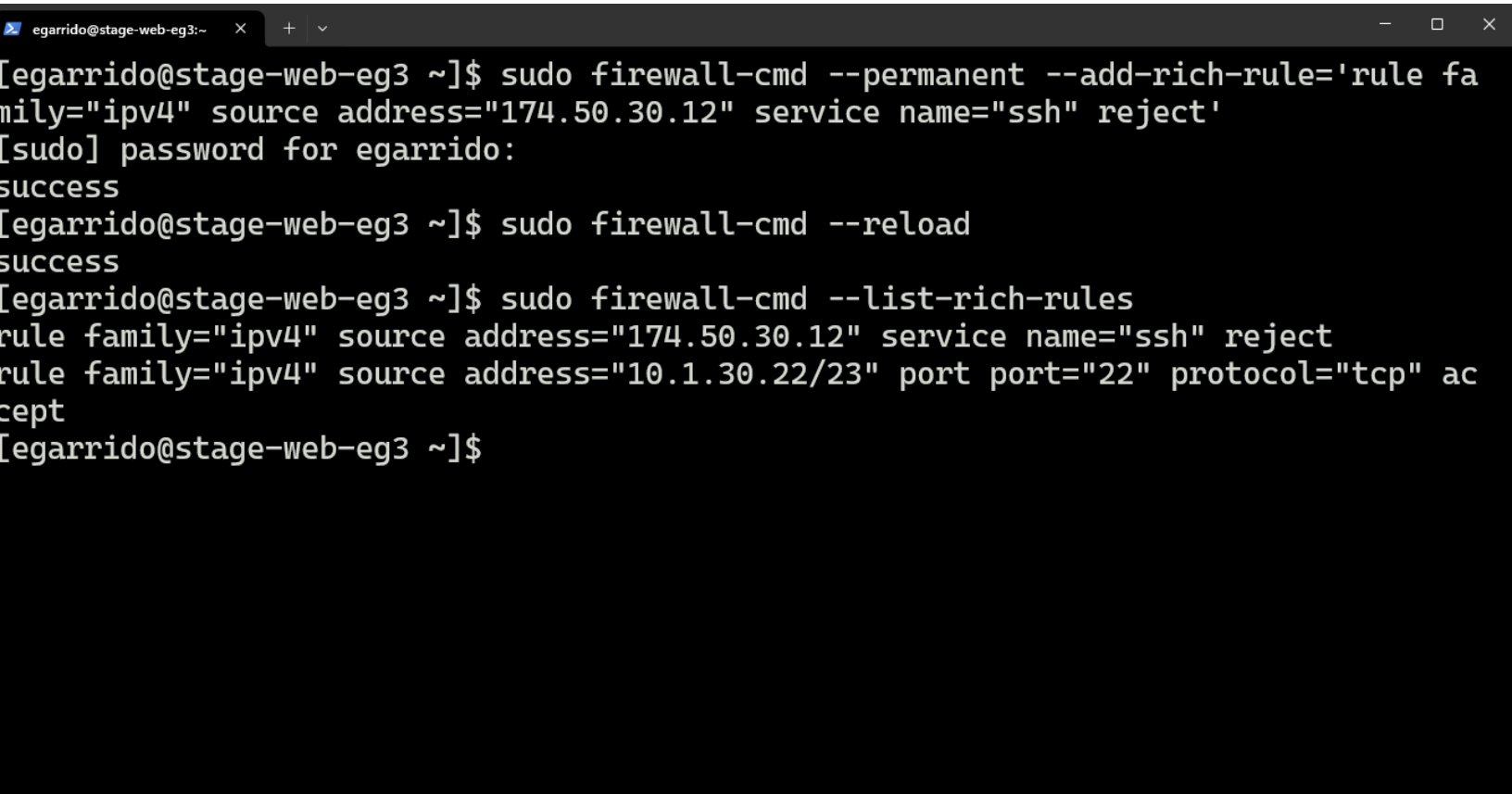


Consistent SSH Firewall Enforcement Across Environments

This step applies and verifies firewalld rich rules on a staging system to enforce consistent SSH access control. A permanent rule is added to explicitly reject SSH connections from a specified external IPv4 address, followed by a firewall reload to activate the change. The active rule set is then listed to confirm both the deny rule for the external source and the allow rule permitting SSH access from an approved internal network range on TCP port 22.

Result:

SSH access is consistently restricted to trusted internal networks while blocking unauthorized external sources, demonstrating uniform firewall hardening across environments using firewalld rich rules.

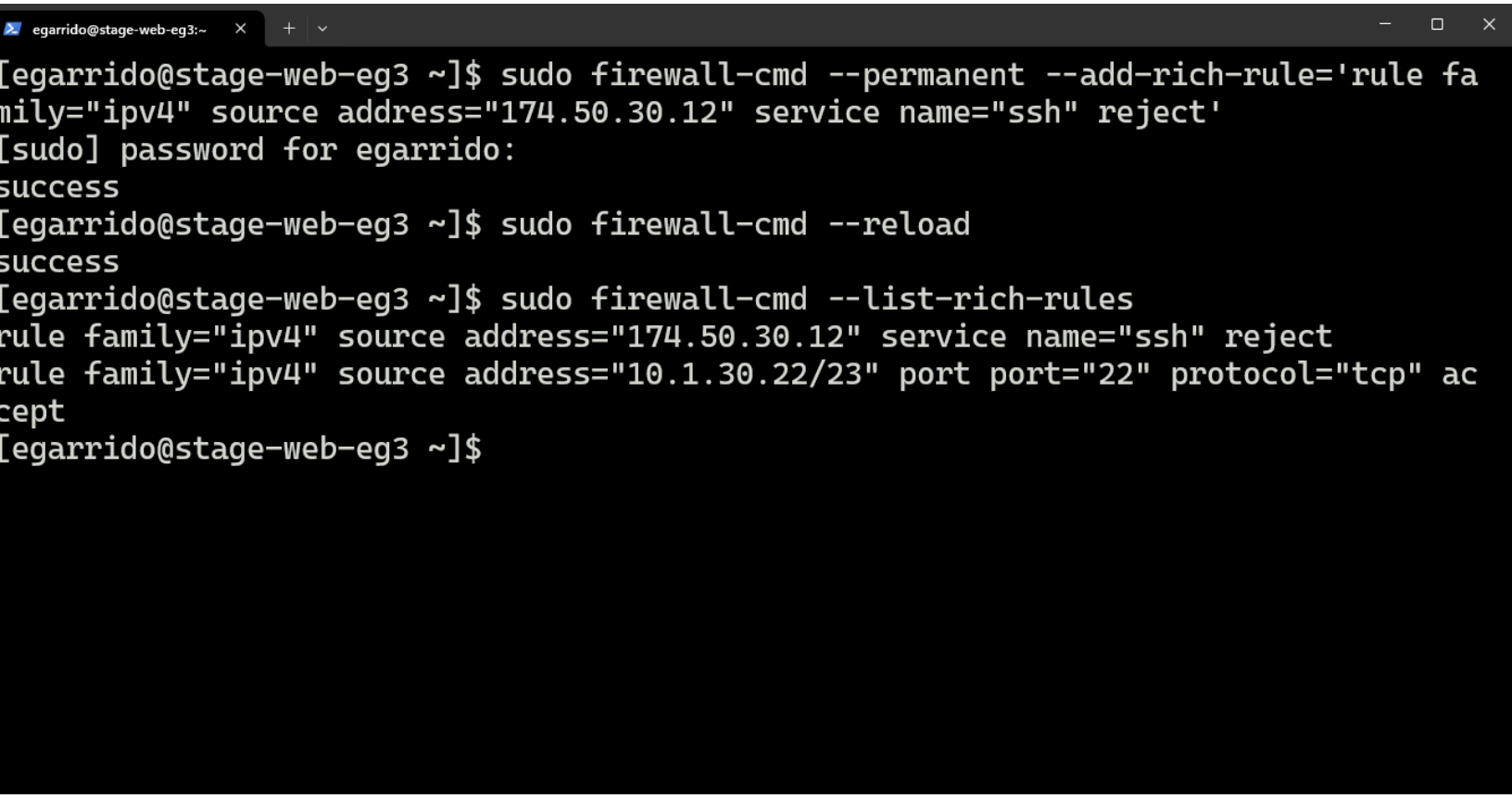


Staging Environment SSH Firewall Hardening

This step applies permanent firewalld rich rules on the staging web server to control SSH access. A deny rule explicitly rejects SSH connections from a specified external IPv4 address, and the firewall is reloaded to activate the configuration. The active rule set is then listed to verify that SSH access is allowed only from the approved internal network range on TCP port 22 while unauthorized external sources are blocked.

Result:

The staging environment enforces restricted, network-based SSH access using explicit allow and deny rules, ensuring consistent security posture and controlled remote administration.



Summary

This work implements and verifies network-based SSH access controls using firewalld rich rules across multiple environments. SSH access is explicitly restricted by rejecting connections from a specified external IPv4 address while allowing access only from an approved internal network range on TCP port 22. Firewall configurations are applied permanently, reloaded safely, and validated to ensure rules are active and enforced as intended.

Outcome:

Consistent, hardened SSH access control that limits exposure to trusted networks while blocking unauthorized external sources, demonstrating precise and repeatable firewall security management.