Firepower Playbook:

General Hardening:

1. Change Admin Passwords:
    a. configure terminal
    b. username admin password <strong-password> privilege 15end
    c. write memory
2. list all current connections to firewall:
    a. show user-identity user active
3. show all user accounts to check for other admin accounts:
    a. show running-config user
4. End current sessions to the firepower:
    a. clear aaa local user lockout <username>
    b. This is equivalent to PA: delete admin-sessions username <username>
5. Disable insecure management services:
    a. System > Configuration > Management Access > Modify Access Control Policy
        i. This includes configuration for access to the management plane from the management interface and data interfaces.
    b. configure terminal
    c. line vty 0 15
    d. transport input ssh
    e. end
6. Create security policies

Other troubleshooting:

1. Network Connectivity Troubleshooting:
    a. Check interface status and configurations:
        i. show interface GigabitEthernet0/0
    b. Verify routing table:
        i. show ip route
    c. Ensure correct NAT configurations (if applicable):
        i. show nat
    d. Check access control policies for any blocking rules:
        i. show access-list
    e. Review traffic logs for dropped packets:
        i. show access-list logging
2. Security Hardening:
    a. Enable basic threat detection:
        i. configure terminal
        ii. threat-detection basic-threat
        iii. end
    b. Enable intrusion prevention system (IPS):
        i. configure terminal
        ii. ips enable

        iii. end
3. Update Software and Signatures:
    a. Check for available updates:
        i. configure terminal
        ii. system-update check
        iii. end
    b. Install updates (if available):
        i. configure terminal
        ii. system-update install
        iii. end
4. Logging and Monitoring:
    a. Configure syslog server for centralized logging:
        i. configure terminal
        ii. logging host <syslog-server-ip> udp/514
        iii. end
    b. Enable logging for access control policies:
        i. configure terminal
        ii. logging enable
        iii. logging buffer-size 16384
        iv. end
5. Documentation and Reporting:
    a. Generate configuration backups:
        i. configure terminal
        ii. write memory
        iii. end
    b. Generate security audit reports:
        i. configure terminal
        ii. show security-report
        iii. end