# Palo Alto Firewalls

***************More specific rules must precede the more general ones (rules are evaluated top to bottom)***************
**Configure mode prompt: #, normal mode prompt: >**

**DON'T FORGET TO COMMIT**

1. Find management IP: `show interface management`
   ****Web GUI is only accessible via HTTPS****
   No web gui: knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cli0CAC
   a. Set static management IP address:
      `configure, set deviceconfig system type static, set deviceconfig system ip-address <ip address> netmask <netmask> default-gateway <default gateway> dns-setting servers primary <DNS ip address>`
      i. Set static IP: Device-> Setup -> Interfaces -> Management
      ii. Set DNS server: Device -> Setup -> Services
      iii. Go to the new IP you set to manage the firewall
2. Change passwords:
   a. Admin: Device -> Administrators -> Click on username, change password
      i. `configure, set mgt-config users admin password`
      ii. Other admins: `show admins, delete mgt-config users <admin>`
   b. Local Users: Device -> Local User Database
      i. `show user user-ids all`
      ii. `configure, set mgt-config users <name> password`
   c. Adding a new user:

```
configure
set mgt-config users <name> password
set mgt-config users <name> permissions role-based <role profile>
```

3. Check for user certificates: see guide
4. Check for SSH keys: see guide
5. ACL for accessing management interface: Device-> Setup -> Interfaces -> Management
   `configure, set deviceconfig system permitted-ip <ipaddress/netmask>`
6. Go through Network tab to get a better understanding of what's going on
   `show config running`
7. Check security rules: Policies -> Security
   a. Disable rules allowing unneeded services
   b. These rules are applied top to bottom
   c. Remember that these rules are evaluated after DoS Protection Policies
   d. Overall vision for applying security policies:
      i. Create a grouping (could be an object/zone/whatever…)
      ii. Create security profiles (can group security profiles into a security profile group)
      iii. Apply policies using security profiles/security profile groups
8. Check NAT rules: Policies -> NAT
9. Check port forwarding rules: Policies -> Policy Based Forwarding
10. Check service definitions (someone may've bound a bad port to a service): Objects -> Services
11. Prevent defined attacks: Objects -> Enable Security Profiles