Palo alto checklist

1. Change password

* Configure
* Set mgt-config users <name> password

1. Get rid of additional users

* Delete mgt-config users administrator

1. Download update, get out of configure

* Request system software check
* Request system software download version 8.1.0
* Request content upgrade check

Check download status after each step and download next version need to go out of configure mode for it, so a little annoying, 8.1.0 finished downloading after step 5 for me, 8.1.13 after step 6

* Show jobs id <job id>
* Request system software download version 8.1.13
* Request content upgrade check
* Request content upgrade download latest
* Request content upgrade install version latest
* Request system software install version 8.1.13

1. Get rid of nat for palo

* Delete rulebase nat rules PA

1. Add new management profile, because i cant figure out how to get rid of mgmt profiles on interfaces from cli, so limiting them until i get into the gui

* Set network profiles interface-management-profile ping ping yes

1. Remove management profile from interfaces

* Set network interface ethernet ethernet1/1 layer3 interface-management-profile ping
* Set network interface ethernet ethernet1/2 layer3 interface-management-profile ping
* Set network interface ethernet ethernet1/3 layer3 interface-management-profile ping
* Set network interface ethernet ethernet1/4 layer3 interface-management-profile ping

1. Set management service settings

* Set deviceconfig system service disable-http yes
* Set deviceconfig system service disable-telnet yes
* Set deviceconfig system service disable-snmp yes
* Set deviceconfig system service disable-icmp yes
* Set deviceconfig system service disable-ssh yes

1. Hopefully you got a gui at this point, if so:

* Commit, just in case
* Request restart system

GUI

1. Network > zone security profiles
2. Refine mgmt config
3. Remove application filter
4. Remove HIP object/policy
5. Delete data pattern > backup
6. Delete custom object > vulnerability
7. Remove dhcp on all interfaces
8. Remove dns proxy
9. Remove mdm
10. Set rules

* Set rulebase security rules <name> from <source zone> source <source address> to <destination zone> destination <destination address> application <application> service application-default action allow
* Set rulebase security rules fedora from any to Public destination 172.20.241.40 application pop3 service application-default action allow
* Set rulebase security rules fedora application smtp
* Set rulebase security rules to-splunk from any to Public destination 172.20.241.20 application splunk service application-default action allow
* Set rulebase security rules to-splunk application rsh
* Set rulebase security rules to-splunk application web-browsing
* Set rulebase security rules to-splunk application ssl
* Set rulebase security rules ubuntu from any to User destination 172.20.242.10 application dns service application-default action allow
* Set rulebase security rules ubuntu application ntp
* Set rulebase security rules win10 from External source 172.31.21.5 to User destination 172.20.242.200 application dns service application-default action allow
* Set rulebase security rules mysql from Public source 172.20.241.30 to Internal destination 172.20.240.20 application mysql service application-default action allow
* Set rulebase security rules ad from any to User destination 172.20.242.200 application dns service application-default action allow
* Set rulebase security rules web from any to External destination any application web-browsing service application-default action allow
* Set rulebase security rules web application ssl
* Set rulebase security rules web application dns
* Set rulebase security ms-update from User source 172.20.242.200 to External destination any application ms-update service application-default action allow
* Set rulebase security ms-update source 172.20.242.100
* Set rulebase security yum from Internal source 172.20.240.10 to External destination any application yum service application-default action allow
* Set rulebase security yum from Public source 172.20.241.20
* Set rulebase security yum source 172.20.241.30
* Set rulebase security yum source 172.20.241.40
* Set rulebase security apt from internal source 172.20.240.20 to External destination any application apt service application-default action allow