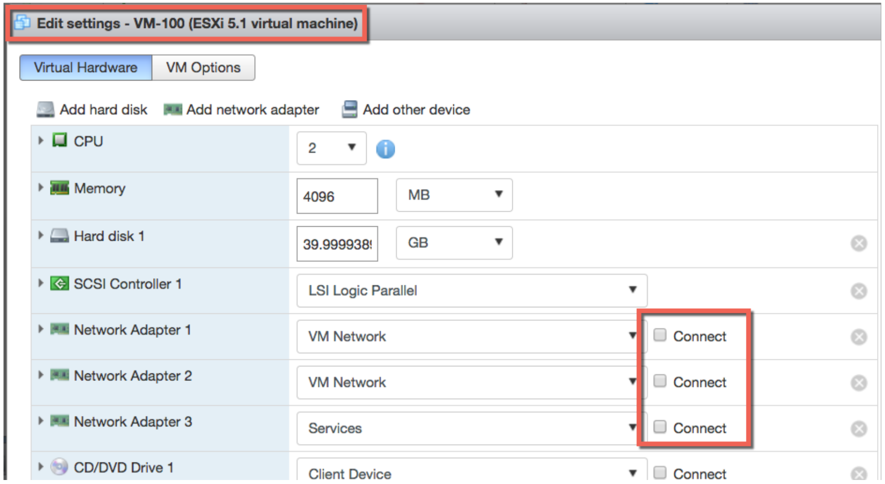
Quick Get Started Guide to Securing Your Virtual Firewall Appliance

When you first enter the room, your first task should be securing your firewall appliance, the below check sheet with CLI commands should help you.

1 Shutdown your interfaces and log in to console.

   a. If it's a VM-100/50 then edit virtual machine settings and disconnect Network Adapter settings interfaces



Edit settings - VM-100 (ESXi 5.1 virtual machine)

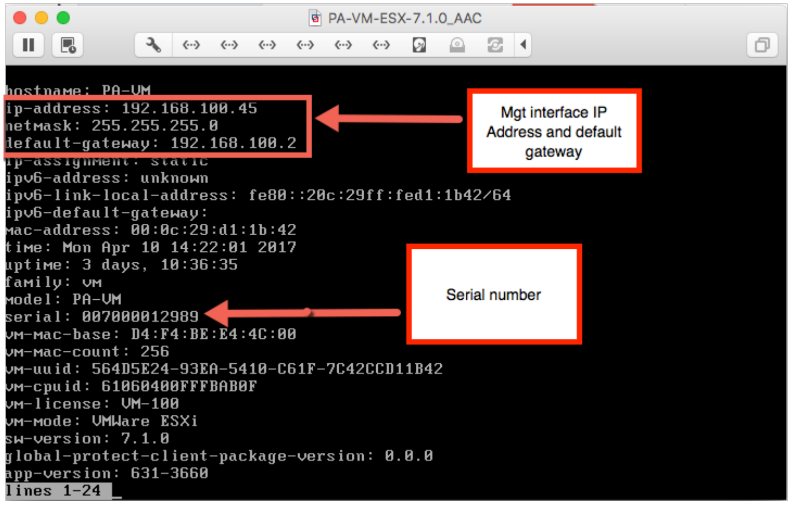
CPU	2		
Memory	4096	MB	
Hard disk 1	39.999938(	GB	
SCSI Controller 1	LSI Logic Parallel		
Network Adapter 1	VM Network		□ Connect
Network Adapter 2	VM Network		□ Connect
Network Adapter 3	Services		□ Connect
CD/DVD Drive 1	Client Device		□ Connect

   b. If it's hardware appliance, easiest way is to shut down connecting switch's port.

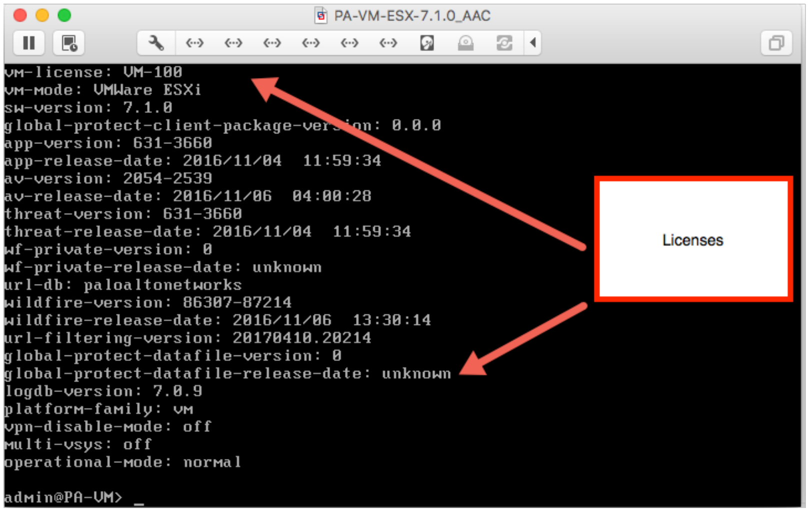
      i. On the console, you can shut down link state of data interfaces using this command in configure mode (#): "set network interface ethernet ethernet1/<> link-state down" and don't forget to commit

2 Log into your firewall appliances console with default username "admin" and default password "admin".

a. Check and see if licenses are installed and management interface ip address with “>show system info”



```
hostname: PA-VM
ip-address: 192.168.100.45
netmask: 255.255.255.0
default-gateway: 192.168.100.2
ip-assignment: static
ipv6-address: unknown
ipv6-link-local-address: fe80::20c:29ff:fed1:1b42/64
ipv6-default-gateway:
mac-address: 00:0c:29:d1:1b:42
time: Mon Apr 10 14:22:01 2017
uptime: 3 days, 10:36:35
family: vm
model: PA-VM
serial: 007000012989
vm-mac-base: D4:F4:BE:E4:4C:00
vm-mac-count: 256
vm-uuid: 564D5E24-93EA-5410-C61F-7C42CCD11B42
vm-cpuid: 61060400FFFBAB0F
vm-license: VM-100
vm-mode: VMWare ESXi
sw-version: 7.1.0
global-protect-client-package-version: 0.0.0
app-version: 631-3660
lines 1-24 _
```



```
vm-license: VM-100
vm-mode: VMWare ESXi
sw-version: 7.1.0
global-protect-client-package-version: 0.0.0
app-version: 631-3660
app-release-date: 2016/11/04  11:59:34
av-version: 2054-2539
av-release-date: 2016/11/06  04:00:28
threat-version: 631-3660
threat-release-date: 2016/11/04  11:59:34
wf-private-version: 0
wf-private-release-date: unknown
url-db: paloaltonetworks
wildfire-version: 86307-87214
wildfire-release-date: 2016/11/06  13:30:14
url-filtering-version: 20170410.20214
global-protect-datafile-version: 0
global-protect-datafile-release-date: unknown
logdb-version: 7.0.9
platform-family: vm
vpn-disable-mode: off
multi-vsys: off
operational-mode: normal

admin@PA-VM> _
```

b. If your VM-100/50 firewall appliance is licensed then take a snapshot, if not then take a snapshot after it’s licensed. When you revert back to your snapshot you won’t lose your licenses.

3 Check and delete any non-essential admin accounts.

a. Use cli command: “show admins”

b. To delete user accounts, use cli command in configure mode: “delete mgt-config users <admin user account name>” and don’t forget to commit change

4 Change your admin password with cli command: “set mgt-config users admin password”. Don’t forget to commit change

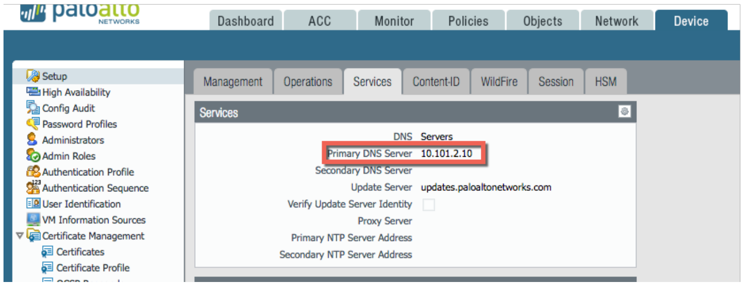
5 Make sure only https, ssh and ping are enabled on your management interface. After you have gained initial access to the Web UI you should disable https and ssh access on your management interface

  a. Use cli command to display services and management interface: “>show system services”
  b. Disable any unnecessary management interface services with cli command in configure mode: “set deviceconfig system service disable-<service> <yes or no>”

6 Configure the management interface so you can access the WebUI, can license your appliance, can install dynamic updates, can enable Wildfire and can enable URL category service. You can configure all the features of the firewall via the command line but it’s much quicker to configure the appliance using the WebUI.

  a. The default management IP address of the virtual firewall appliance is set to dhcp client. You will probably have to change it to an IP address that can access the internet and Palo Alto Networks update server: updates.paloaltonetworks.com where you can download dynamic updates and get url categorizations. The management interface also is used to submit copies of suspicious files to Wildfire cloud sandbox for categorization and if necessary signature generation.
  b. Use the cli command to configure mgt interface’s IP address, default gateway and preferred dns server in configure mode: “set deviceconfig system ip-address <mgt IP address> netmask <mask> default-gateway <your default gateway> dns-setting <preferred dns-server address.

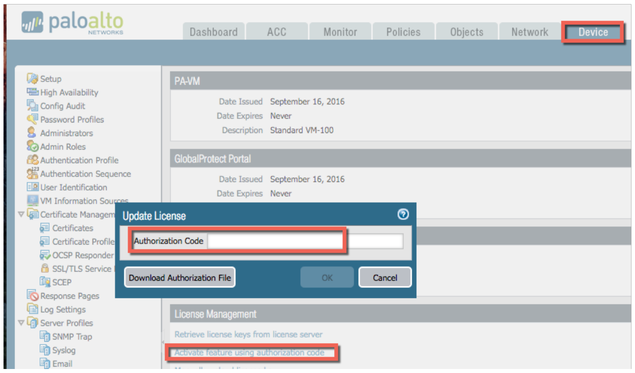
7 Access the management interfaces WebUI, https://<mgt ip address>. In WebUI’s Device tab>Setup>Services and confirm you have a preferred dns server configured for your management interface.



Services

DNS	Servers
Primary DNS Server	10.101.2.10
Secondary DNS Server	
Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	□
Proxy Server	
Primary NTP Server Address	
Secondary NTP Server Address	

8 If you’re VM-100/50 is unlicensed, navigate to the WebUI Device tab>Licenses>License Management and select “Activate feature using authorization” code. Enter the authcode that was provided to you.



PA-VM

Date Issued September 16, 2016
Date Expires Never
Description Standard VM-100

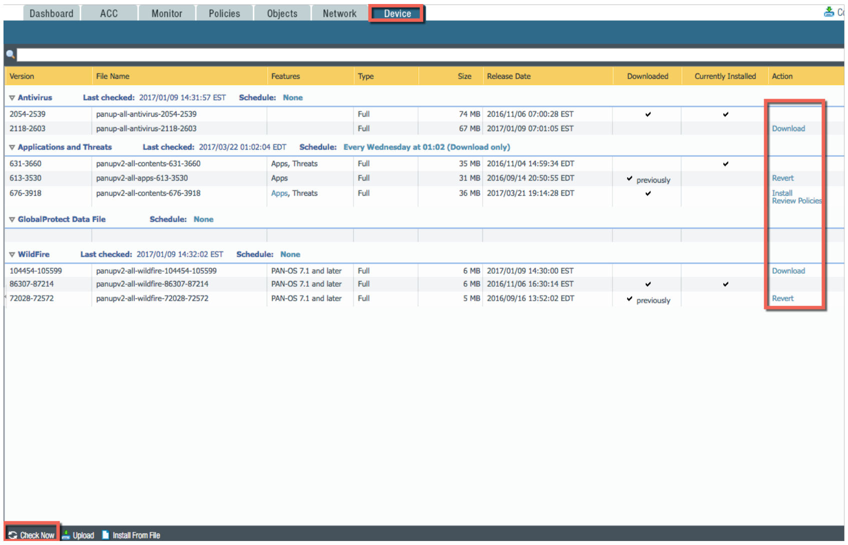
GlobalProtect Portal

Date Issued September 16, 2016
Date Expires Never

Authorization Code

License Management

9 After you install licenses with authcode or if already licensed, navigate to WebUI Device tab>Dynamic Updates. You will need to download the most current AppID and ContentID signatures. At the bottom of the Web page select “Check Now” and then download and install signatures. Continue to “Check Now” and download and install updates until there are no more. You will then need to commit the changes in your WebUI.



Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action
Antivirus	**Last checked:** 2017/01/09 14:31:57 EST	**Schedule:** None						
2054-2539	panup-all-antivirus-2054-2539		Full	74 MB	2016/11/06 07:00:28 EST	✓	✓	
2118-2603	panup-all-antivirus-2118-2603		Full	67 MB	2017/01/09 07:01:05 EST			Download
Applications and Threats	**Last checked:** 2017/03/22 01:02:04 EDT	**Schedule:** Every Wednesday at 01:02 (Download only)						
631-3660	panupv2-all-contents-631-3660	Apps, Threats	Full	35 MB	2016/11/04 14:59:34 EDT		✓	
613-3530	panupv2-all-apps-613-3530	Apps	Full	31 MB	2016/09/14 20:50:55 EDT	✓ previously		Revert
676-3918	panupv2-all-contents-676-3918	Apps, Threats	Full	36 MB	2017/03/21 19:14:28 EDT	✓		Install Review Policies
GlobalProtect Data File	**Schedule:** None							
WildFire	**Last checked:** 2017/01/09 14:32:02 EST	**Schedule:** None						
104454-105599	panupv2-all-wildfire-104454-105599	PAN-OS 7.1 and later	Full	6 MB	2017/01/09 14:30:00 EST			Download
86307-87214	panupv2-all-wildfire-86307-87214	PAN-OS 7.1 and later	Full	6 MB	2016/11/06 16:30:14 EST	✓	✓	
72028-72572	panupv2-all-wildfire-72028-72572	PAN-OS 7.1 and later	Full	5 MB	2016/09/16 13:52:02 EDT	✓ previously		Revert

10 Take a snapshot of your firewall appliance’s running configuration after it is fully licensed via device tab>Operations>Save named configuration snapshot. You can revert to this snapshot and keep your licenses.

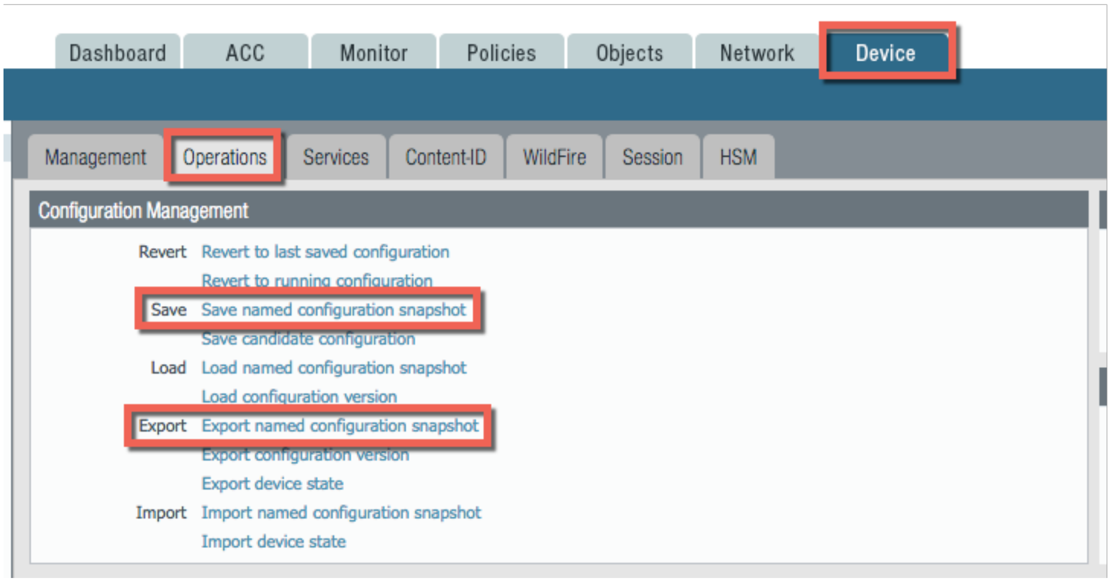
11 Follow the instructions in CCDC Moodle slide deck and videos to configure your interfaces, zones and security policies. The instructions show you how to configure a simple 2 zone deployment (Trust/Untrust) on your VM-100 using Layer 3 interfaces and destination NATs to configure secure access from and to

your internal clients and servers. You can add interfaces and zones to segment your traffic for better lateral, east-west security. If you set up your security policies to inspect all traffic moving across your internal zones you will limit the impact of an intrusion.

12 You should add an Interface management profile to your internal interface so you can only access your WebUI from on your interface assigned to your trust zone. Turn off https and ssh access on your management interface which is accessible from public Internet.

13 Hardware appliances are preconfigured to operate in Virtual Wire Mode. A virtual wire is a transparent bridge with ingress and egress interface so you don't need to configure any IP address. The firewall appliance will filter traffic between your ingress and egress interfaces per your security policies. It is easy to set up but you lose the firewall features requiring IP addresses such as VPNs.

14 Make a backup your VM-100/50's configuration and exporting it. In the WebUI navigate to Device tab>Setup>Operations>Save named configuration snapshot & Export named configuration snapshot.


Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Management
Operations
Services
Content-ID
WildFire
Session
HSM
Configuration Management
Revert
Revert to last saved configuration
Revert to running configuration
Save
Save named configuration snapshot
Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version
Export device state
Import
Import named configuration snapshot
Import device state

15 If you lose access to your firewall appliance you can reset to factory default configuration. If you do this you will lose your license so you will have to relicense your firewall appliance

a. To access maintenance mode in your VM-100, reboot the virtual machine and during the boot process, hit any key type "maint" and select factory reset.

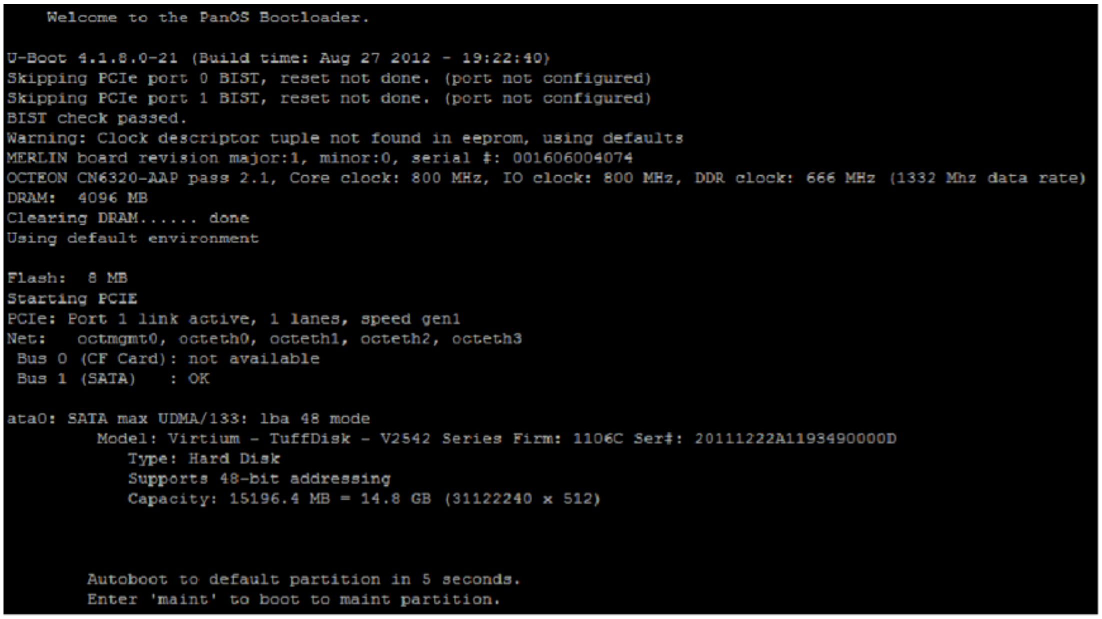
b. To access maintenance mode on the hardware appliance follow these steps:

c. Connect the Console cable, which is provided by Palo Alto Networks, from the "Console" port to a computer, and use a terminal program (9600,8,n,1) to connect to the Palo Alto Networks device.
Note: A USB-to-serial port will have to be used if the computer does not have a 9-pin serial port.

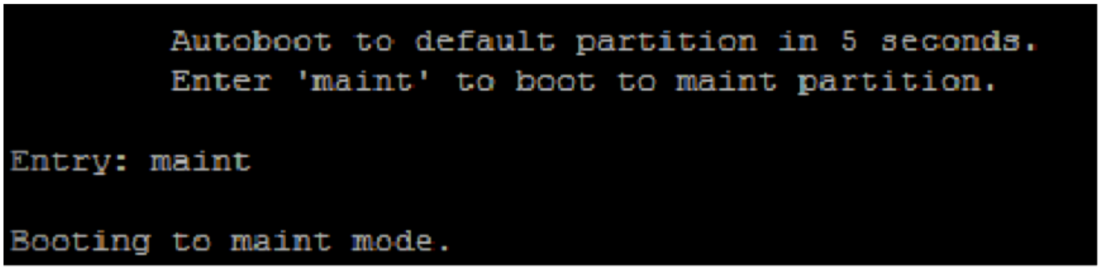
d. Power on to reboot the device.

e. During the boot sequence, the screen should look like this:

f. Type ***maint*** to enter maintenance mode.



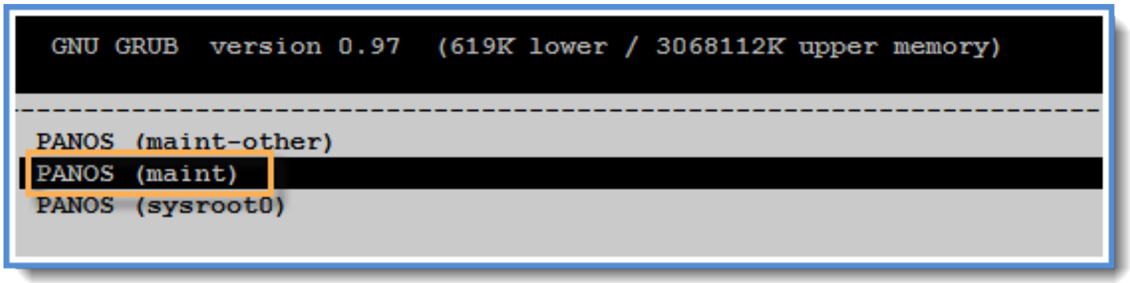
```
    Welcome to the PanOS Bootloader.

U-Boot 4.1.8.0-21 (Build time: Aug 27 2012 - 19:22:40)
Skipping PCIe port 0 BIST, reset not done. (port not configured)
Skipping PCIe port 1 BIST, reset not done. (port not configured)
BIST check passed.
Warning: Clock descriptor tuple not found in eeprom, using defaults
MERLIN board revision major:1, minor:0, serial #: 001606004074
OCTEON CN6320-AAP pass 2.1, Core clock: 800 MHz, IO clock: 800 MHz, DDR clock: 666 MHz (1332 Mhz data rate)
DRAM:  4096 MB
Clearing DRAM...... done
Using default environment

Flash:  8 MB
Starting PCIE
PCIe: Port 1 link active, 1 lanes, speed gen1
Net:   octmgmt0, octeth0, octeth1, octeth2, octeth3
 Bus 0 (CF Card): not available
 Bus 1 (SATA)    : OK

ata0: SATA max UDMA/133: lba 48 mode
         Model: Virtium - TuffDisk - V2542 Series Firm: 1106C Ser#: 20111222A1193490000D
            Type: Hard Disk
            Supports 48-bit addressing
            Capacity: 15196.4 MB = 14.8 GB (31122240 x 512)



        Autoboot to default partition in 5 seconds.
        Enter 'maint' to boot to maint partition.
```



```
        Autoboot to default partition in 5 seconds.
        Enter 'maint' to boot to maint partition.

Entry: maint

Booting to maint mode.
```

g. **PAN-OS 7.1 NOTE:** When performing this on PAN-OS 7.1, you will see a "CHOOSE PANOS" screen with the following options: **PANOS (maint-other)**, **PANOS (maint)** or **PANOS (sysroot0)**. Please choose **PANOS (maint).** Press enter to continue.

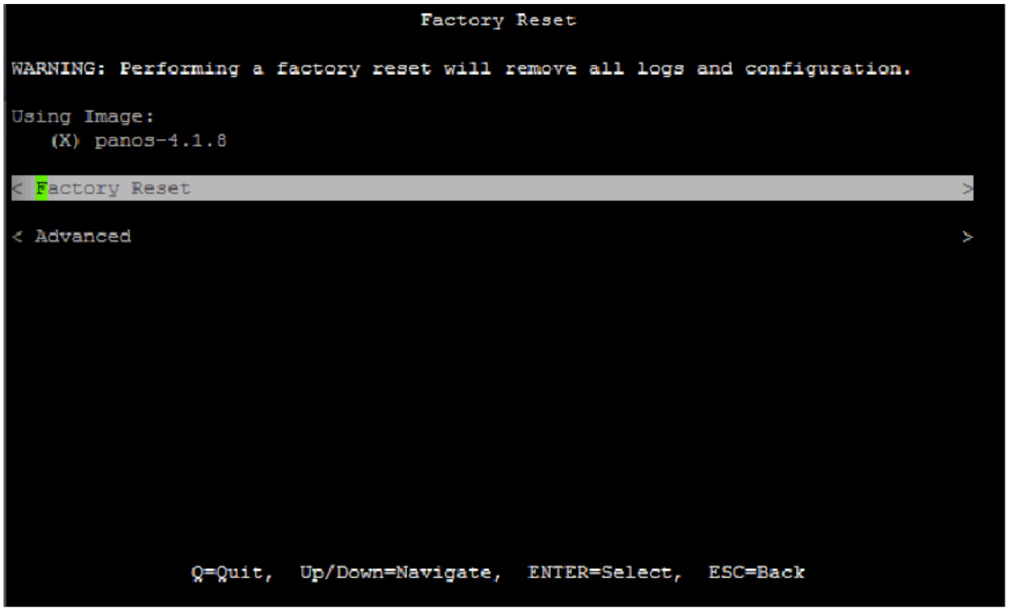
PAN-OS 7.1 GNU GRUB boot menu.



```
 GNU GRUB  version 0.97  (619K lower / 3068112K upper memory)

------------------------------------------------------------------
 PANOS (maint-other)
 PANOS (maint)
 PANOS (sysroot0)
```

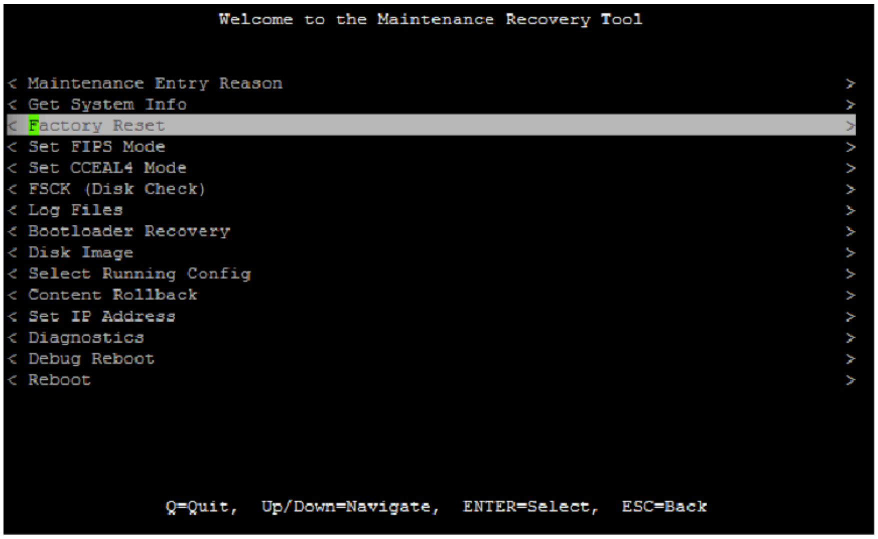
h. Once in maintenance mode, the following is displayed, please press enter to Continue:

16 Arrow down to **Factory Reset** and press **Enter** to display the menu:



```
                              Factory Reset

WARNING: Performing a factory reset will remove all logs and configuration.

Using Image:
    (X) panos-4.1.8

< Factory Reset                                                          >

< Advanced                                                               >




          Q=Quit,  Up/Down=Navigate,  ENTER=Select,  ESC=Back
```

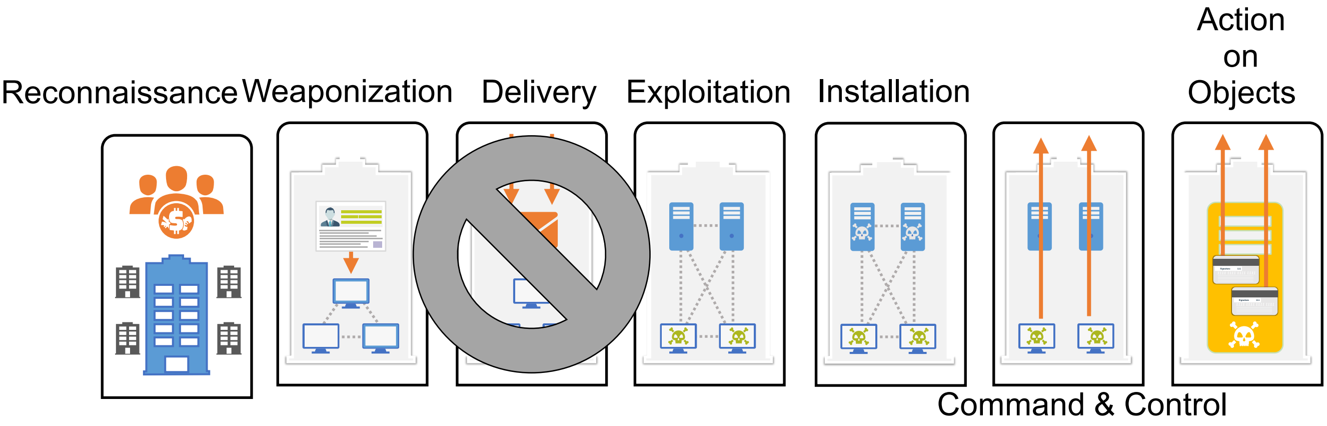
17 You will see the Image that will be used to perform the factory reset. Select **Factory Reset** and press Enter **again**:



```
                    Welcome to the Maintenance Recovery Tool


< Maintenance Entry Reason                                                   >
< Get System Info                                                            >
< Factory Reset                                                              >
< Set FIPS Mode                                                              >
< Set CCEAL4 Mode                                                            >
< FSCK (Disk Check)                                                          >
< Log Files                                                                  >
< Bootloader Recovery                                                        >
< Disk Image                                                                 >
< Select Running Config                                                      >
< Content Rollback                                                           >
< Set IP Address                                                             >
< Diagnostics                                                                >
< Debug Reboot                                                               >
< Reboot                                                                     >




               Q=Quit,  Up/Down=Navigate,  ENTER=Select,  ESC=Back
```

18 The unit will reboot when complete. Please be aware that it may take several minutes before the autocommit to complete and allow the admin/admin login to work properly.

19 You should have a plan to configure and deploy the firewall to disrupt the kill chain. This is called the “0” trust model. To implement 0 trust model using your firewall appliance you should segment your networks into subnets, assign your corresponding firewall interfaces to different zones and then set up security policies to block exploits and malware traversing between all your zones and to



Stop the attack at any point!

only allow the applications you need. By default the firewall will block traffic between 2 different zones, you have to define what traffic to allow. That is the reason why it’s a great idea to divide up your network into multiple zones to prevent lateral exploitation of your network.