



PCNSA

Resting to Factory Default

Step by Step Configuration Guide

Intellectual Property

*The Copyright in this work is vested in **Fortray Networks Limited** and the document is issued in confidence for the express purpose for which it is supplied. It must not be reproduced, in whole or in part, or be used for any other purpose without prior written consent being obtained from **Fortray Networks Limited**, and then only on the condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly therefrom shall be given orally or in writing or communicated in any manner whatsoever to any third party without the prior written consent of **Fortray Networks Limited**.*

© Copyright Fortray Networks Limited 2011-2020

Table of Contents

- 1. Fortray - Palo Alto - Version Control..... 4
- 2. Fortray - Palo Alto - Reference Document 4
- 3. Fortray - Palo Alto - Assumption..... 4
- 4. Fortray - Palo Alto - Network Topology 5
- 5. Fortray - Palo Alto - Notes About Task 6
- 6. Fortray - Palo Alto - Task: Resting to Factory Default..... 7
- 7. Fortray - Palo Alto - Configuration: Resting to Factory Default..... 8
 - 7.1. Step 1: Login to Palo Alto Firewall using Console 8
 - 7.2. Step 2: Entering Firewall Maintenance Mode 8
 - 7.3. Step 3: End User License and Machine Name 9
- 8. Fortray - Palo Alto - Configuration:..... 14
 - 8.1. Step1: Login to Firewall using Console 14

1. Fortray - Palo Alto - Version Control

Version	Date	Notes	Created By	Release
1.0	15/03/2018	Student Workbook for LAB	Mazhar Minhas	Draft
1.1	15/03/2018	Topology update	Mazhar Minhas	Initial Release
1.2	08/07/2020	Diagram and document redesign and Formatting	Farooq Zafar	Final Release

2. Fortray - Palo Alto - Reference Document

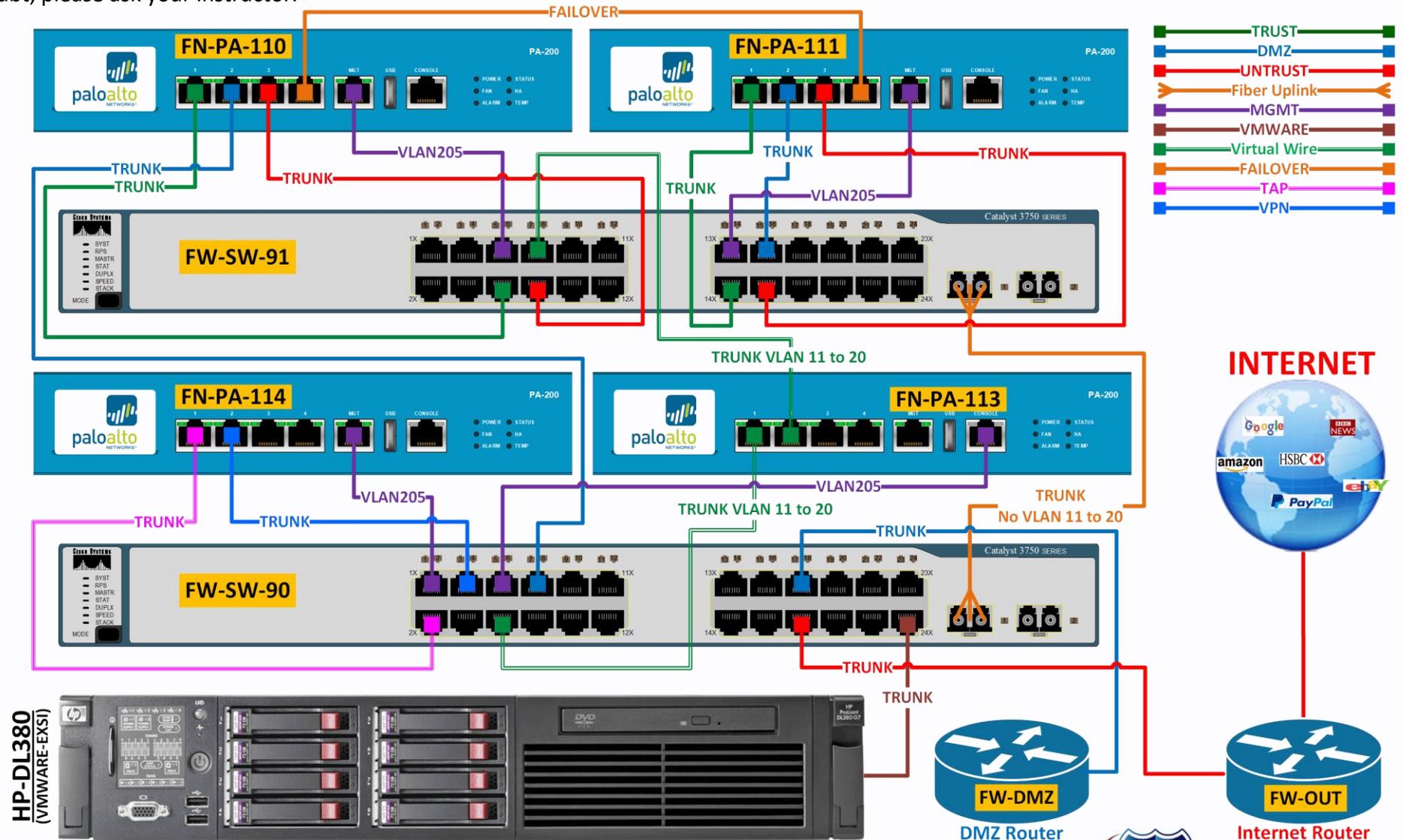
[Click for the Reference document](#)

3. Fortray - Palo Alto - Assumption

- ✓ We understand that delegate already understand L2/L3, Routing.
- ✓ The delegate already knows the "**Fortray Networks - Palo Alto Firewall**" physical and logical connection.
- ✓ The delegate already has a basis Troubleshooting skill, such as ping and trace.
- ✓ The delegate already has access to the "**Fortray Networks - Palo Alto Firewall**" Spreadsheet encompassing the Basic Layer, 2, 3 and allocated subnet information. For more details refer to the "**Student Folder**".
- ✓ This document is created to show an example for one topology only. The candidate needs to refer to his own topology and follow this step by step guide.
- ✓ We assume that delegate already has installed the VPN software and him/she have VPN user / Password. If any issue, contact our Technical team.
- ✓ Our VPN software is supported by PC, MAC, Android, and IOS devices.
- ✓ It's also assumed that delegate has access to PC/Laptop i5 with 4GB RAM.
- ✓ For optimal connectivity, we recommend at least 10MB internet connection.
- ✓ We assume that we already have INTERNAL, DMZ, OUTSIDE interfaces that are already configured.

4. Fortray - Palo Alto - Network Topology

The below network topology is just for information purpose only. Please refer to your student folder and your designated topology. If any doubt, please ask your instructor.



5. Fortray - Palo Alto - Notes About Task

Connect a serial cable from your computer to the Console port and connect to the firewall using terminal emulation software (9600-8-N-1).

If your computer does not have a 9-pin serial port, use a USB-to-serial port connector.

Workbook Shapes:

- ✓  Next Step Window
- ✓  Next Sub Steps Window
- ✓  Step Number
- ✓  Required Value
- ✓  Information / Verification



Resetting the firewall to factory defaults will result in the loss of all configuration settings and logs.

6. Fortray - Palo Alto - Task: Resting to Factory Default

Fortray Networks Engineering Team has been asked to reset currently installed Firewall in branch office, needs to be installed in head office.



In this task, Palo Alto Firewall needs to be reset to factory default.

Summary of the Configuration Steps:

- Login to Palo Alto Firewall using console
- Entering Firewall Maintenance Mode
- Reset the system to factory default settings
- Verification

7. Fortray - Palo Alto - Configuration: Resting to Factory Default

In this section, we need to reset Palo Alto Firewall to Factory Default Values.

7.1. Step 1: Login to Palo Alto Firewall using Console

Connect firewall using console cable.

```
PN-PA-BACKUP-111 login: admin
Password:
System initializing; please wait... (CTRL-C to bypass)

Number of failed attempts since last successful login: 0

admin@PN-PA-BACKUP-111>
```

7.2. Step 2: Entering Firewall Maintenance Mode

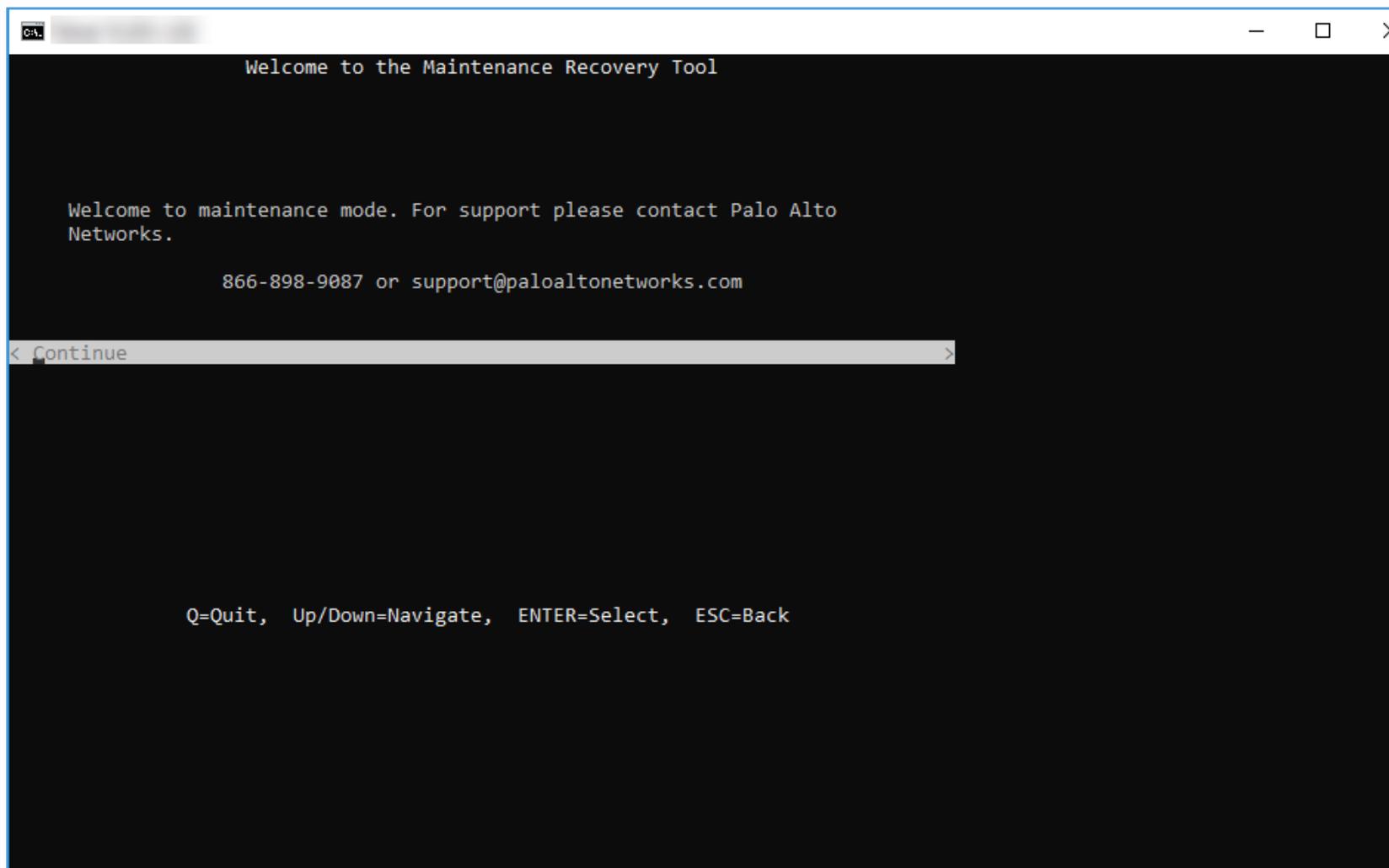
Using **debug system maintenance-mode** command, the firewall will enter in maintenance mode. After issuing this command the firewall will reboot to maintenance mode.

```
admin@PN-PA-BACKUP-111> debug system maintenance-mode
Executing this command will disconnect the current session and reboot the system into maintenance
mode. Do you want to continue? (y or n)y

Broadcast message from root (Tue Stopping PAN Software: [ OK ]
Shutting down NFS mountd: [ OK ]
Shutting down NFS daemon: nfsd: last server has exited, flushing export cache
[ OK ]
Shutting down NFS services: [ OK ]
Stopping xinetd: [ OK ]
```

7.3. Step 3: End User License and Machine Name

After Firewall reboot enter on **"Continue"** to proceed reset procedure.



```

Welcome to the Maintenance Recovery Tool

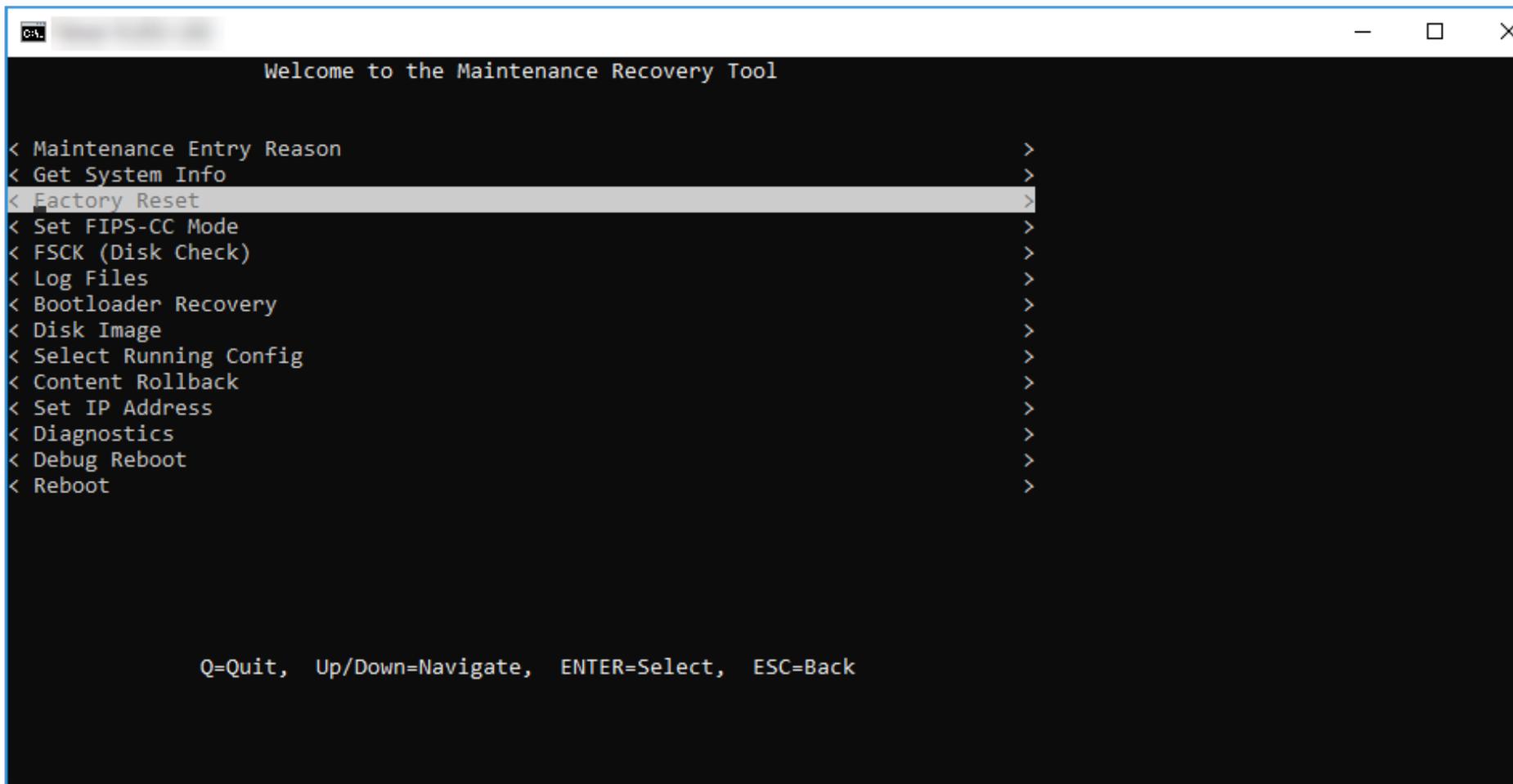
Welcome to maintenance mode. For support please contact Palo Alto
Networks.

866-898-9087 or support@paloaltonetworks.com

< Continue >

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

On next screen, select “**Factory Reset**” and Press Enter to continue.



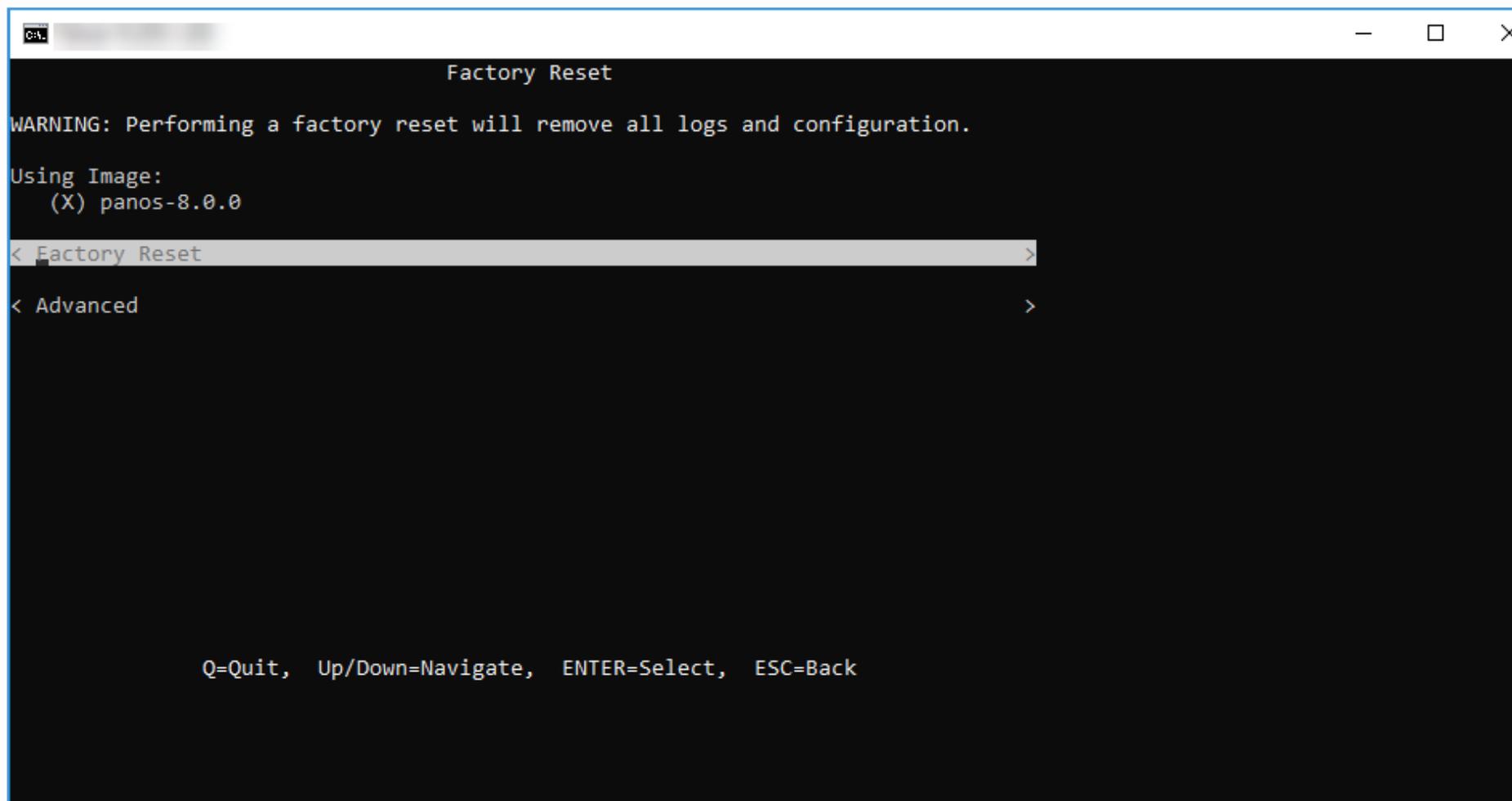
```

Welcome to the Maintenance Recovery Tool

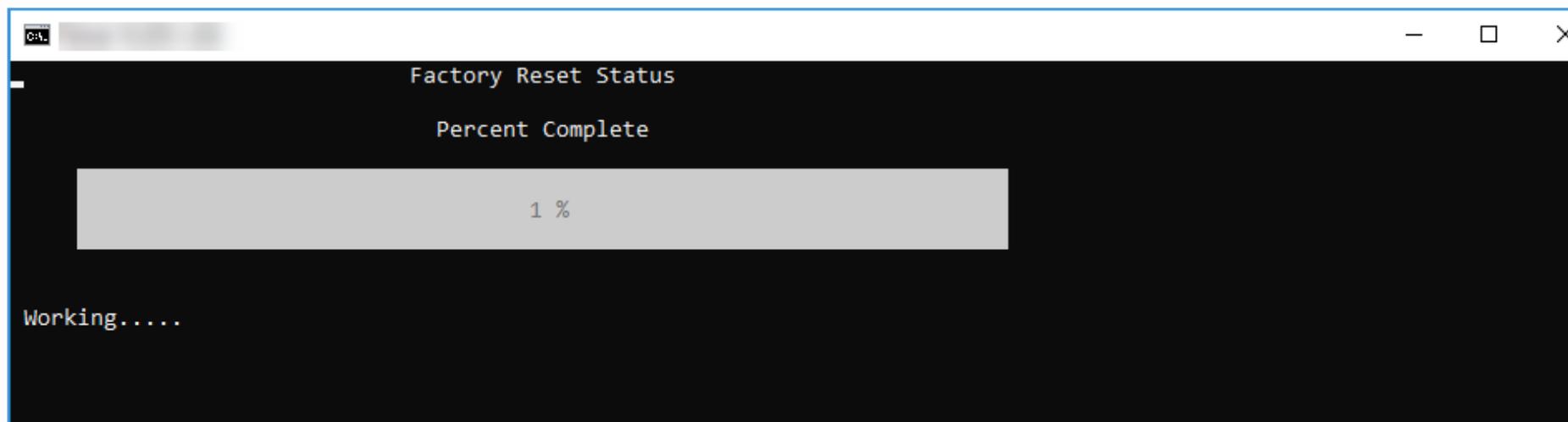
< Maintenance Entry Reason >
< Get System Info >
< Factory Reset >
< Set FIPS-CC Mode >
< FSCK (Disk Check) >
< Log Files >
< Bootloader Recovery >
< Disk Image >
< Select Running Config >
< Content Rollback >
< Set IP Address >
< Diagnostics >
< Debug Reboot >
< Reboot >

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

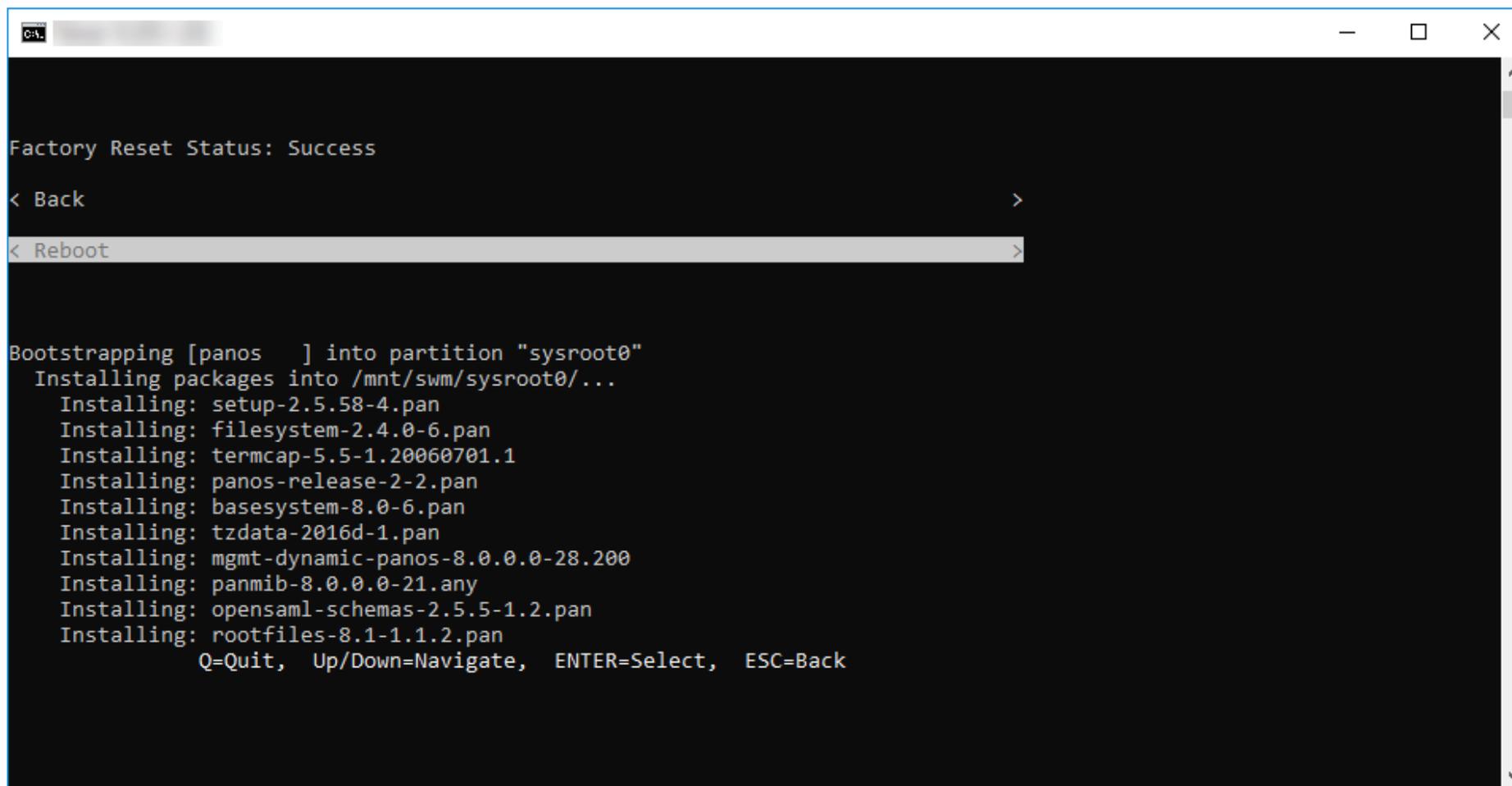
On next screen, confirm Factory rest.



At this point, the reset process starts.



After completing reset procedure, reboot firewall.



```
C:\>

Factory Reset Status: Success

< Back >
< Reboot >

Bootstrapping [panos ] into partition "sysroot0"
Installing packages into /mnt/swm/sysroot0/...
Installing: setup-2.5.58-4.pan
Installing: filesystem-2.4.0-6.pan
Installing: termcap-5.5-1.20060701.1
Installing: panos-release-2-2.pan
Installing: basesystem-8.0-6.pan
Installing: tzdata-2016d-1.pan
Installing: mgmt-dynamic-panos-8.0.0.0-28.200
Installing: panmib-8.0.0.0-21.any
Installing: opensaml-schemas-2.5.5-1.2.pan
Installing: rootfiles-8.1-1.1.2.pan
Q=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back
```

8. Fortray - Palo Alto - Configuration:

In this section, we need verify the device reset status.

8.1. Step1: Login to Firewall using Console

Login to firewall using console. Here we can see default status highlighted yellow.

```
200 login: Waiting for another core to setup the IPD hardware...Done
```

```
PA-HDF login: admin
```

```
Password:
```

```
Login incorrect
```

```
System initializing; please wait... (CTRL-C to bypass)
```

```
Number of failed attempts since last successful login: 0
```

```
Warning: Your device is still configured with the default admin account credentials. Please change your password prior to deployment.
```

```
admin@PA-200>
```

Thanks, and Good Luck