



# CCDC Quick Start Guide for NGFW Deployment and Configuration



Jim Boardman – Cybersecurity Academy  
Tom Trevethan – Cybersecurity Academy

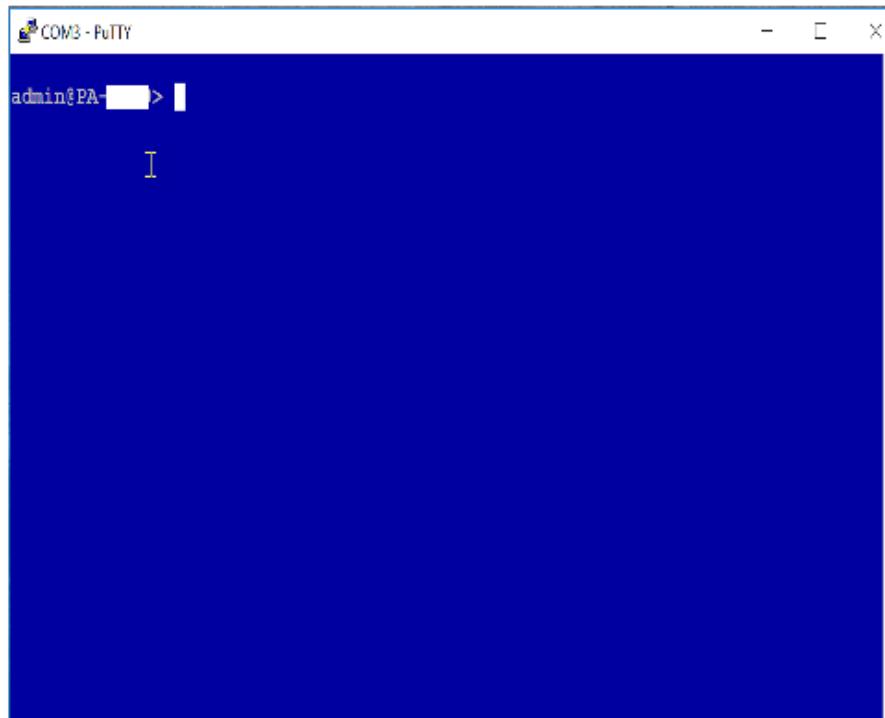
# Quick Start - Critical Steps to Secure and Deploy the Firewall Appliance in order to Protect the Network

1. Secure your firewall appliance and your firewall appliance's management interface
  - By default, the firewall management interface requires Internet access to license the Firewall and retrieve the latest malware signatures
2. License the firewall appliance
3. Download the latest malware signatures for the firewall appliance
4. Determine and configure the network deployment for the firewall appliance (Vwire, Layer2, Layer3). Configure security policies and assign security profiles to the security policies.
5. Turn on decryption (It will add some latency so keep that in mind)
6. How to reset the firewall after a loss of control

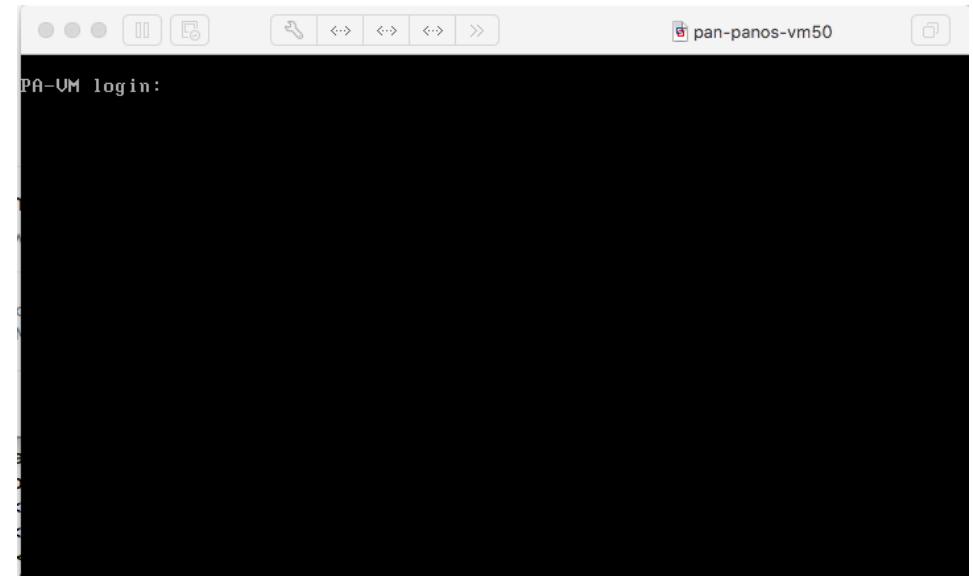
# Step 1: Secure the firewall appliance and the firewall appliance's management interface

# Securing the FW Appliance: Access VM-100 Console via hypervisor and or PA 3260 Serial Port

- PA 3260 Console Port



- Hypervisor Console Port

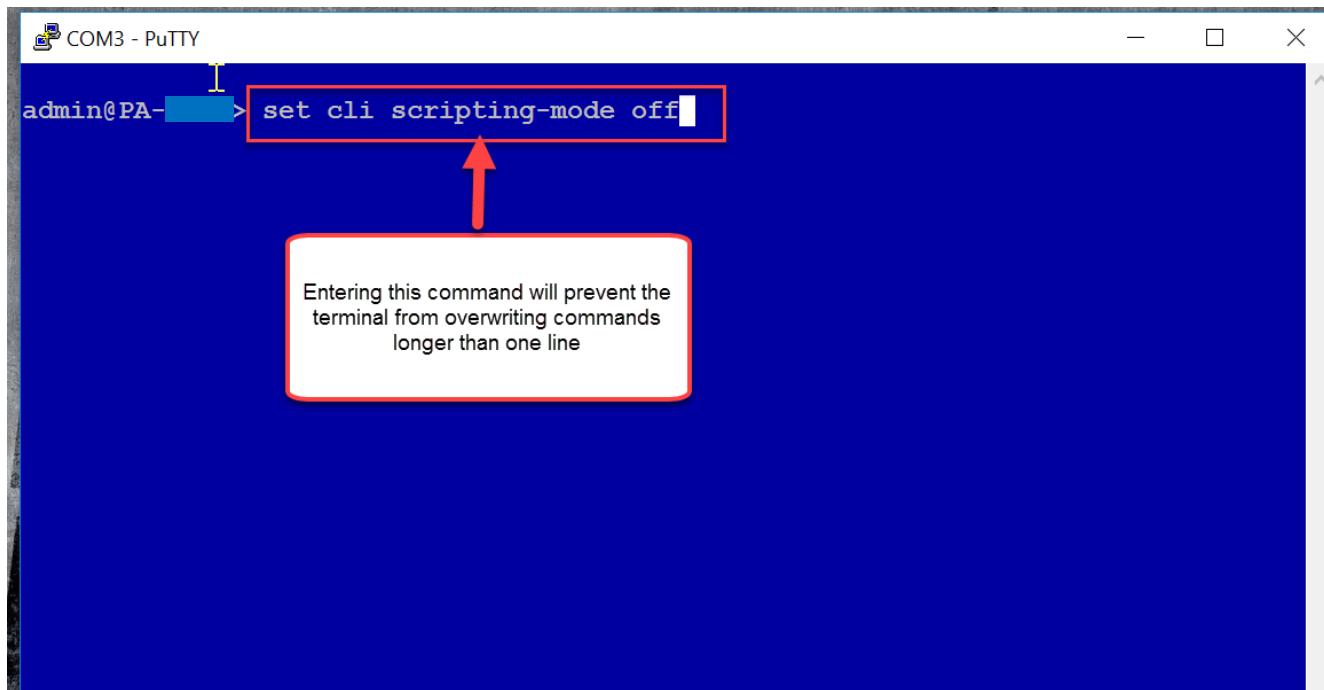


# Securing the Firewall Interface: Connecting to the PA 3260 Console Serial Settings

- Very important that the serial settings are correct to access the console port
- The settings in the Hyper Terminal need to be set correctly; otherwise, no access or garbage characters may show up on the screen. When setting up the connection, use these settings:
  - Bits per sec : 9600
  - Data bits : 8
  - Parity : none
  - Stop bits : 1
  - Flow control : none
- <https://live.paloaltonetworks.com/t5/Management-Articles/What-are-the-Serial-Settings-to-Access-Console-Port/ta-p/62022>
- <https://www.cyberciti.biz/faq/unix-linux-apple-osx-bsd-screen-set-baud-rate/>
- If connecting to PA 3260 console from Linux client use “screen”, sudo apt-get install screen
- Use Putty if connecting from Windows client
- Enter following command in Linux terminal to connect to FW console: **sudo screen /dev/ttyUSB0 9600,cs8,-ixon,ixoff**
- **Ctl + L to clear screen on console**

# Securing the Firewall Appliance: Connect to Your PA 3260 – Turn off Scripting Mode

- Turning off scripting mode in console operations mode: > set cli scripting-mode off



The screenshot shows a PuTTY terminal window titled "COM3 - PuTTY". The session title is "admin@PA-". In the terminal window, the command "set cli scripting-mode off" is typed. A red box highlights this command. An orange arrow points from a callout box below the command to the command itself. The callout box contains the text: "Entering this command will prevent the terminal from overwriting commands longer than one line".

# Securing the PA 3260 FW Appliance: Turn Off Management Interface Temporarily - You Don't Know Who Is Accessing It

- Configure Mode **#set deviceconfig system permitted-ip 127.0.0.1**

**#Commit**

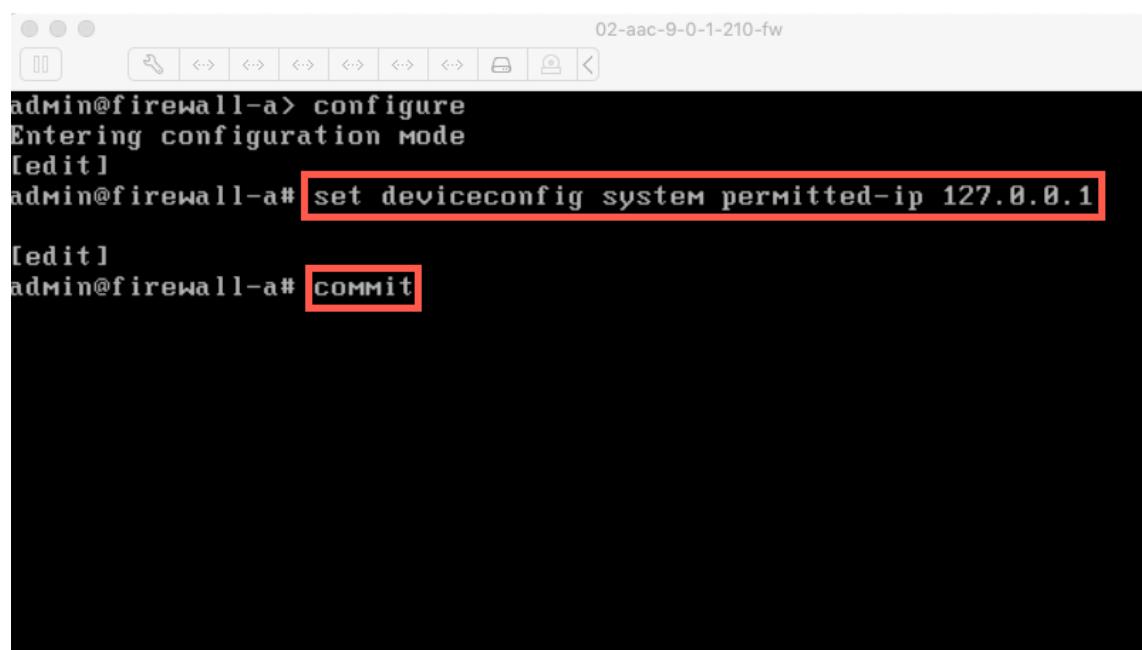
```
admin@PA      > configure
Entering configuration mode
[edit]
admin@PA      # set deviceconfig system permitted-ip 127.0.0.1

[edit]
admin@PA-3050# commit
```

# Securing the Virtual FW Appliance: Turn Off Management Interface Temporarily - You Don't Know Who Is Accessing It

- Configure Mode **#set deviceconfig system permitted-ip 127.0.0.1**

**#Commit**



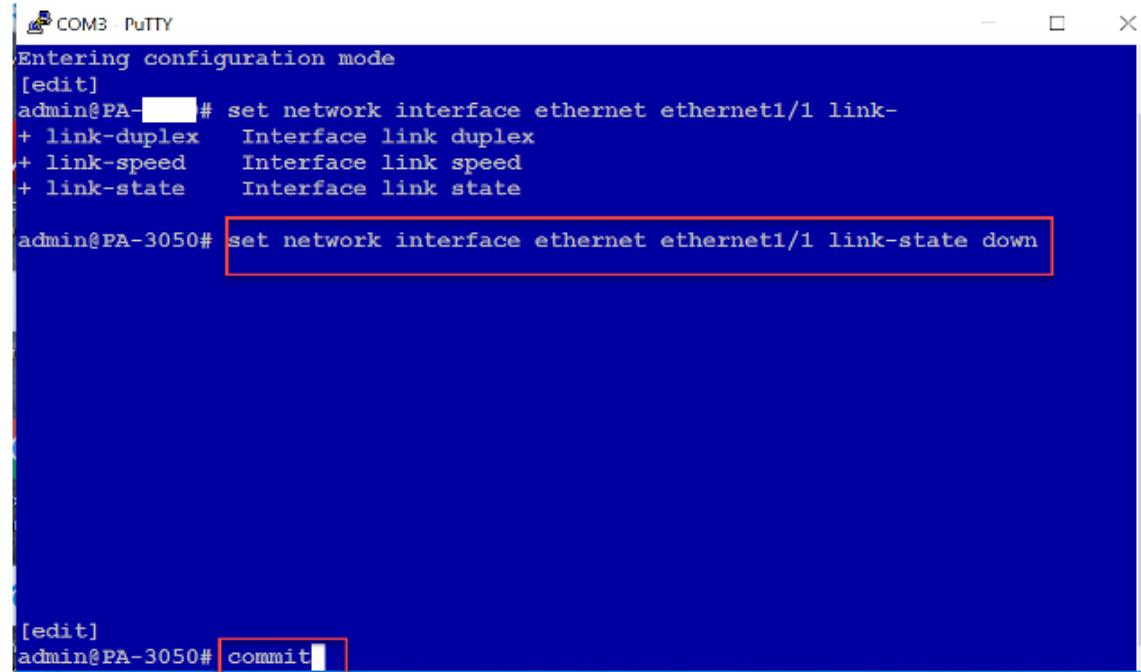
The screenshot shows a terminal window titled "02-aac-9-0-1-210-fw". The command history is as follows:

```
admin@firewall-a> configure  
Entering configuration mode  
[edit]  
admin@firewall-a# set deviceconfig system permitted-ip 127.0.0.1  
[edit]  
admin@firewall-a# commit
```

The command `set deviceconfig system permitted-ip 127.0.0.1` and the final command `commit` are highlighted with red boxes.

# Securing the PA 3260 FW Appliance: Turn Off External Data Interface Temporarily if connected – Red Team Could Be Managing FW Via Data Interface

- Configure Mode #**set network interface ethernet ethernet1/x link-state down**
- **#commit**



A screenshot of a PuTTY terminal window titled "COM3 - PuTTY". The window shows the following configuration mode commands:

```
Entering configuration mode
[edit]
admin@PA-[REDACTED]# set network interface ethernet ethernet1/1 link-
+ link-duplex  Interface link duplex
+ link-speed   Interface link speed
+ link-state   Interface link state

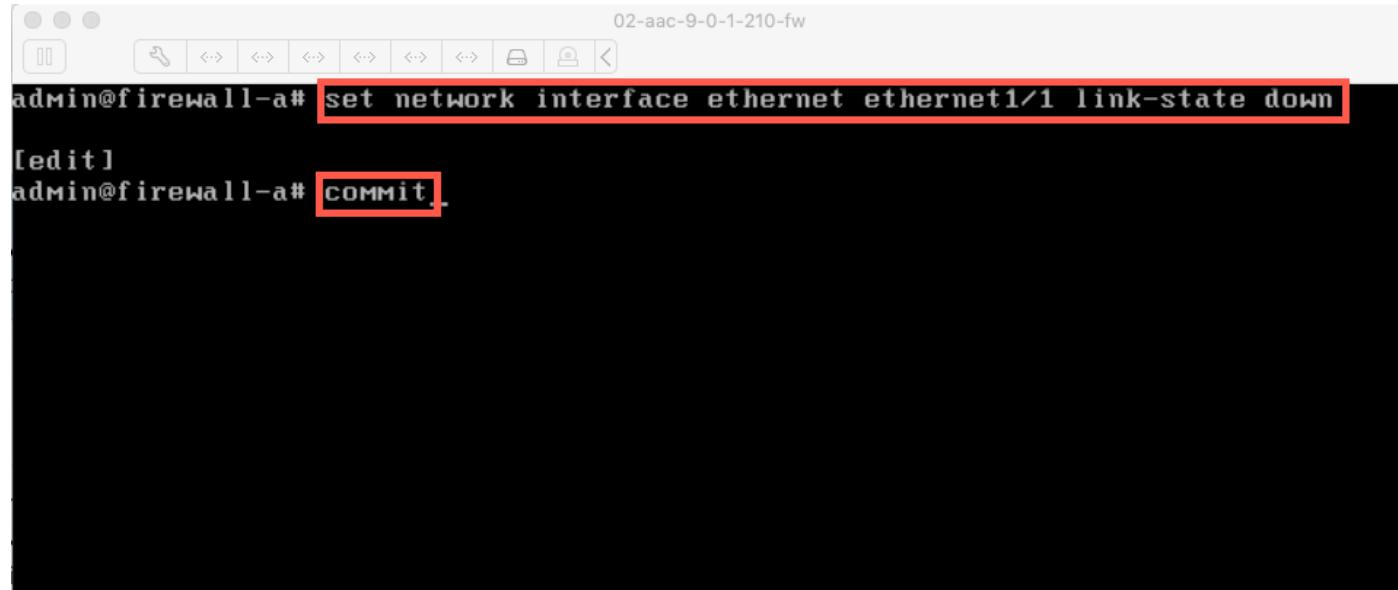
admin@PA-3050# set network interface ethernet ethernet1/1 link-state down
```

The command "set network interface ethernet ethernet1/1 link-state down" is highlighted with a red rectangle.

[edit]
admin@PA-3050# commit

# Securing the Virtual FW Appliance: Turn Off Data External Interface Temporarily if connected – Red Team Could Be Managing FW Via Data Interface

- Configure Mode #**set network interface ethernet ethernet1/x link-state down**
- **#commit**



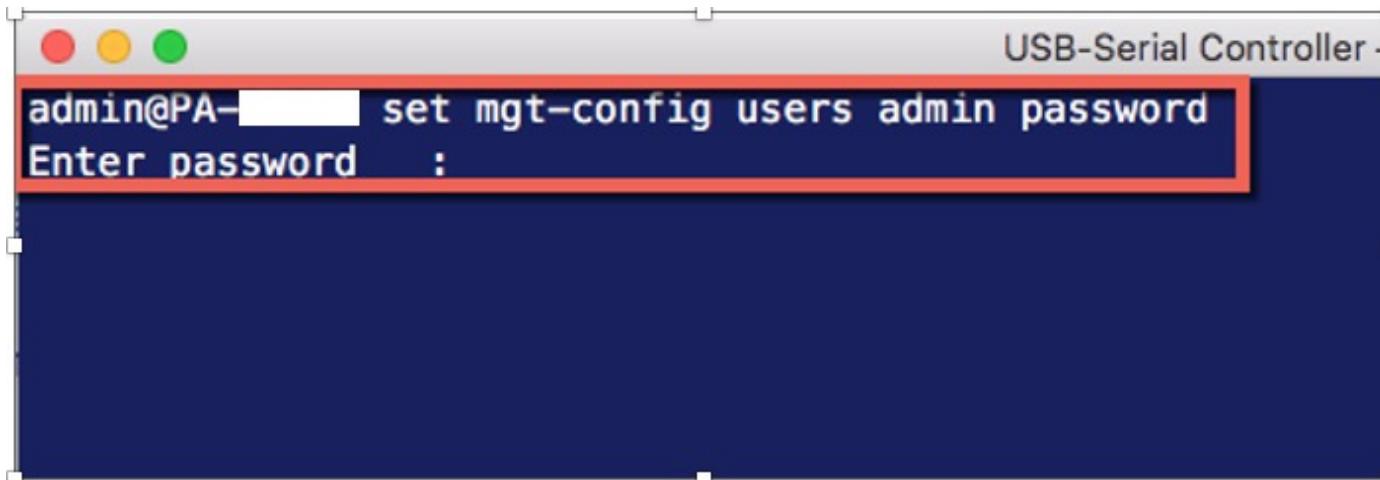
The screenshot shows a terminal window titled "02-aac-9-0-1-210-fw". It displays the following command sequence:

```
admin@firewall-a# set network interface ethernet ethernet1/1 link-state down
[edit]
admin@firewall-a# commit.
```

The command `set network interface ethernet ethernet1/1 link-state down` and the `commit` command are highlighted with a red box.

# Securing the PA 3260 FW Appliance: Change the Admin Password

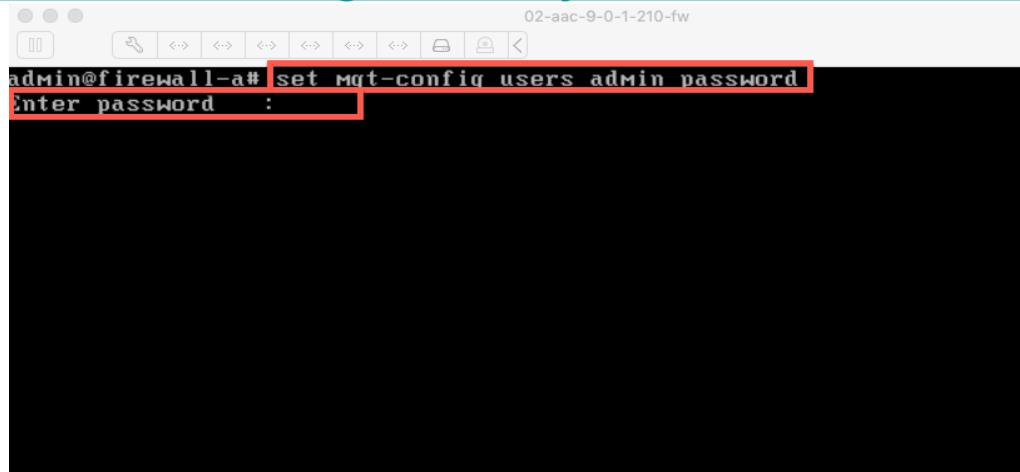
- Change default admin password
  - Operations Mode > **configure**
  - Configure Mode # **set mgt-config users admin password <new password>**
  - Consider using ssh key for authentication
    - <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-ssh-key-based-administrator-authentication-to-the-cli>



A screenshot of a terminal window titled "USB-Serial Controller -". The window shows a command-line interface with the following text:  
admin@PA-[REDACTED] set mgt-config users admin password  
Enter password :  
The "Enter password :" line is highlighted with a red rectangular box.

# Securing the Virtual FW Appliance: Change the Admin Password

- Change default admin password
  - Operations Mode > **configure**
  - Configure Mode # **set mgt-config users admin password <new password>**
  - Consider using ssh key for authentication
    - <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-ssh-key-based-administrator-authentication-to-the-cli>



```
02-aac-9-0-1-210-fw
admin@firewall-a# set mgt-config users admin password
Enter password : [REDACTED]
```

# Securing the PA 3260 FW Appliance: Review System Info

- General system info
  - Operations Mode> **show system info**

```
USB-Serial Controller — 80x24 — 9600.8.N.1

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

admin@PA-3050> show system info

hostname: PA-[REDACTED]
ip-address: 192.168.1.1
netmask: 255.255.255.0
default-gateway: 192.168.1.1
ip-assignment: static
ipv6-address: unknown
ipv6-link-local-address: unknown
ipv6-default-gateway:
mac-address: 00:1b:17:ff:f6:28
time: Tue Feb 20 13:36:42 2018
uptime: 0 days, 0:21:44
family: 3000
model: [REDACTED]

serial: 001701002152
sw-version: 8.0.7
global-protect-client-package-version: 4.0.3
app-version: 777-4484
app-release-date: 2018/02/06 21:20:15
```

You will need to change. Mgt interface needs Internet access

Check PANOS version and Licenses

# Securing the Virtual FW Appliance: Review System Info

- General system info+

- Operations Mode> **show system info**

CLI command to turn off dhcp-client on management interface for VM series:

```
admin@PA-VM# set deviceconfig system type  
> dhcp-client DHCP client option  
    static      Static IP-address/Netmask  
<Enter>     Finish input
```

```
admin@PA-VM# set deviceconfig system type static
```

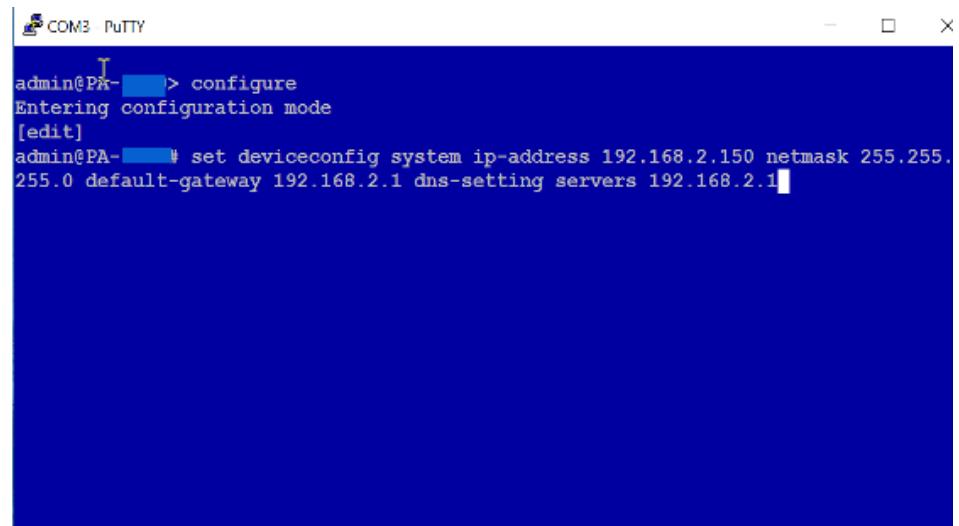
```
hostname: firewall-a  
ip-address: 192.168.1.254  
public-ip-address: unknown  
netmask: 255.255.255.0  
default-gateway: 192.168.1.1  
ip-assignment: static  
ipv6-address: unknown  
ipv6-link-local-address: fe80::250:56ff:feb9:162d/64  
ipv6-default-gateway:  
mac-address: 00:50:56:b9:16:2d  
time: Thu Oct 15 14:58:34 2020  
uptime: 44 days, 20:36:04  
family: VM  
model: PA-UM  
serial: 015351000035873  
vm-Mac-base: 7C:89:C1:06:77:00  
vm-Mac-count: 256  
vm-uuid: 4239A91D-CEF6-64AF-87F2-D3DD973FAB17  
vm-cpuid: ESX:63060500FFFFB8B1F  
vm-license: VM-50  
vm-mode: VMWare ESXi  
cloud-mode: non-cloud  
sw-version: 9.0.1  
global-protect-client-package-version: 5.1.1  
Lines 2-25
```

The default setting for VM series mgt interface is dhcp client. You will need to turn off dhcp client before configuring a static address.

Check panos version and licensing

# Securing the PA 3260 FW Appliance: Change Management Interface IP Address If Required (same command on virtual)

- Changing Mgt Interface IP Address
  - Configure Mode: **#set deviceconfig system ip-address x.x.x.x netmask x.x.x.x default-gateway x.x.x.x dns-setting servers primary x.x.x.x**
- Enter command “**commit**” to commit changes to running configuration
- Configure an IP address, default gateway and preferred DNS that will allow Internet access



```
COM3 PUTTY
admin@PA-[REDACTED] > configure
Entering configuration mode
[edit]
admin@PA-[REDACTED] # set deviceconfig system ip-address 192.168.2.150 netmask 255.255.255.0 default-gateway 192.168.2.1 dns-setting servers 192.168.2.1
```

# Securing FW Appliance: Only Allow Secure Protocols To Connect to Mgt Interface (same command for virtual and PA 3260 appliance)

- Secure the FW management interface for allowed services
  - Only allow secure services: ssh, https, ping (for troubleshooting)
  - Configure mode: **#set deviceconfig system service disable-https no**

**#commit**

```
admin@PA-VM> show system services
```

HTTP	: Disabled
HTTPS	: Enabled
Telnet	: Disabled
SSH	: Enabled
Ping	: Enabled
SNMP	: Disabled

```
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# set deviceconfig system service disable-
+ disable-http
+ disable-https
+ disable-ssh
+ disable-telnet
+ disable-userid-service
+ disable-userid-syslog-listener-ssl
+ disable-userid-syslog-listener-udp
admin@PA-VM# set deviceconfig system service disable-
```

# Secure FW Appliance: Show all Admin Accounts (same command for virtual and PA 3260 appliance)

- Make sure there are only two admin accounts unless directed otherwise:  
(admin and panorama -- default configuration)
  - **> show admins all**
  - **# delete mgt-config users redteam and # commit**

The image contains two side-by-side terminal window screenshots. The left window, titled 'USB-Serial C', shows the command `> show admins all` being entered. The right window, titled 'COM3 - PuTTY', shows the configuration mode process where the `redteam` user is deleted.

**Left Terminal (USB-Serial C):**

```
admin@PA-> show admins all
```

**Right Terminal (PuTTY):**

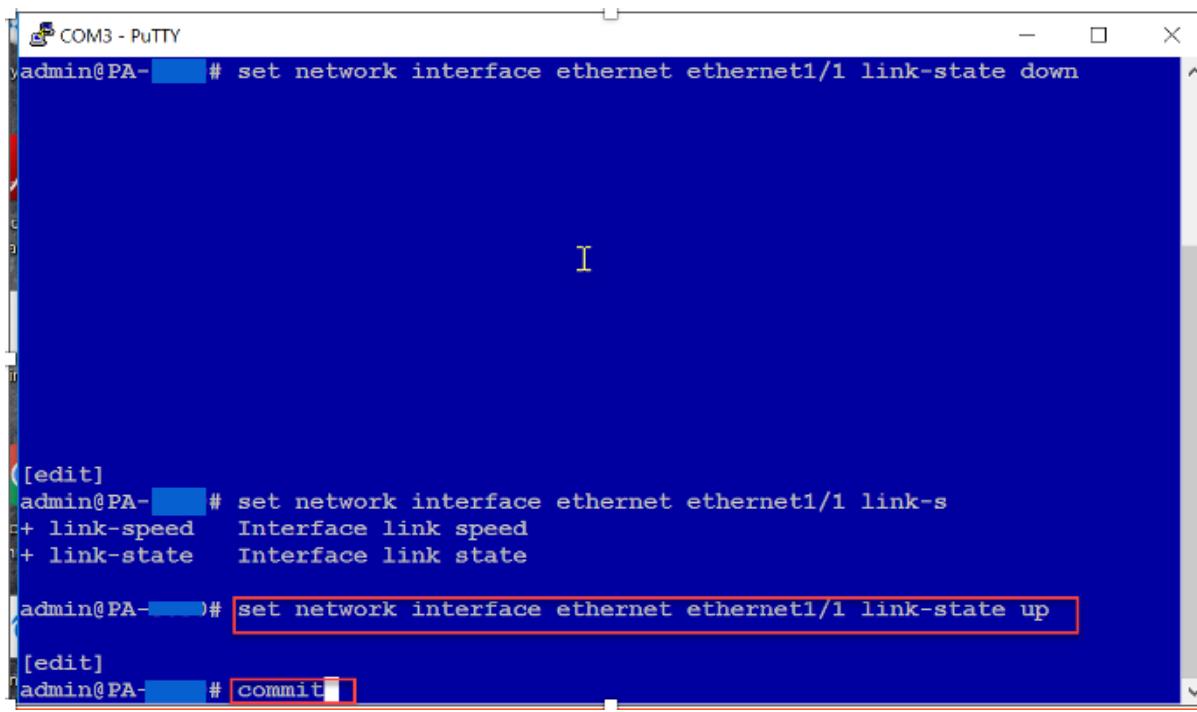
```
I
```

```
admin
panorama
redteam

admin@PA-> configure
Entering configuration mode
[edit]
admin@PA-> delete mgt-config users redteam
[edit]
admin@PA-> commit
```

# Secure FW Appliance: Turn Data Interfaces Back On If Turned Off (same command for virtual and PA 3260 appliance)

Configuration Mode #set network interface ethernet ethernet1/1 link-state up



The screenshot shows a Putty terminal window titled "COM3 - PUTTY". The session is in configuration mode, indicated by the prompt "admin@PA- [edit]". The user has entered the command "# set network interface ethernet ethernet1/1 link-state down", which is displayed in blue. Below this, the configuration mode menu is shown, with "link-speed" and "link-state" being expanded. The user then enters the command "# set network interface ethernet ethernet1/1 link-state up", which is highlighted with a red rectangle. Finally, the user enters the command "# commit", also highlighted with a red rectangle. The entire session is displayed in a dark blue background with white text.

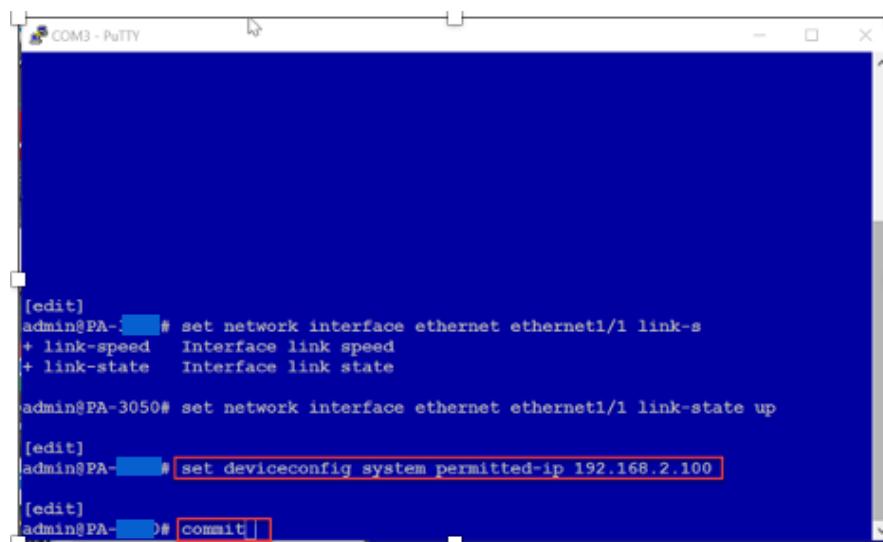
```
admin@PA- [edit] # set network interface ethernet ethernet1/1 link-state down
[edit]
admin@PA- [edit] # set network interface ethernet ethernet1/1 link-s
+ link-speed  Interface link speed
+ link-state  Interface link state

admin@PA- [edit] # set network interface ethernet ethernet1/1 link-state up

[edit]
admin@PA- [edit] # commit
```

# Securing the FW Appliance: Turn Management Interface Back On (same command for virtual and PA 3260 appliance)

- Only allow management Interface access from your team's computer
  - Configuration Mode# **set deviceconfig system permitted-ip X.X.X.X**
- Manage your FW appliance via mgt interface Web-UI

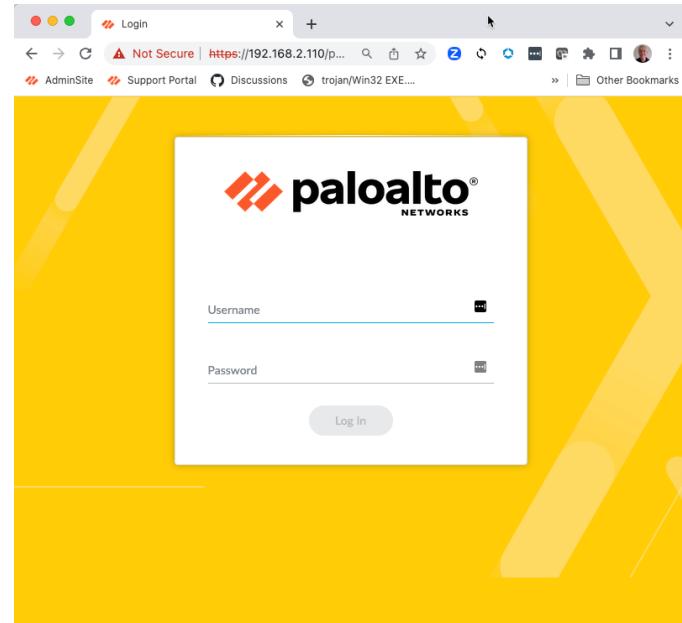


```
[edit]
admin@PA-[REDACTED]# set network interface ethernet1/1 link-speed
+ link-speed    Interface link speed
+ link-state   Interface link state

admin@PA-3050# set network interface ethernet1/1 link-state up

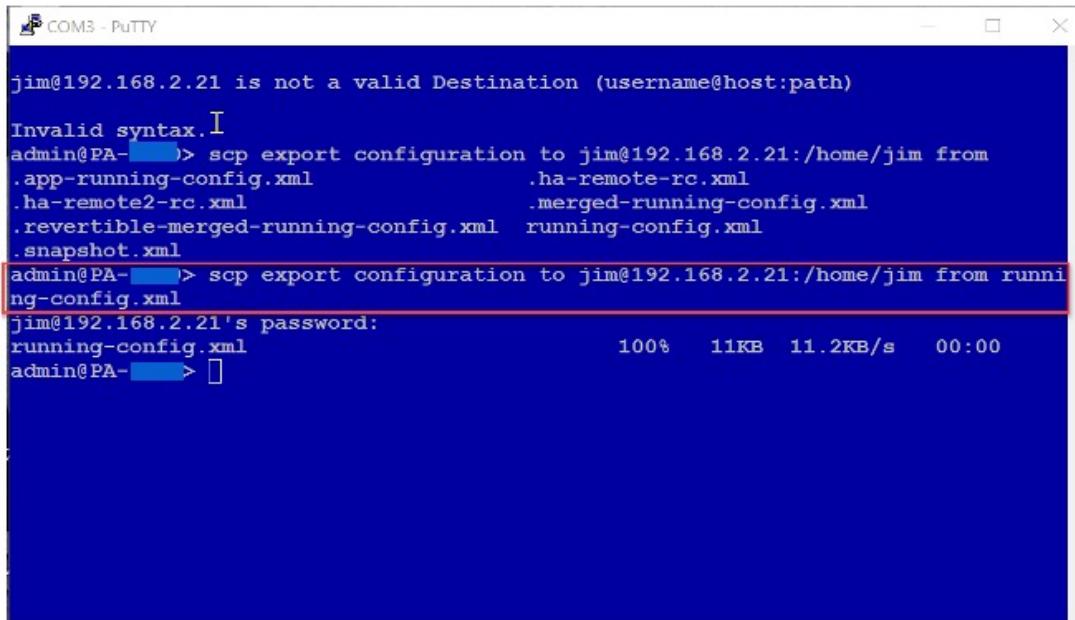
[edit]
admin@PA-[REDACTED]# set deviceconfig system permitted-ip 192.168.2.100

[edit]
admin@PA-[REDACTED]# commit |
```



# Securing the FW: Back Up Your FW Config and/or Take Snapshot of Virtual Firewall Appliance (same command for virtual and PA 3260 appliance)

- Operations Mode >**scp export configuration to username@host:/home/secops from running-config.xml**



A screenshot of a Putty terminal window titled "COM3 - PuTTY". The window shows a command-line session. The user has typed "admin@PA-> scp export configuration to jim@192.168.2.21:/home/jim from running-config.xml" and is prompted for a password. The password entry field is redacted. The session ends with "admin@PA->".

```
jim@192.168.2.21 is not a valid Destination (username@host:path)
Invalid syntax.I
admin@PA-> scp export configuration to jim@192.168.2.21:/home/jim from
.app-running-config.xml          .ha-remote-rc.xml
.ha-remote2-rc.xml                .merged-running-config.xml
.revertible-merged-running-config.xml  running-config.xml
.snapshot.xml
admin@PA-> scp export configuration to jim@192.168.2.21:/home/jim from runni
ng-config.xml
jim@192.168.2.21's password:
running-config.xml                  100%   11KB  11.2KB/s  00:00
admin@PA->
```

## Step 2: License the firewall appliance

# Licensing Your FW Appliance: It's a dumb box w/o licenses

The image shows two screenshots of the Palo Alto Networks Management Console. The left screenshot shows the 'DEVICE' tab selected in the navigation bar. A red box highlights the 'License Management' section under the 'Setup' category, which contains options: 'Retrieve license keys from license server', 'Activate feature using authorization code', 'Manually upload license key', and 'Deactivate VM'. A red circle with the number '3' is placed over the 'Activate feature using authorization code' option. The right screenshot shows a detailed view of various license entries for the device PA-VM. A large red box highlights the 'Adv Threat Prevention', 'DNS Security', 'GlobalProtect Portal', 'Premium', 'Threat Prevention', and 'WildFire License' sections. A red circle with the number '2' is placed over the 'WildFire License' section. A red circle with the number '4' is placed over the 'Reboot' button at the bottom of the left screenshot.

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

PA-VM

Not Secure | https://192.168.2.92/#device::vsyst:device/licenses

AdminSite Support Portal Discussions trojan/Win32 EXE... Inbox (144) - jobs... cygwin 1 | Academy Pro... Palo Alto Networks... Index of /CourseF... Palo Alto Networks... P

PA-VM

Dashboard ACC Monitor Policies Objects Network Device

Setup High Availability Config Audit Password Profiles Administrators Admin Roles Authentication Profile Certificate Management Certificates Certificate Profile QSCP Response Pages SSL Decryption Exclusion SSH Service Profile Response Pages Log Sources User Profiles Snort Trap Syslog Email Radius TACACS+ LDAP Kerberos Multi Factor Identity Provider Local User Database Users User Groups Generated Log Export Services GlobalProtect Client Dynamic Updates Plugins VM-Series Licenses

3

4 Reboot

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

PA-VM

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: Standard VM-50 Eval

Adv Threat Prevention

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: Adv Threat Prevention Sub

BrightCloud URL Filtering

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: BrightCloud URL Filtering  
Active: No

GlobalProtect Gateway

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: GlobalProtect Gateway License

PAN-DB URL Filtering

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: Palo Alto Networks URL Filtering License  
Active: Yes

SD WAN

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: License to enable SD WAN feature

WildFire License

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: WildFire signature feed, integrated WildFire logs, WildFire API

GlobalProtect Portal

Date Issued: March 07, 2023  
Date Expires: Never  
Description: GlobalProtect Portal License

Premium

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: 24 x 7 phone support; advanced replacement hardware service

Threat Prevention

Date Issued: March 07, 2023  
Date Expires: March 07, 2024  
Description: Threat Prevention

License Management

Remove license keys from license server  
Activate feature using authorization code  
Manually upload license key  
Deactivate VM  
Upgrade VM capacity

## Step 3: Download the latest malware signatures for the firewall appliance

# Signatures: Dynamic Updates, Need All The Current Malware Signatures Because It's a Dumb Box w/o Them

The screenshot shows the Palo Alto VM (PA-VM) interface under the 'DEVICE' tab. The left sidebar contains a tree view of configuration categories. The main area displays a table of updates categorized by module:

- Antivirus:** Last checked: 2023/04/24 13:44:13 PDT. Schedule: Every day at 06:30 [Download and Install].
- Applications and Threats:** Last checked: 2023/04/24 13:31:53 PDT. Schedule: Every Wednesday at 01:02 [Download and Install].
- GlobalProtect Clientless VPN:** Last checked: 2023/04/24 13:49:33 PDT. Schedule: Every Sunday at 07:45 [None].
- Device Dictionary:** Last checked: 2023/04/24 13:31:20 PDT.
- WildFire:** Last checked: 2023/04/24 13:51:00 PDT. Schedule: Real-time.

A red box highlights the 'Schedule' column for the 'Antivirus' and 'Applications and Threats' sections. A red arrow points to the 'Check Now' button at the bottom of the table, which is also highlighted with a red box. A red callout bubble above the 'Check Now' button says: "Click Check now and then download and install the latest updates and schedule future downloads and installations."

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION
4423-4940	panup-all-antivirus-4423-4940		Full	119 MB	42a6c45cf6124...	2023/04/17 10:01:05 PDT	✓ previously		Revert
4426-4943	panup-all-antivirus-4426-4943		Full	119 MB	3787457d5a6b3...	2023/04/20 09:26:27 PDT			Download
4427-4944	panup-all-antivirus-4427-4944		Full	119 MB	77e52114dc1e...	2023/04/21 09:14:08 PDT			Download
4428-4945	panup-all-antivirus-4428-4945		Full	119 MB	3cd1bdc438f7...	2023/04/22 09:06:17 PDT			Download
4429-4946	panup-all-antivirus-4429-4946		Full	119 MB	5e90cf76e231...	2023/04/23 08:51:3 PDT			Download
4430-4947	panup-all-antivirus-4430-4947		Full	120 MB	5f06ba81cc5c2...	2023/04/24 10:16:15 PDT	✓	✓	
8691-7946	panupv2-all-contents-8691-7946	Apps, Threats	Full	64 MB	53ff4b83c81f65...	2023/03/27 14:04:55 PDT			Download
8692-7955	panupv2-all-contents-8692-7955	Apps, Threats	Full	64 MB	a4bcd05493ee7...	2023/03/29 13:20:18 PDT			Download
8693-7959	panupv2-all-contents-8693-7959	Apps, Threats	Full	64 MB	898546713927...	2023/03/31 10:04:55 PDT			Download
8694-7964	panupv2-all-contents-8694-7964	Apps, Threats	Full	64 MB	e28268579954...	2023/04/03 14:38:09 PDT			Download
8695-7968	panupv2-all-contents-8695-7968	Apps, Threats	Full	64 MB	b57b585d2126...	2023/04/05 15:32:53 PDT			Download
8696-7977	panupv2-all-contents-8696-7977	Apps, Threats	Full	64 MB	4984d1666769...	2023/04/11 13:08:12 PDT	✓ previously		Revert
8697-7981	panupv2-all-contents-8697-7981	Apps, Threats	Full	64 MB	45315fe83649...	2023/04/13 19:18:35 PDT			Download
8698-7988	panupv2-all-contents-8698-7988	Apps, Threats	Full	64 MB	3ae74c8ed12cf...	2023/04/17 19:02:31 PDT			Download
8699-7991	panupv2-all-contents-8699-7991	Apps, Threats	Full	65 MB	988fe92658614...	2023/04/18 20:13:16 PDT	✓	✓	Review Policies
90-212	panup-all-gp-90-212	GlobalProtectClientless...	Full	77 KB	f142d69de2601...	2021/01/07 18:43:43 PST	✓ previously		Revert
97-245	panup-all-gp-97-245	GlobalProtectClientless...	Full	77 KB	c696eb3c135f0...	2023/01/27 14:38:39 PST	✓	✓	
71-382	panup-all-deviceid-71-382	IoT	Full	172 KB	77b9b7c692914...	2023/03/30 07:51:39 PDT			
72-385	panup-all-deviceid-72-385	IoT	Full	173 KB	15363d3d8d54...	2023/04/06 10:57:47 PDT	✓ previously		
73-387	panup-all-deviceid-73-387	IoT	Full	173 KB	49baefbd3d04...	2023/04/13 21:46:23 PDT	✓	✓	
74-389	panup-all-deviceid-74-389	IoT	Full	174 KB	e2528c8e65fb...	2023/04/20 18:45:46 PDT			
762610-766072	panupv3-all-wildfire-762610-766072	PAN OS 10.0 And Later	Full	8 MB	dd1291d57921a...	2023/04/24 12:57:49 PDT	✓ previously		Revert
762620-766082	panupv3-all-wildfire-762620-766082	PAN OS 10.0 And Later	Full	8 MB	6f4f5046cc82f2...	2023/04/24 13:47:34 PDT	✓	✓	

**Check Now** Up to date

Click Check now and then download and install the latest updates and schedule future downloads and installations.

**Step 4:**  
Determine and Configure the Network Deployment for the Firewall (Vwire, Layer2, Layer3). Configure Security Policies and assign Security Profiles to the Security Policies

## 3 Network Deployment Options:

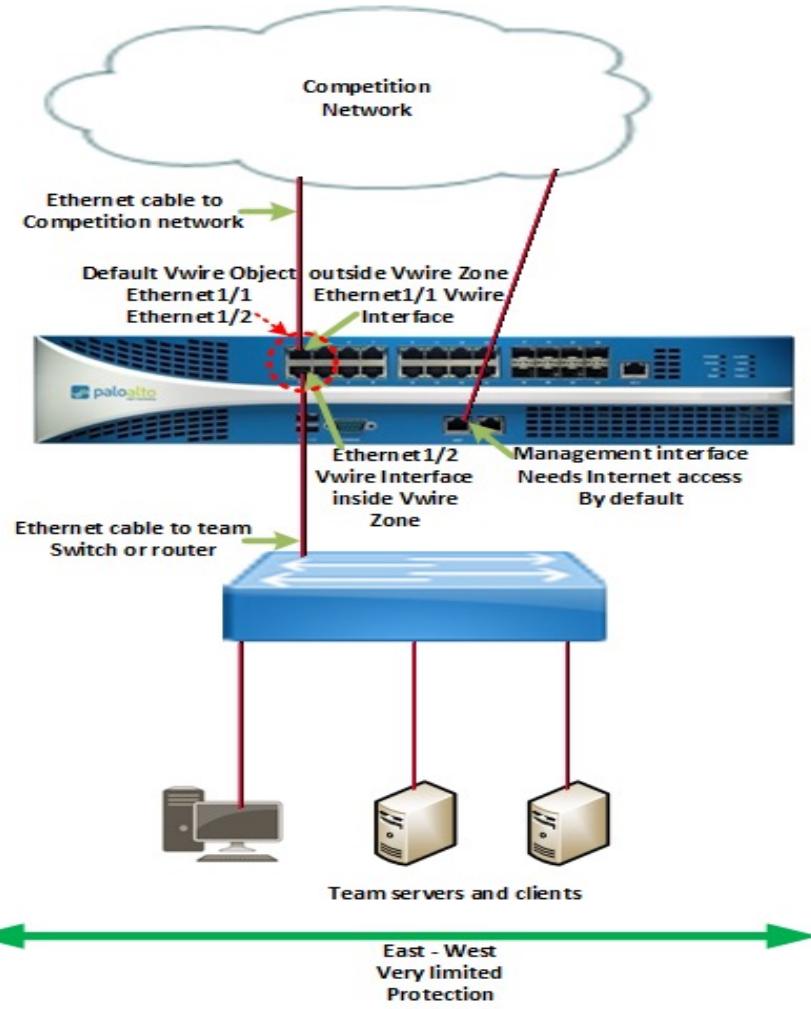
1. Virtual Wire
2. Layer 2
3. Layer 3

## Network Deployment Option 1: Virtual Wire (Vwire)

- Rapid deployment: the easiest and quickest set up
  - PA 3050 preconfigured for Vwire
  - Works for virtual firewall appliances with similar setup
  - Sets up a network bridge between 2 FW interfaces
  - No IP or Layer 2 addressing – therefore invisible to attackers!
- Cons: Only provides North-South full protection
  - Can't segment internal traffic into multiple internal zones to defend against East-West pivoting
- PA 3260 setup
  - Find the Ethernet cable coming into the room and connect it to the FW ethernet1/1 port (This is your ingress interface)
  - Connect a cable from the FW ethernet1/2 interface to the room's switch/router
  - Configure outside Vwire zone for ethernet1/1 and inside Vwire zone for ethernet1/2
  - Configure the inbound and outbound security policies

# Network Deployment (Option 1): Vwire Architecture

North – South  
Full protection  
Using security  
Policies with  
Security profiles



## Network Deployment (Option 1): Vwire Security Policies

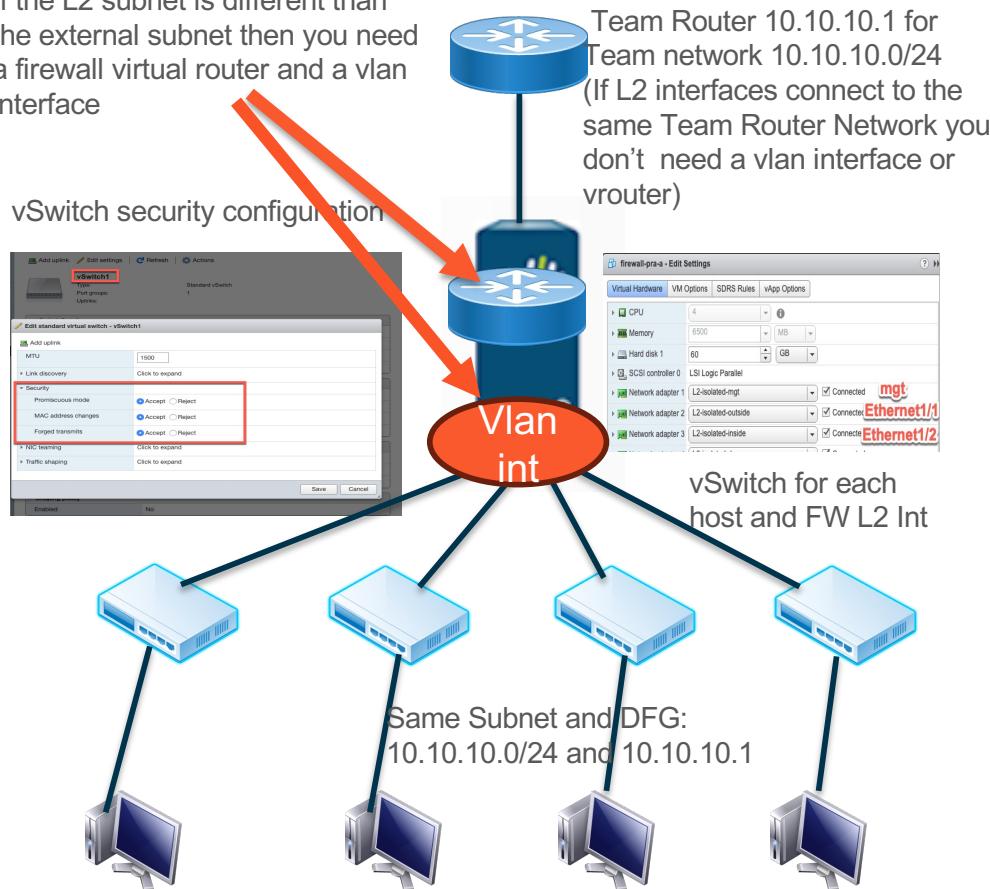
- Configure an inbound and outbound block rule to block unknown and bad urls
- Configure inbound allow rule(s) for scored services
  - Make rules as specific as possible by using allowed applications and destination IP addresses
- Configure outbound allow rule(s)
  - Make rules as specific as possible by using allowed applications (application default) and destination IP addresses
  - Only allow outbound traffic from specific IP addresses that are absolutely necessary for your organization and scoring
- Make sure to assign Security Profiles to all Allow rules
  - The FW will not block malware without Security Profiles assigned to Security Policies

# Network Deployment (Option 2): Layer 2 (L2)

- **Most applicable** if your team is assigned 1 subnet, 1 switch, and no router
  - All team hosts are configured with a default gateway located in competition network and your team has no control over this default gateway
- Pro: Provides both North-South and East-West full protection
- Con: more complex to set up than Vwire, hosts need to be in same subnet and corresponding Ethernet broadcast domain. L2 interfaces can't be configured to support VPN's
- Ideal setup for virtual firewall appliances.
  - Configure a separate ESXi vSwitch for each L2 firewall interface then connect VM host and firewall to same vSwitch
- **For your PA 3260: Replace your team switch** with your firewall configured with L2 interfaces
  - Create L2 interfaces and assign them to same firewall vlan object
  - Assign L2 zones to each L2 interface
  - Connect your team hosts to separate L2 interfaces
  - Create security policies to allow only essential North-South and East-West traffic

# ESXi VM-100 L2 Deployment

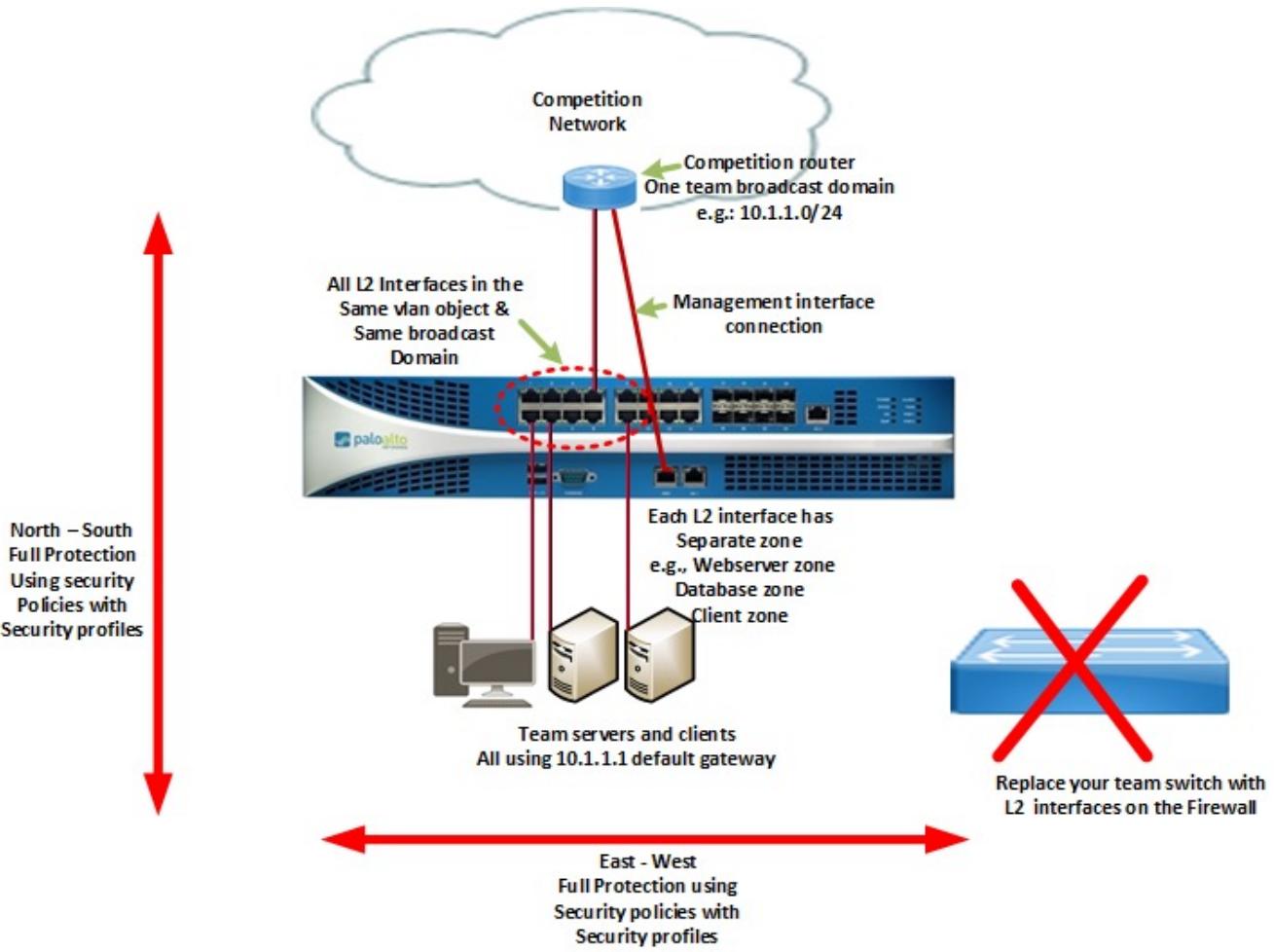
If the L2 subnet is different than the external subnet then you need a firewall virtual router and a vlan interface



## L2 Configuration Steps

1. Create vSwitch for each L2 FW port and protected host
2. Create FW L2 zone(s)
3. Create FW Vlan Obj
4. Create FW L2 Interfaces and assign to same Vlan Obj and to appropriate L2 zone(s)
5. If connecting different networks, create VLAN interface (10.10.10.x) assign it to a L3 internal zone
6. If connecting to different networks, connect the FW VLAN int and your FW external interface to same vRouter and create default gateway
7. Create zone-based security policies from the L-3 internal to external zones for North-South protection and between the L2 Zones if there is more than 1 for East-West protection

# Network Deployment PA 3260 (Option 2): L2 Architecture



# Network Deployment L2 (Option 2): Security Policies

- Configure, FW L2 zone(s) and vlan object
- Configure L2 interfaces and assign all to same vlan object and appropriate L2 zone(s)
- Configure a FW VLAN interface and assign it to the L3 inside zone. Assign the L3 external interface to L3 outside zone
- Assign the L3 VLAN interface and the L3 external interface to the same vRouter and configure default gateway
- Configure North South security policy rules between internal L3 inside zone and L3 outside zone
  - Configure an inbound and outbound block rule to block unknown and bad urls
  - Configure inbound allow rule(s) for scored services
  - Make rules as specific as possible by using allowed applications and destination IP addresses
- Configure East-West rule(s) for internal traffic between L2 zones if there is more than 1 L2 zone
  - Make rules as specific as possible by using allowed applications (application default) and destination IP addresses
  - Only allow internal traffic from specific IP addresses that are absolutely necessary to keep your services up
  - DHCP is a 2-way protocol requiring ingress and egress rules
- Make sure to assign Security Profiles to all your Allow rules
  - Your FW will not block malware without Security Profiles assigned to Security Policies

# Network Deployment L2 (Option 2): Security Policies

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

**Security**

NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS						DEVICE
4 Block-Bad-IP-Out	none	universal	L2-dmz	any	any	any	L2-outside	Palo Alto Net...	any	any	application...	Drop	none	
5 allow-pnw-updates	none	universal	L2-mgt	any	any	any	L2-outside	Palo Alto Net...	any	any	dns	Allow		
6 outside-dmz	none	universal	L2-outside	any	any	any					paloalto-aut...			
7 dmz-outside	egress	universal	L2-dmz	any	any	any					paloalto-dir...			
8 inside-outside	egress	universal	L2-inside	any	any	any	L2-outside	any	any		paloalto-dns...			
9 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	dns	Allow	none	none
10 interzone-default	none	interzone	any	any	any	any	any	any	any	any	application...	Deny	none	

1. Allow only the apps needed to conduct your business and block everything else

2. Use Monitor>Manage Custom Reports>Custom Report to determine the applications running in your network.

3. Enable Zero Trust by segmenting network and only allowing app traffic that is need for that zone/segment

Assign your custom security profiles to a Security Group and then assign the Security Group to your allow policies-

# Use Custom Reports to Determine What Apps Are in Your Network

The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR (which is highlighted with a red box), POLICIES, OBJECTS, NETWORK, and DEVICE. The left sidebar has sections for Logs (Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel Inspection, Configuration, System, Alarms, Authentication, Unified, Packet Capture, App Scope, Session Browser, PDF Reports, Manage PDF Summary, User Activity Report, SaaS Application Usage, Report Groups, and Email Scheduler). At the bottom of the sidebar, 'Manage Custom Reports' is highlighted with a red box. The main area displays a 'Custom Report' dialog box. Inside, the 'Report Setting' tab is active, showing 'Load Template' (Run Now), 'Name' (Inside to outside Apps), 'Description' (Traffic Log), 'Database' (Traffic Log), 'Time Frame' (Last Hour), 'Sort' (Bytes, Top 100), and 'Group By' (App Category, 50 Groups). To the right, there are two columns: 'Available Columns' (Destination UUID, Destination Vendor, Device Name, Device SN) and 'Selected Columns' (Application, Bytes Sent, Bytes Received, Source Zone, Destination Zone). The 'Selected Columns' section is highlighted with a red box. Below the dialog is a 'Query Builder' section with a text input field ('Please type (or) add a filter using the filter builder') and a 'Filter Builder' button. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

# Custom Security Profile: Anti Virus

**Antivirus Profile**

Name: AV Profile  
Description:

Action | Signature Exceptions | WildFire Inline ML

Enable Packet Capture

Decoders

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	drop	drop	drop
http	drop	drop	drop
http2	drop	drop	drop
imap	alert	alert	alert
pop3	alert	alert	alert
smb	drop	drop	drop
smtp	alert	alert	start

Application Exceptions

APPLICATION	ACTION

Add  Delete

For North-South Traffic Set Actions to Drop  
East-West Set Actions to reset-both

OK Cancel

**Antivirus Profile**

Name: AV Profile  
Description:

Action | Signature Exceptions | WildFire Inline ML

Available Models

MODEL	DESCRIPTION	ACTION SETTING
Windows Executables	Machine Learning engine to dynamically identify malicious PE files	enable (inherit per-protocol actions)
PowerShell Script 1	Machine Learning engine to dynamically detect malicious PowerShell scripts with known length	enable (inherit per-protocol actions)
PowerShell Script 2	Machine Learning engine to dynamically detect malicious PowerShell scripts without known length	enable (inherit per-protocol actions)

File Exceptions

PARTIAL HASH	FILENAME	DESCRIPTION

Add  Delete

Enable inline Machine Learning to stop 0 Day attacks

OK Cancel

# Custom Security Profile: Anti Spyware

Anti-Spyware Profile

POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
drop-crit-hi	critical high	drop	disable
All Alert	any	alert	disable

For North-South Traffic Set Actions to Drop Critical and High and Alert for all other severity levels

East-West Set Actions to reset-both for Critical and High and Alert for other severity levels

Add  Delete  Move Up  Move Down  Clone  Find Matching Signatures

OK Cancel

Anti-Spyware Profile

DNS Policies	Sinkhole	Action	Enabled
default-paloalto-dns	sinkhole	disable	
Ad Tracking Domains	default (informational)	default (allow)	disable
Command and Control Domains	default (high)	sinkhole	disable
Dynamic DNS Hosted Domains	default (informational)	default (allow)	disable
Grayware Domains	default (low)	sinkhole	disable
Malware Domains	default (medium)	sinkhole	disable

Set DNS Security policy to sinkhole and consider setting up your own sinkhole server to capture intelligence on Red team or use loopback address as your sinkhole

DNS Sinkhole Settings

Sinkhole IPv4: IPv4 Loopback IP (127.0.0.1)  
Sinkhole IPv6: IPv6 Loopback IP (-1)

OK Cancel

# Custom Security Profile: Vulnerability Protection

Vulnerability Protection Profile

Name: VP Profile

Description:

Rules | Exceptions

	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Drop-Crit-Hi	any	any	any	critical high	drop	disable
<input checked="" type="checkbox"/>	Alert-All	any	any	any	any	alert	disable

For North-South Traffic set Actions to Drop Critical and High and Alert for all other severity levels

For East-West Traffic set Actions to reset-both for Critical and High and Alert for other severity levels

Add Delete Move Up Move Down

OK Cancel

The screenshot shows a 'Vulnerability Protection Profile' configuration window. The 'Name' field is set to 'VP Profile'. The 'Rules' tab is selected, showing two entries in the table:

	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Drop-Crit-Hi	any	any	any	critical high	drop	disable
<input checked="" type="checkbox"/>	Alert-All	any	any	any	any	alert	disable

Below the table, there are two text boxes with instructions:

- For North-South Traffic set Actions to Drop Critical and High and Alert for all other severity levels
- For East-West Traffic set Actions to reset-both for Critical and High and Alert for other severity levels

At the bottom, there are buttons for 'Add', 'Delete', 'Move Up', 'Move Down', 'OK', and 'Cancel'.

# Custom Security Profile: URL Filtering

**URL Filtering Profile**

Name: URL Profile  
Description:

**Categories** | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
duolingo	alert	allow
business-and-economy	alert	allow
<b>command-and-control</b>	<b>block</b>	<b>block</b>
computer-and-internet-info	alert	allow
content-delivery-networks	alert	allow
copyright-infringement	alert	allow
cryptocurrency	alert	allow
dating	alert	allow

\* indicates a custom URL category, + indicates external  
Check URL Category

**1.** At a minimum block these categories:  
- command and control  
- grayware  
- hacking  
- malware  
**2.** newly registered domains  
- proxy avoidance and anonymizers  
- ransomware

**2. Set all other categories to alert**

OK Cancel

**URL Filtering Profile**

Name: URL Profile  
Description:

**Categories** | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | **Inline ML**

**Available Models**

MODEL	DESCRIPTION	ACTION
Javascript Exploit Detection	Machine Learning engine to dynamically detect Javascript based exploitation attacks	block
Phishing Detection	Machine Learning engine to dynamically identify credential phishing pages for panos versions after 10.2.0	block

**Exceptions**

**Stop 0 day attacks by enabling inline machine learning action to block**

Add Delete OK Cancel

# Custom Security Profile: File Blocking

File Blocking Profile

Name: FB Profile

Description:

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
<input type="checkbox"/> Block Executable files	any	apk asp aspx bat	both	alert
<input checked="" type="checkbox"/> Alert All other downloads	any	any	both	alert

**Add** **Delete**

Block downloading and uploading dangerous files

Alert on all file uploads and downloads

OK Cancel

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
<input type="checkbox"/> Block Executable files	any	apk asp aspx bat	both	alert
<input checked="" type="checkbox"/> Alert All other downloads	any	any	both	alert

# Custom Security Profile: WildFire Analysis

WildFire Analysis Profile (Read Only) ?

Name  Description

**Use Default WildFire Analysis Profile**

<input type="checkbox"/>	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input type="checkbox"/>	default	any	any	both	public-cloud

+ Add - Delete

OK Cancel

<input type="checkbox"/>	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input type="checkbox"/>	default	any	any	both	public-cloud

# Custom Security Groups

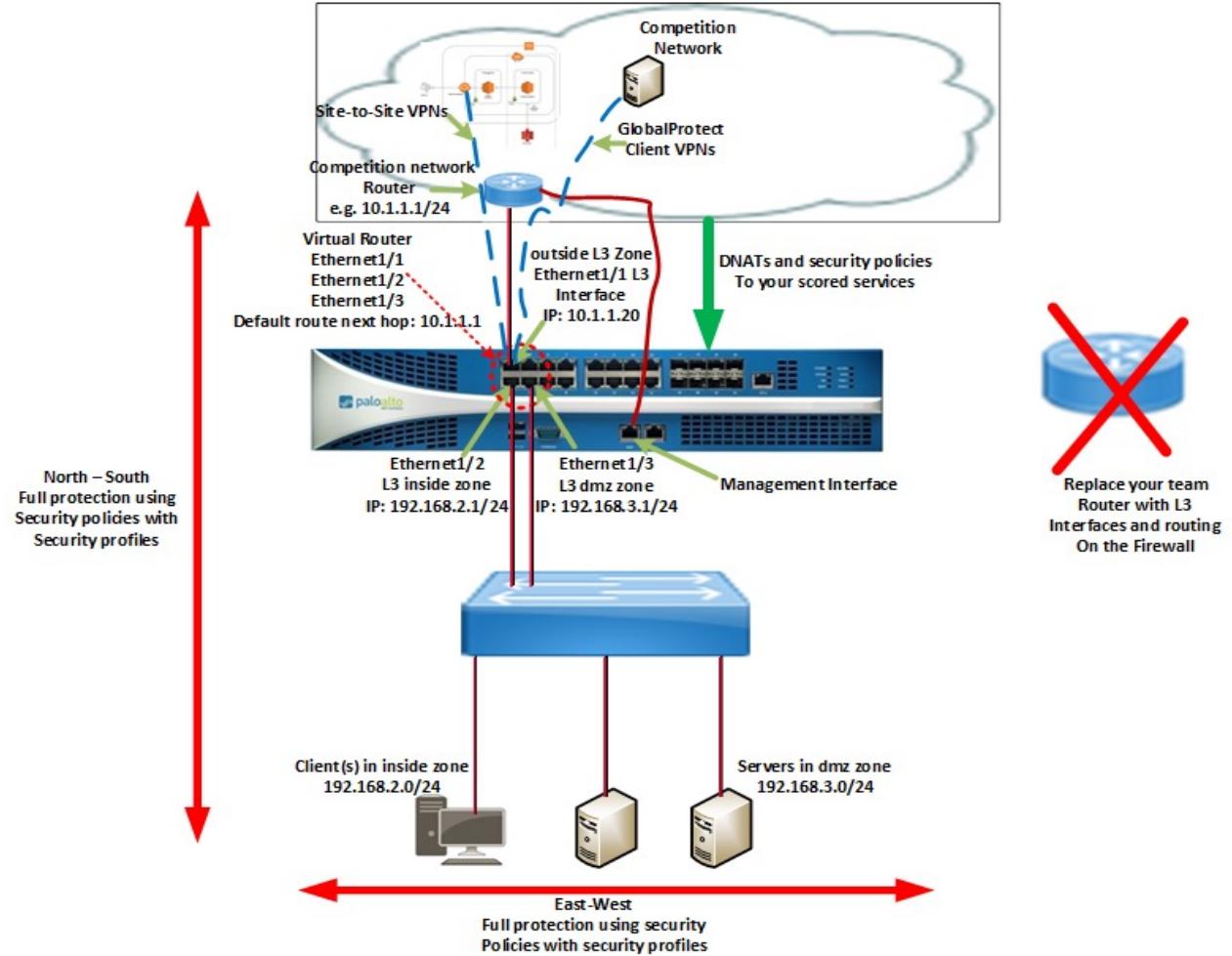
The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. A red box highlights the 'Security Profile Groups' section in the left sidebar. A second red box highlights the 'Name' field in the 'Security Profile Group' dialog, which contains the value 'North-South SG'. The dialog also lists various protection profiles: Antivirus Profile (AV Profile), Anti-Spyware Profile (AS Profile), Vulnerability Protection Profile (AV Profile), URL Filtering Profile (URL Profile), File Blocking Profile (FB Profile), Data Filtering Profile (None), and WildFire Analysis Profile (default). Buttons for 'OK' and 'Cancel' are at the bottom.

The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. A red box highlights the 'Security Profile Groups' section in the left sidebar. A second red box highlights the 'Name' field in the 'Security Profile Group' dialog, which contains the value 'East-West SG'. The dialog lists various protection profiles: Antivirus Profile (AV Profile), Anti-Spyware Profile (AS Profile), Vulnerability Protection Profile (AV Profile), URL Filtering Profile (URL Profile), File Blocking Profile (FB Profile), Data Filtering Profile (None), and WildFire Analysis Profile (default). Buttons for 'OK' and 'Cancel' are at the bottom.

## Network Deployment Option 3: Layer 3 (L3)

- **Most applicable** if your team has a router that you can replace using firewall
  - You will need to create Destination NATs (DNATs) for scored services
  - Firewall supports dynamic routing: ripv2, ospf, ospfv3, bgp
- Pro: Provides both North-South and East-West full protection
  - Allows you to configure firewall site-to-site VPNs and GlobalProtect client VPNs
  - Allows you to use data interfaces for Web-UI access and dynamic updates instead of management interface
- Con: Most complex to set up correctly
- **Replace your team router** with your firewall configured with L3 interfaces
  - Create L3 interfaces and assign them to same firewall virtual router
  - Create a virtual router default static route if not using dynamic routing to competition gateway
  - Assign L3 zones to each L3 interface
  - Connect your team hosts to separate L3 interfaces/zones
  - Create source NAT for egress traffic and Destination NAT policies for scored services
  - Create security policies to allow only essential North-South and East-West traffic

# Network Deployment L3 (Option 3): Network Architecture



## Network Deployment L3 (Option 3): Security Policies

- Configure an inbound and outbound block rule to block unknown and bad urls
- Configure inbound allow rule(s) corresponding to your DNAT policy(ies) for scored services
  - Make rules as specific as possible by using allowed applications and destination IP addresses
- Configure East-West rule(s) for internal traffic
  - Make rules as specific as possible by using allowed applications (application default) and destination IP addresses
  - Only allow internal traffic to and from specific internal IP addresses that are absolutely necessary to keep your services up
- Make sure you assign Security Profiles to all your Security Policy Allow rules
  - The FW will not block malware without Security Profiles assigned to Security Policies
  - Best practice is to create your own Security Profiles to turn on Machine Learning and stop zero-day attacks instead of using pre-configured security profiles
  - Assign your security profiles to a Security Group

# Network Deployment L3 (Option 3): NAT Policies

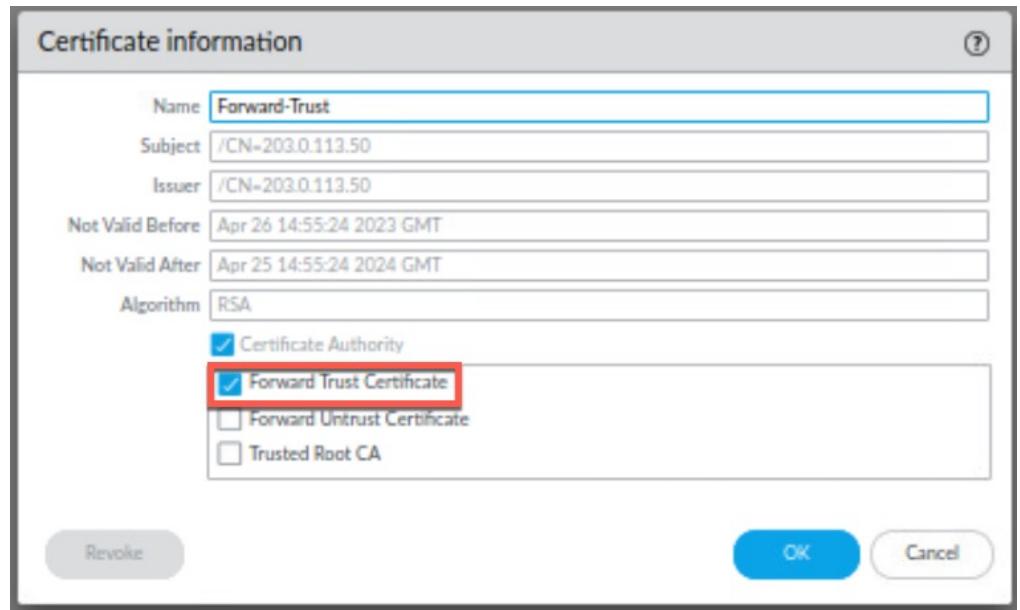
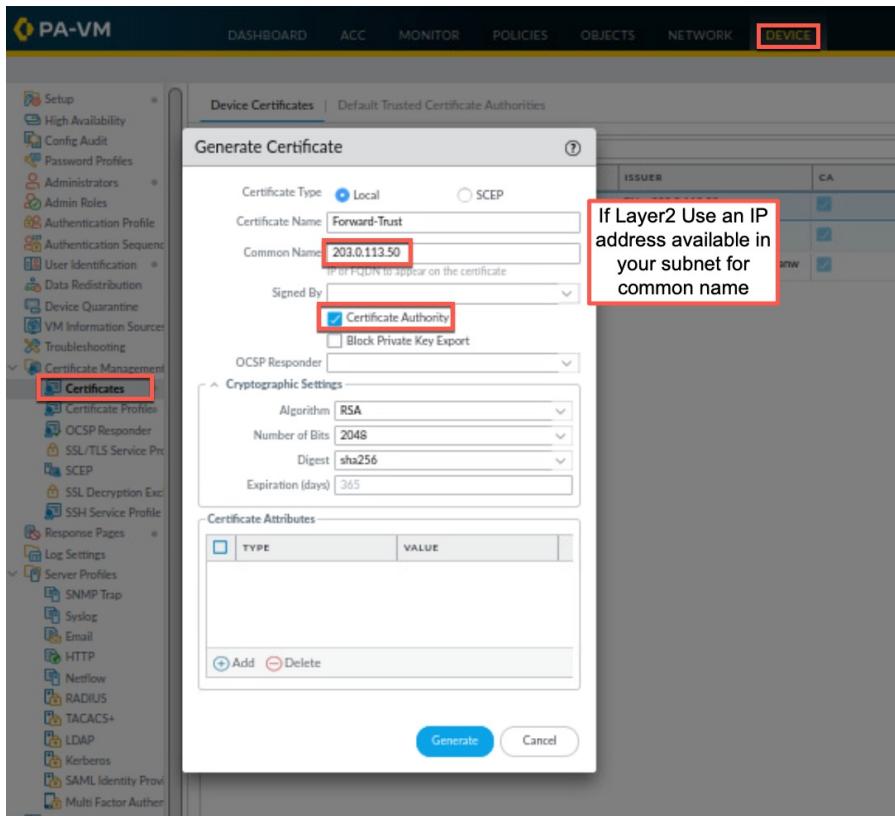
The screenshot shows the Palo Alto VM interface with the following details:

- Header:** DASHBOARD, ACC, MONITOR, POLICIES (highlighted with a red box), OBJECTS, NETWORK, DEVICE.
- Left Sidebar:** Security, NAT (highlighted with a red box), QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, SD-WAN.
- Table:** Displays three NAT policies.

NAME	TAGS	Original Packet						Translated Packet			HIT COUNT
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION		
1 Static-DMZ-NAT	none	dmz	outside	ethernet1/1	192.168.50.10	any	any	static-ip 203.0.113.40 bi-directional: yes	none	-	
2 source-egress-outside	egress	inside	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none	-	
3 Destination-NAT-ec...	none	outside	outside	any	any	203.0.113.75	any	none	destination-translation address: 192.168.50.20	-	

## Step 5: Turn on Decryption

# Forward Trust Decryption for Outbound traffic: Create Trust Certificate



# Forward Trust Decryption for Outbound traffic: Create Untrust Certificate

The image shows two overlapping windows from the PA-VM (Palo Alto Virtual Machine) interface.

**Left Window: Generate Certificate**

- Header:** PA-VM, DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS
- Left Sidebar:** Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, Data Redistribution, Device Quarantine, VM Information Source, Troubleshooting, Certificate Management, Certificates, Certificate Profiles, OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exceptions, SSH Service Profile, Response Pages, Log Settings, Server Profiles, SNMP Trap, Syslog, Email, HTTP, Netflow, RADIUS, TACACS+.
- Form Fields:**
  - Certificate Type: Local (radio button selected)
  - Certificate Name: Forward-untrust (highlighted with a red box)
  - Common Name: forward-untrust (highlighted with a red box)
  - Signed By: Certificate Authority (checkbox checked)
  - OCSP Responder: [dropdown]
  - Cryptographic Settings:
    - Algorithm: RSA
    - Number of Bits: 2048
    - Digest: sha256
    - Expiration (days): 365
  - Certificate Attributes:

Type	Value

Add, Delete buttons
- Buttons:** Generate, Cancel

**Right Window: Certificate information**

- Fields:**
  - Name: Forward-untrust
  - Subject: /CN=forward-untrust
  - Issuer: /CN=forward-untrust
  - Not Valid Before: Apr 26 15:04:13 2023 GMT
  - Not Valid After: Apr 25 15:04:13 2024 GMT
  - Algorithm: RSA
  - Certificate Authority (checkbox checked)
  - Forward Trust Certificate (checkbox unchecked)
  - Forward Untrust Certificate (checkbox checked)
  - Trusted Root CA (checkbox unchecked)
- Buttons:** Revoke, OK, Cancel

# Configure Decryption Profile

The screenshot shows the 'Decryption Profile' configuration page in the PA-VM interface. The 'OBJECTS' tab is selected. The profile name is 'Decrypt Profile'. Under 'SSL Decryption', the setting is 'No Decryption'. In the 'Server Certificate Verification' section, three checkboxes are selected: 'Block sessions with expired certificates', 'Block sessions with untrusted issuers', and 'Block sessions with unknown certificate status'. These three checkboxes are highlighted with a red box. In the 'Unsupported Mode Checks' section, two checkboxes are selected: 'Block sessions with unsupported versions' and 'Block sessions with unsupported cipher suites'. These two checkboxes are also highlighted with a red box. A note at the bottom states: 'Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.' There are 'Details' and 'Cancel' buttons at the bottom.

The screenshot shows the 'Decryption Profile' configuration page with the 'No Decryption' setting selected. A note on the right side of the screen says: 'You want to block bad certs even for traffic you aren't decrypting'. This note is enclosed in a red box. The 'SSL Decryption' dropdown also has a red box around it. The 'No Decryption' option is highlighted. The 'Details' and 'Cancel' buttons are visible at the bottom right.

# Configure Forward Decryption Policy for Outbound Traffic

The screenshot displays three windows from the Palo Alto Networks PA-VM interface:

- Top Left Window:** Shows the main navigation bar with tabs: DASHBOARD, ACC, MONITOR, POLICIES (highlighted), OBJECTS, NETWORK, DEVICE. A sidebar on the left lists various policy categories, with "Decryption" highlighted.
- Top Right Window:** Titled "Decryption Policy Rule". It has tabs: General, Source, Destination, Service/URL Category (highlighted), Options. Under "Service/URL Category", a list shows "service-https" selected. A red box highlights "service-https" and a callout box states: "Use url categories to define the traffic you want to decrypt".
- Bottom Window:** Titled "Decryption Policy Rule". It has tabs: General, Source, Destination, Service/URL Category, Options (highlighted). Under "Action", "Decrypt" is selected (radio button highlighted). Under "Type", "SSL Forward Proxy" is selected (dropdown highlighted). Under "Decryption Profile", "Decrypt Profile" is selected (dropdown highlighted).

# Inbound Decryption: Import Certificates From Your DMZ Server

The screenshot shows the Palo Alto VM (PA-VM) interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The left sidebar has sections like Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management (with Certificates selected), Response Pages, Log Settings, Server Profiles (with SNMP Trap, Syslog, Email, HTTP, and Mailflow selected), and a general section. The main area displays 'Device Certificates | Default Trusted Certificate Authorities' with a table showing three certificates: Forward-Trust, Forward-untrust, and commerce-server. A modal dialog titled 'Import Certificate' is open, showing fields for Certificate Name (commerce-server), Certificate File (C:\fakepath\certificate.pem), File Format (Base64 Encoded Certificate (PEM)), and Key File (C:\fakepath\privatekey.pem). The 'Import Private Key' checkbox is checked. Buttons for OK and Cancel are at the bottom.

# Configure Inbound Decryption for Your DMZ Server

The screenshot displays the Palo Alto Networks Management Console interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES (highlighted with a red box), OBJECTS, NETWORK, and DEVICE. On the left sidebar, under the Security section, the 'Decryption' option is selected (also highlighted with a red box). The main content area shows a table of existing decryption policies:

NAME	TAGS	Source				Destination	
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1 Forward-Decryption	none	L2-dmz	any	any	any	L2-outside	any
2 Inbound-decryption	none	L2-outside	any	any	any	L2-dmz	any

A modal window titled 'Decryption Policy Rule' is open, showing the configuration for a new rule named 'Inbound-decryption'. The 'General' tab is selected. The 'Name' field contains 'Inbound-decryption'. The 'Description' field is empty. The 'Tags' dropdown is set to 'None'. The 'Group Rules By Tag' dropdown is also set to 'None'. The 'Audit Comment' field is empty. At the bottom of the modal are 'OK' and 'Cancel' buttons.

To the right of the modal, a detailed configuration window for the 'Inbound-decryption' rule is shown. It has tabs for General, Source, Destination, Service/URL Category, Options (selected), and Log Settings. Under Options, the 'Action' is set to 'Decrypt' (radio button selected). The 'Type' is 'SSL Inbound Inspection'. The 'Certificate' dropdown is set to 'commerce-server'. The 'Decryption Profile' dropdown is set to 'Decrypt Profile'. Under Log Settings, the 'Log Successful SSL Handshake' checkbox is unchecked, and the 'Log Unsuccessful SSL Handshake' checkbox is checked. The 'Log Forwarding' dropdown is set to 'None'. At the bottom of this window are 'OK' and 'Cancel' buttons.

# How to Perform a Factory Reset

## How to perform a factory reset if you lose control of your NGFW

**“I give you the light of Eärendil, our most beloved star. May it be a light for you in dark places, when all other lights go out.”**

- Hopefully, you backed up your firewall configuration settings, but hope is not a strategy
- You will need to relicense your appliance after a reset

URL Article for hardware appliances:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldXCAS>

Youtube video for Virtual Appliance: [https://www.youtube.com/watch?v=47H\\_sSjMMJw](https://www.youtube.com/watch?v=47H_sSjMMJw)

- Only difference for virtual appliances is you hit the space bar at the instant of reboot and then quickly type "maint"
- Much better to restore a virtual appliance from a licensed snapshot.
- Hopefully, you took a snapshot of your appliance after you licensed it and configured it
- But then hope is not a strategy

#### Resolution

The following steps describe how to perform a factory reset on a Palo Alto Networks device.

Note: If running PAN-OS 8.1.x and above, review the following link to perform SSH into Maintenance Mode: [How to SSH into Maintenance Mode](#)

#### Steps

1) 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.

2) Power on to reboot the device.

3) During the boot sequence, the screen should look like this:

```
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: octetmgm0, 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#: 20111222A11934900000
      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.

Entry: maint

Booting to maint mode.
```

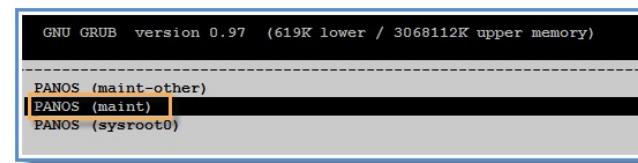
1) Type **maint** to enter maintenance mode.

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

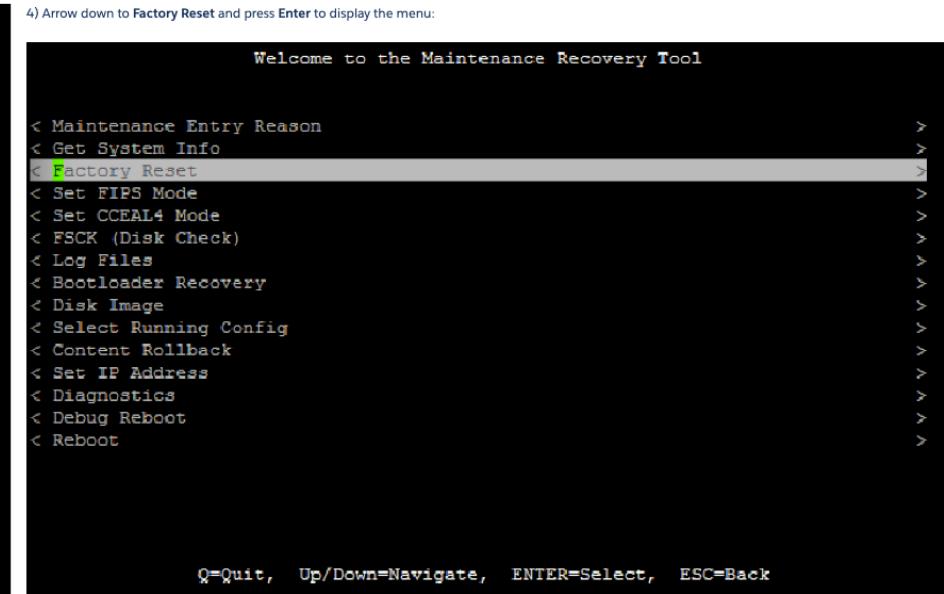
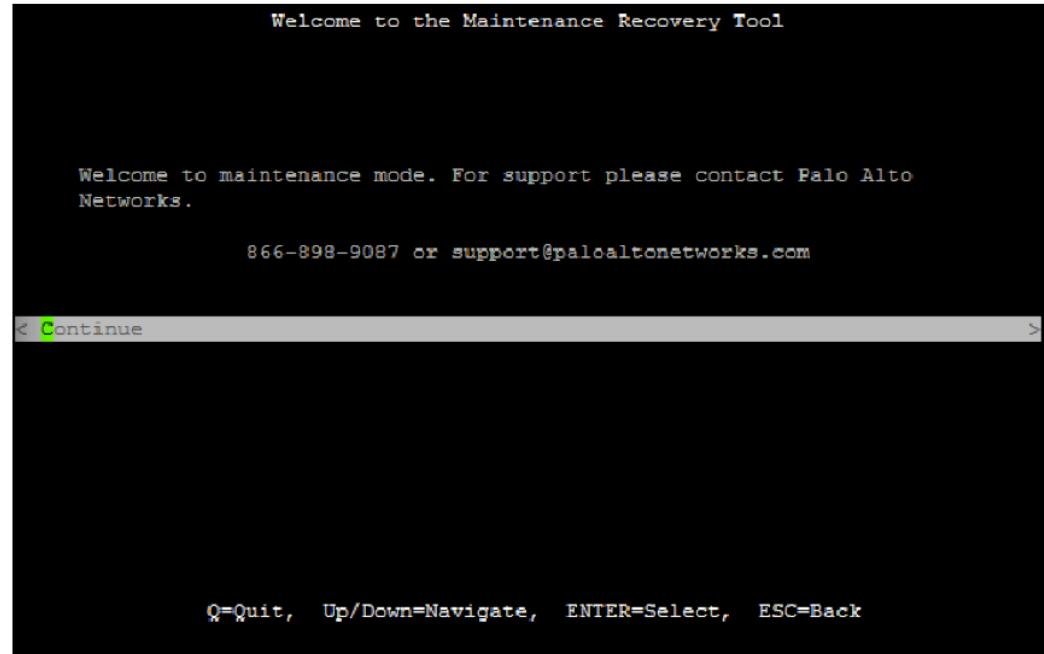
**Entry: maint**

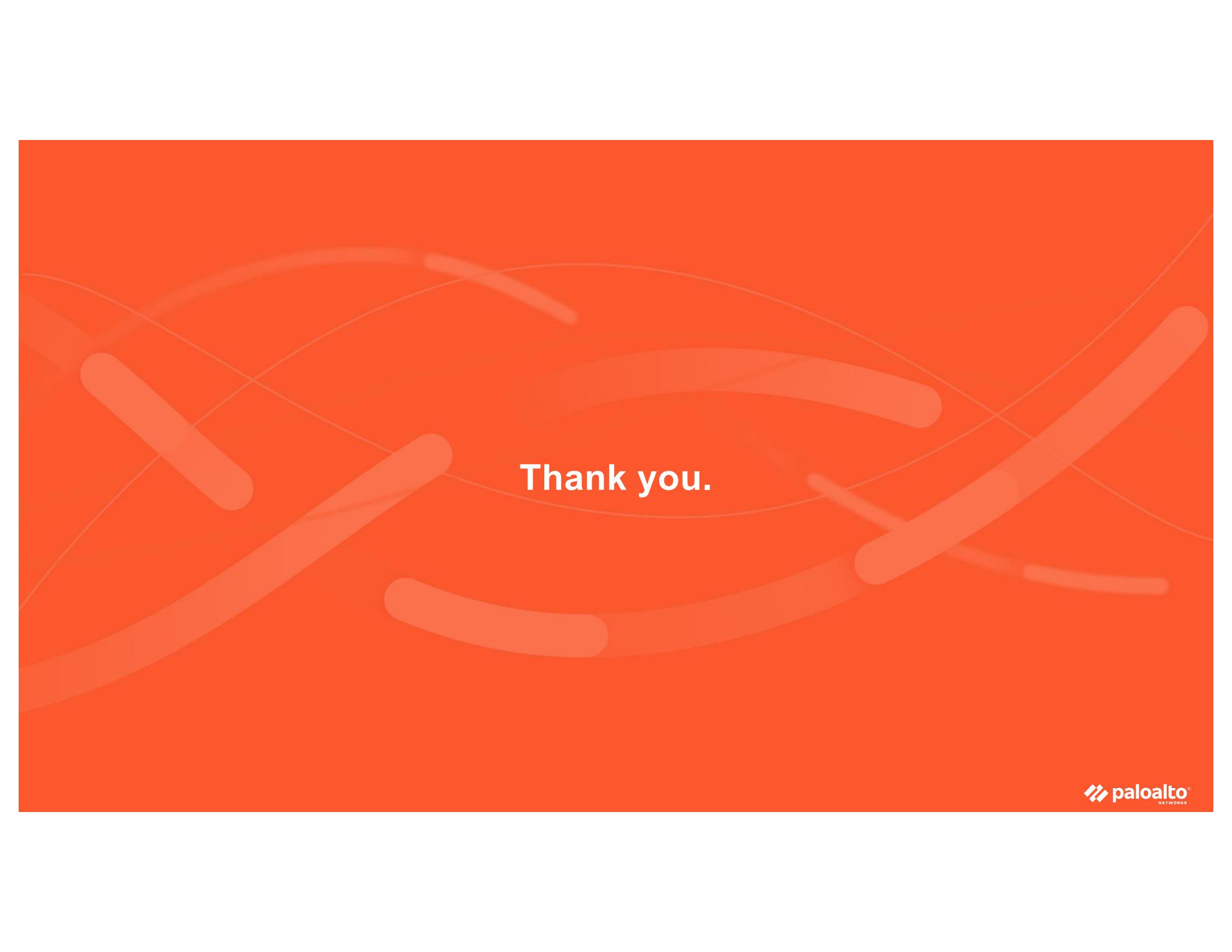
**Booting to maint mode.**

2) 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 continue.



3) Once in maintenance mode, the following is displayed, please press enter to continue:





Thank you.