



CCDC Quick Start Guide for NGFW Deployment and Configuration



Jim Boardman – Cybersecurity Academy
Tom Trevethan – Cybersecurity Academy

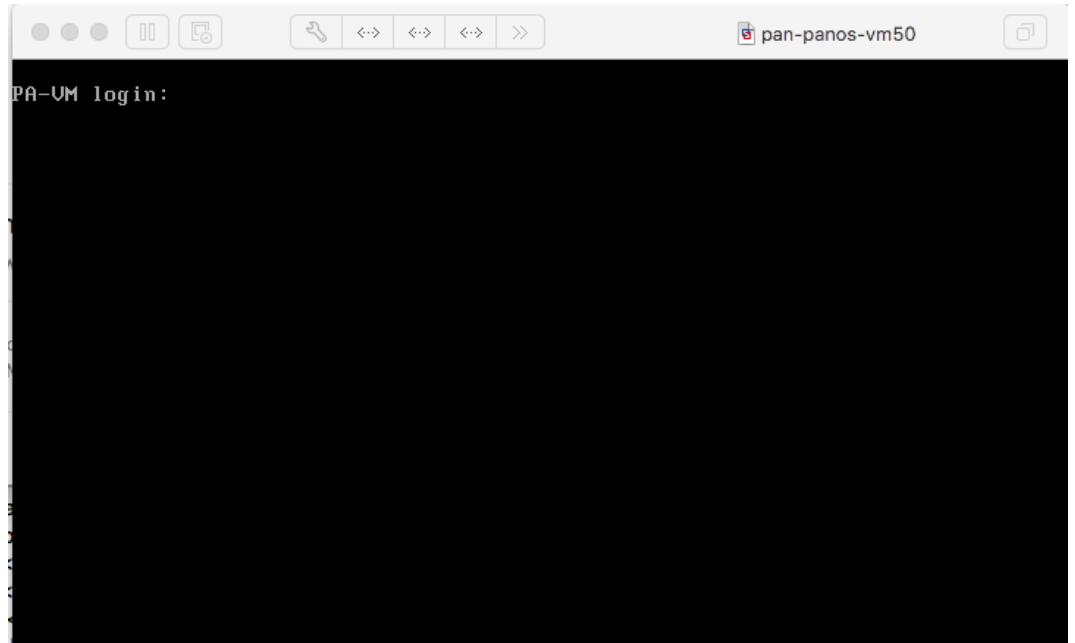
Quick Start - Critical Steps to Secure and Deploy the Firewall Appliance in order to Protect the Network

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

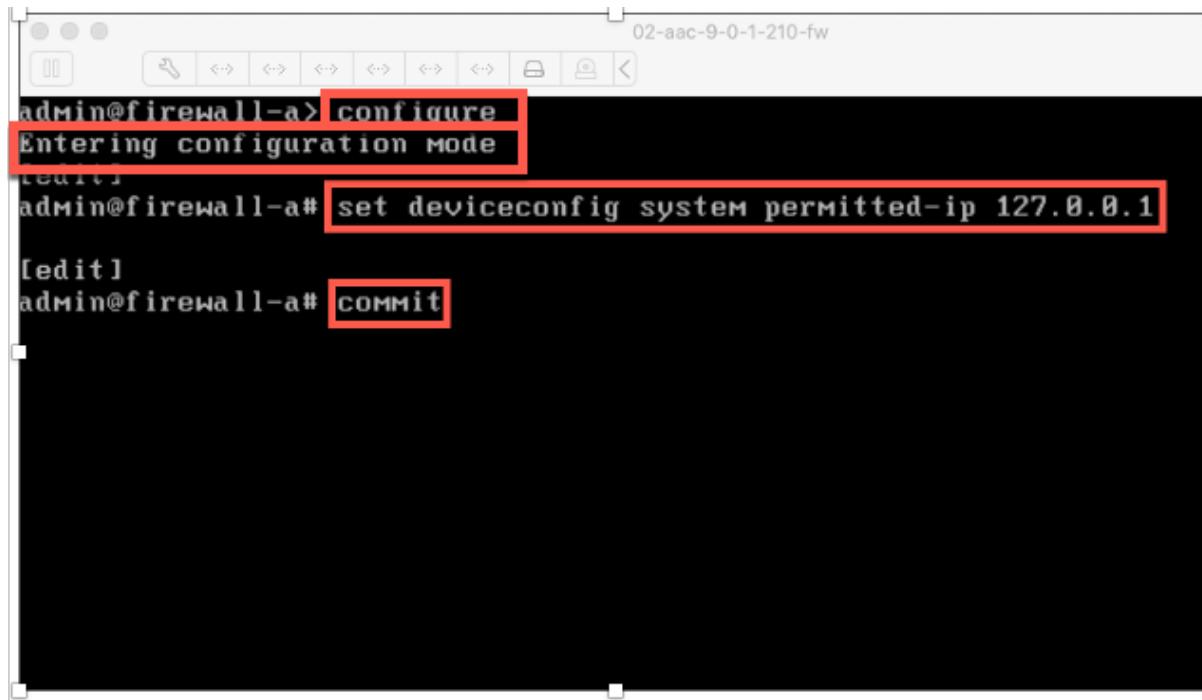
- Hypervisor Console Port
 - Default UN: admin
 - Default PWD: admin



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



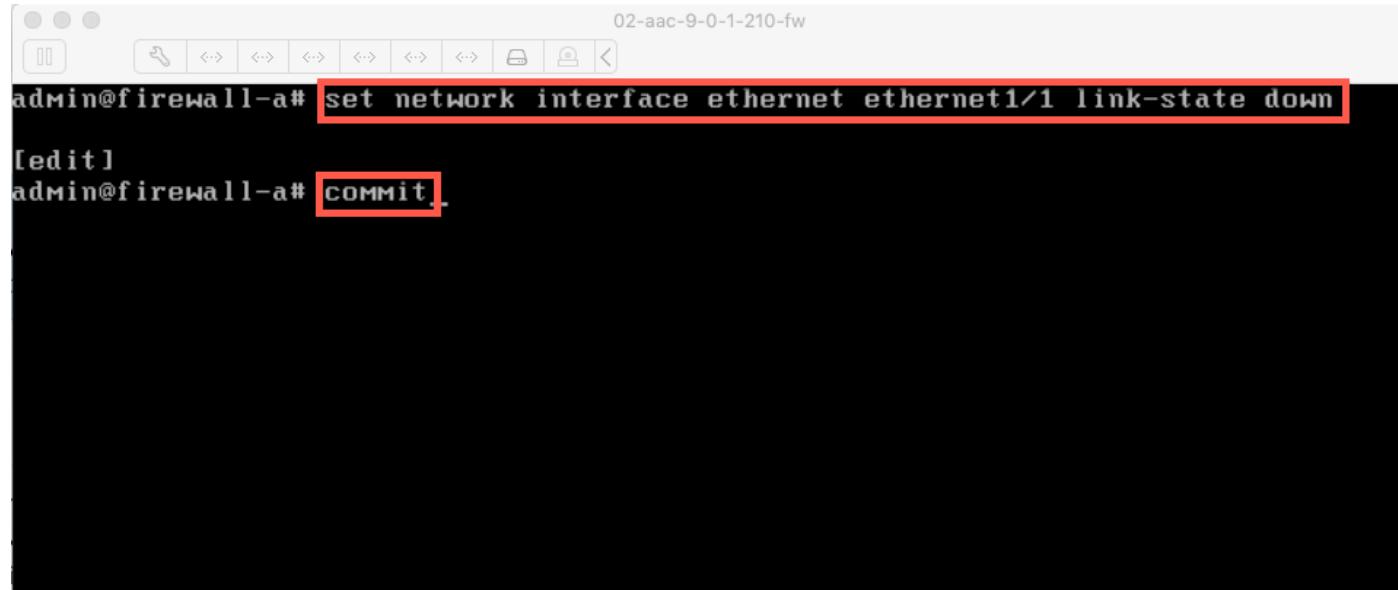
The screenshot shows a terminal window titled "02-aac-9-0-1-210-fw". The command history is as follows:

```
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 commands "configure", "set deviceconfig system permitted-ip 127.0.0.1", and "commit" are highlighted with red boxes.

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

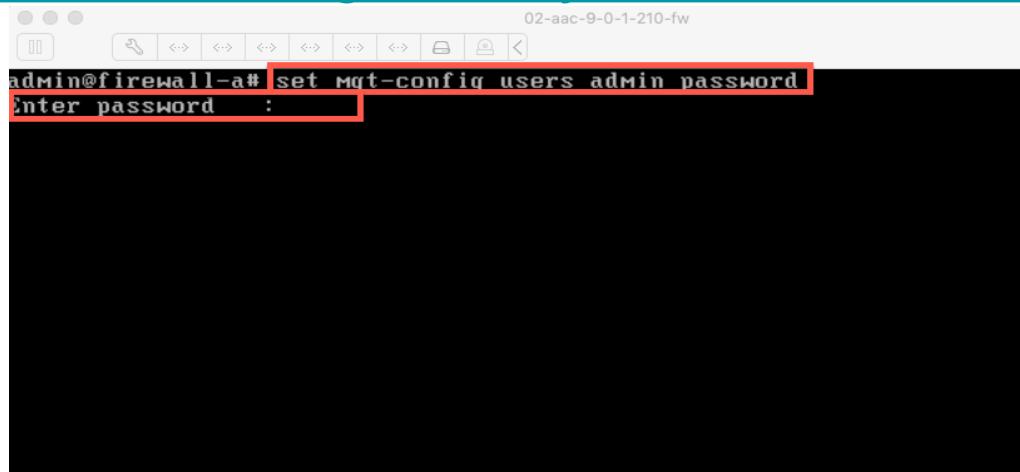
- Configure Mode **#set network interface ethernet ethernet1/x link-state down**
- **#commit**



The screenshot shows a terminal window titled "02-aac-9-0-1-210-fw". The command entered is "admin@firewall-a# set network interface ethernet ethernet1/1 link-state down". Below it, the command "[edit]" is shown, followed by "admin@firewall-a# commit". The "set" command and the "commit" command are highlighted with a red 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/11-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-ssh-key-based-administrator-authentication-to-the-cli>



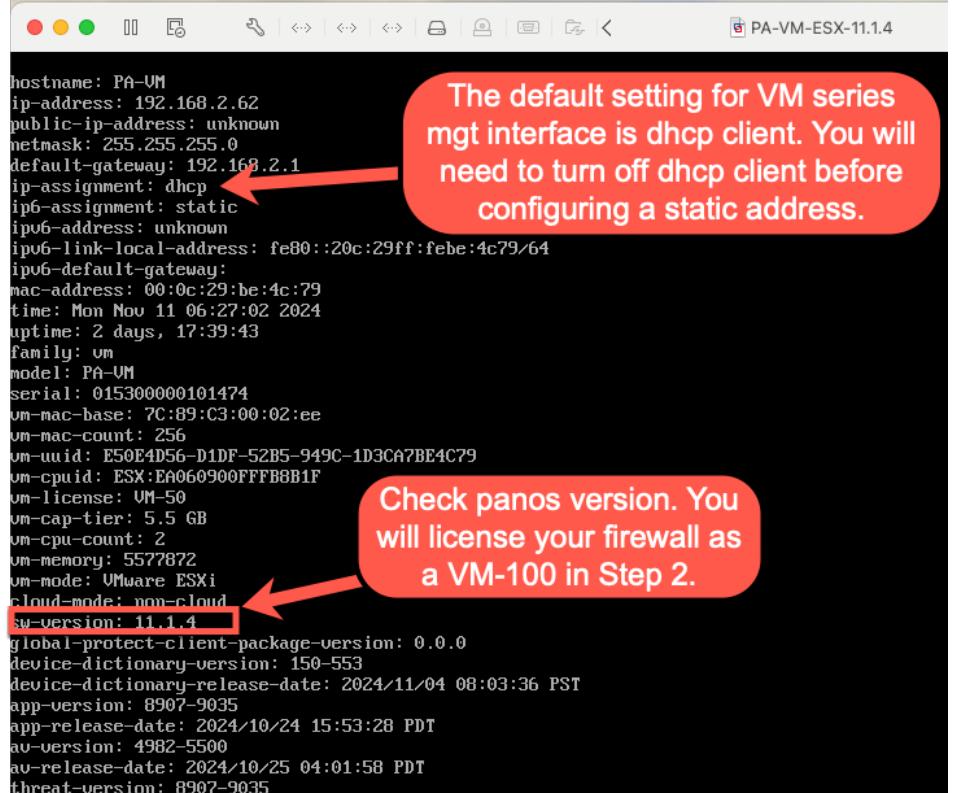
```
02-aac-9-0-1-210-fw
admin@firewall-a# set mgt-config users admin password
Enter password : [REDACTED]
```

Securing the 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: PA-VM  
ip-address: 192.168.2.62  
public-ip-address: unknown  
netmask: 255.255.255.0  
default-gateway: 192.168.2.1  
ip-assignment: dhcp  
ip6-assignment: static  
ip6-address: unknown  
ip6-link-local-address: fe80::20c:29ff:febe:4c79/64  
ip6-default-gateway:  
mac-address: 00:0c:29:be:4c:79  
time: Mon Nov 11 06:27:02 2024  
uptime: 2 days, 17:39:43  
family: vm  
model: PA-VM  
serial: 015300000101474  
vm-mac-base: 7C:89:C3:00:02:ee  
vm-mac-count: 256  
vm-uuid: E50E4D56-D1DF-52B5-949C-1D3CA7BE4C79  
vm-cpuid: ESX:EA060900FFFB8B1F  
vm-license: VM-50  
vm-cap-tier: 5.5 GB  
vm-cpu-count: 2  
vm-memory: 5577872  
vm-mode: VMware ESXi  
cloud-mode: non-cloud  
sw-version: 11.1.4  
global-protect-client-package-version: 0.0.0  
device-dictionary-version: 150-553  
device-dictionary-release-date: 2024/11/04 08:03:36 PST  
app-version: 8907-9035  
app-release-date: 2024/10/24 15:53:28 PDT  
av-version: 4982-5500  
av-release-date: 2024/10/25 04:01:58 PDT  
threat-version: 8907-9035
```

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. You will license your firewall as a VM-100 in Step 2.

Securing FW Appliance: Only Allow Secure Protocols To Connect to Mgt Interface

- 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-http
+ disable-http-ocsp             disable-http-ocsp
+ disable-https                 disable-https
+ disable-icmp                  disable-icmp
+ disable-snmp                  disable-snmp
+ disable-ssh                   disable-ssh
+ disable-telnet                disable-telnet
+ disable-userid-service        disable-userid-service
+ disable-userid-syslog-listener-ssl disable-userid-syslog-listener-ssl
+ disable-userid-syslog-listener-udp disable-userid-syslog-listener-udp
admin@PA-VM# set deviceconfig system service disable-
```

Secure FW Appliance: Show all Admin Accounts

- 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 displays two terminal windows side-by-side. Both windows have a black background and white text. The top window shows the command `show admins all` and lists four users: `admin`, `panorama`, `_openconfig`, and `red_team`. A red box highlights the `red_team` entry, and a red arrow points from it to a red callout bubble containing the text "Delete this one". The bottom window shows the configuration mode sequence: `configure`, `[edit]`, `delete mgt-config users red_team`, and `[edit]`. The command `delete mgt-config users red_team` and its confirmation in configuration mode are highlighted with red boxes.

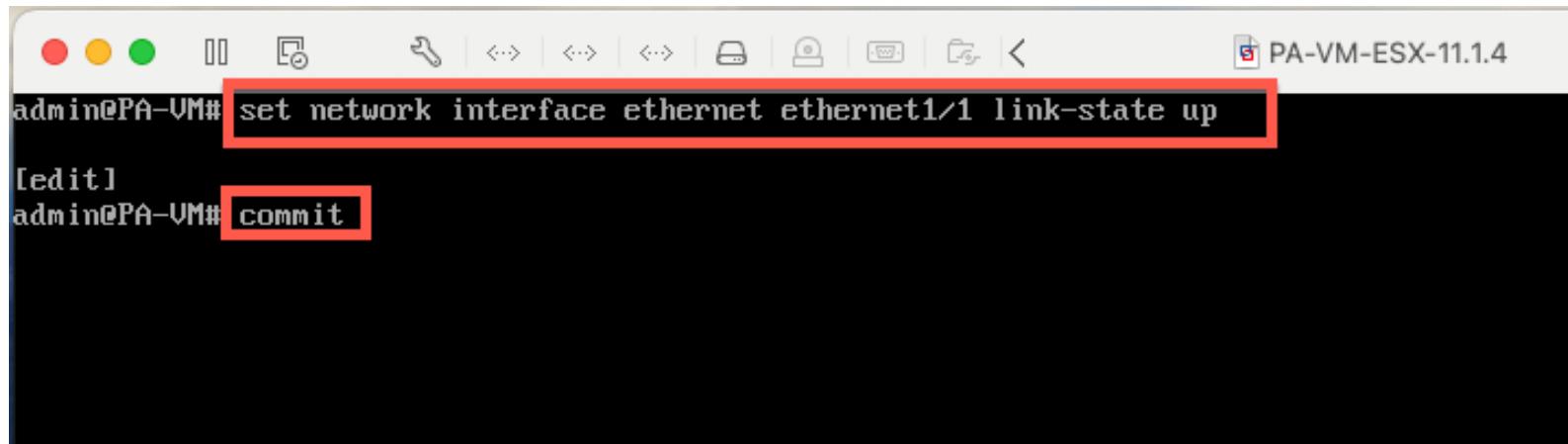
```
admin@PA-VM> show admins all
admin
panorama
_openconfig
red_team
Delete this one
admin@PA-VM>

admin@PA-VM> show admins all
admin
panorama
__openconfig
red_team

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

Secure FW Appliance: Turn Data Interfaces Back On If Turned Off

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

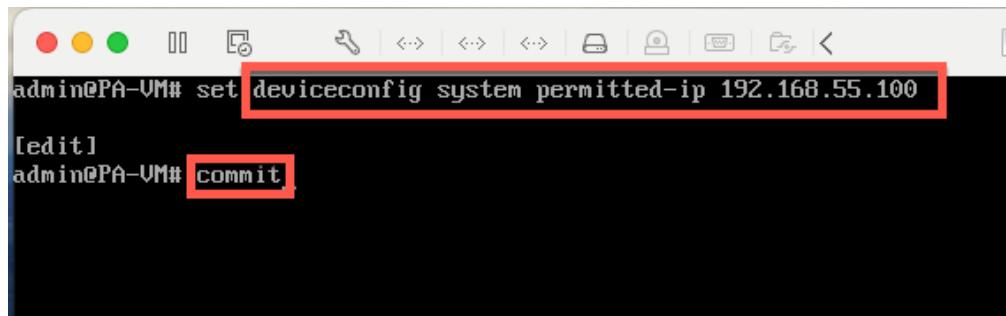


The screenshot shows a terminal window with a black background and white text. At the top, there are several icons followed by the text "PA-VM-ESX-11.1.4". Below this, the command "admin@PA-VM# set network interface ethernet ethernet1/1 link-state up" is entered, highlighted with a red box. After pressing Enter, the text "[edit]" appears. Then, the command "admin@PA-VM# commit" is entered and highlighted with a red box.

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

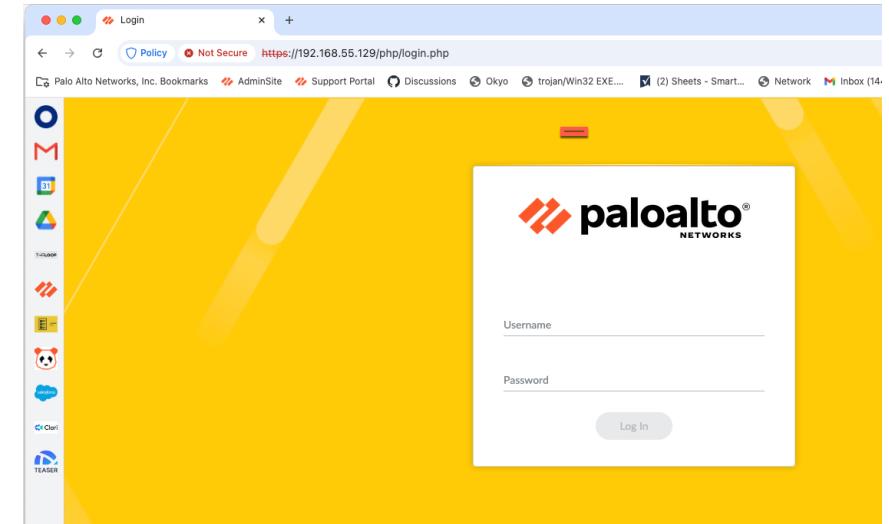
Securing the FW Appliance: Turn Management Interface Back On

- 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



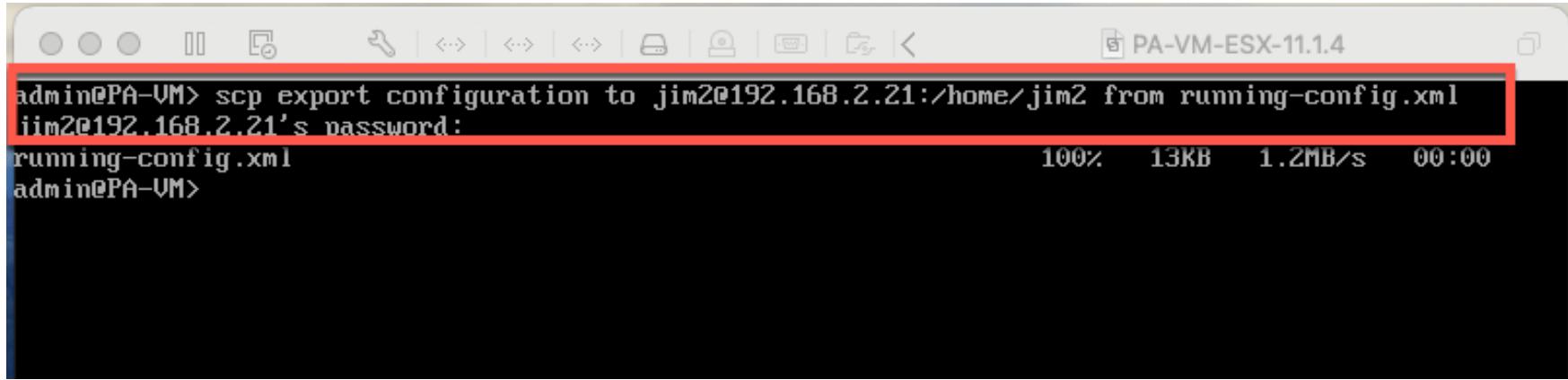
A terminal window showing configuration mode commands. The user has entered 'set deviceconfig system permitted-ip 192.168.55.100' and then '[edit]'. The line 'set deviceconfig system permitted-ip 192.168.55.100' is highlighted with a red box.

```
admin@PA-VM# set deviceconfig system permitted-ip 192.168.55.100
[edit]
admin@PA-VM# commit
```



Securing the FW: Back Up Your FW Config and/or Take Snapshot of Virtual Firewall Appliance

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



The screenshot shows a terminal window titled "PA-VM-ESX-11.1.4". The command entered is "admin@PA-VM> scp export configuration to jim2@192.168.2.21:/home/jim2 from running-config.xml". A red box highlights this command. The terminal then prompts for a password: "jim2@192.168.2.21's password:". Below the command, the status of the transfer is shown: "running-config.xml" with progress "100%", size "13KB", rate "1.2MB/s", and time "00:00". The command concludes with "admin@PA-VM>".

Step 2: License the firewall appliance

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

The screenshot shows two views of the Palo Alto Networks VM interface. The top view is a full-screen window titled 'PA-VM' with a red border. The bottom view is a smaller window titled 'PA-VM' with a black border.

Top View (Red Border):

- Header: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE (highlighted).
- Left Sidebar:
 - Setup
 - High Availability
 - Config Audit
 - Password Profiles
 - Administrators
 - Role Based Access Control
 - Authentication Profile
 - User Identification
 - Data Redistribution
 - Virtual Machine
 - VM Information Sources
 - Troubleshooting
 - Certificate Management
 - Certificates
 - SSL/TLS Profile
 - OCSP Responder
 - SSL/TLS Service Profile
 - SCP
 - SSL Decryption
 - SSH Service Profile
 - Response Pages
- Main Content:
 - License Management**
 - Retrieve license keys from license server
 - Activate feature using authorization code (highlighted)
 - Manually upload license key
 - Deactivate VM
 - Upgrade VM capacity
- Bottom Right: A red circle with the number '3'.

Bottom View (Black Border):

- Header: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE (highlighted).
- Left Sidebar:
 - SSH Service Profile
 - Response Pages
 - Log Settings
 - Server Profiles
 - SNMP Trap
 - Syslog
 - Email
 - HTTP
 - Netflow
 - RADIUS
 - SCP
 - TACACS+
 - LDAP
- Main Content:
 - License Management**
 - Retrieve license keys from license server
 - Activate feature using authorization code (highlighted)
 - Manually upload license key
 - Deactivate VM
 - Upgrade VM capacity
 - Update License**
 - Authorization Code (highlighted)
 - Download Authorization File
 - OK
 - Cancel
- Bottom Left: A red circle with the number '4'.

Right Side (Red Box):

- DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE (highlighted).
- PA-VM
- Adv Threat Prevention
- BrightCloud URL Filtering
- GlobalProtect Gateway
- PAN-DB URL Filtering
- SD WAN
- STI WAN
- Threat Prevention
- Premium
- DNS Security
- GlobalProtect Portal
- License Management

Each license entry includes fields for Date Issued, Date Expires, and Description.

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 Networks PA-VM Device interface. The 'DEVICE' tab is selected. In the left sidebar, under 'Dynamic Updates', there is a red box around the 'Check Now' button. A large red arrow points from this button towards the bottom of the screen, where a red box contains the text: 'Click Check now and then download and install the latest updates and schedule future downloads and installations.' There are also red boxes highlighting the 'Schedule' fields for different sections: 'Every day at 06:30 (Download and Install)' for Antivirus, 'Every Wednesday at 01:02 (Download and Install)' for Applications and Threats, and 'Every Sunday at 07:45 (None)' for GlobalProtect Clientless VPN.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION
Antivirus									
Last checked: 2023/04/24 13:44:13 PDT	Schedule: Every day at 06:30 (Download and Install)								
4423-4940	panup-all-antivirus-4423-4940		Full	119 MB	42a6c45fc6124...	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	5ec90cf76e231...	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	✓	✓	
Applications and Threats									
Last checked: 2023/04/24 13:31:53 PDT	Schedule: Every Wednesday at 01:02 (Download and Install)								
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	b57b585d2126c...	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
GlobalProtect Clientless VPN									
Last checked: 2023/04/24 13:49:33 PDT	Schedule: Every Sunday at 07:45 (None)								
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	✓	✓	
GlobalProtect File									
Schedule: None									
Device Dictionary									
Last checked: 2023/04/24 13:31:20 PDT									
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			
WildFire									
Last checked: 2023/04/24 13:51:00 PDT	Schedule: Real-time								
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	✓	✓	

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

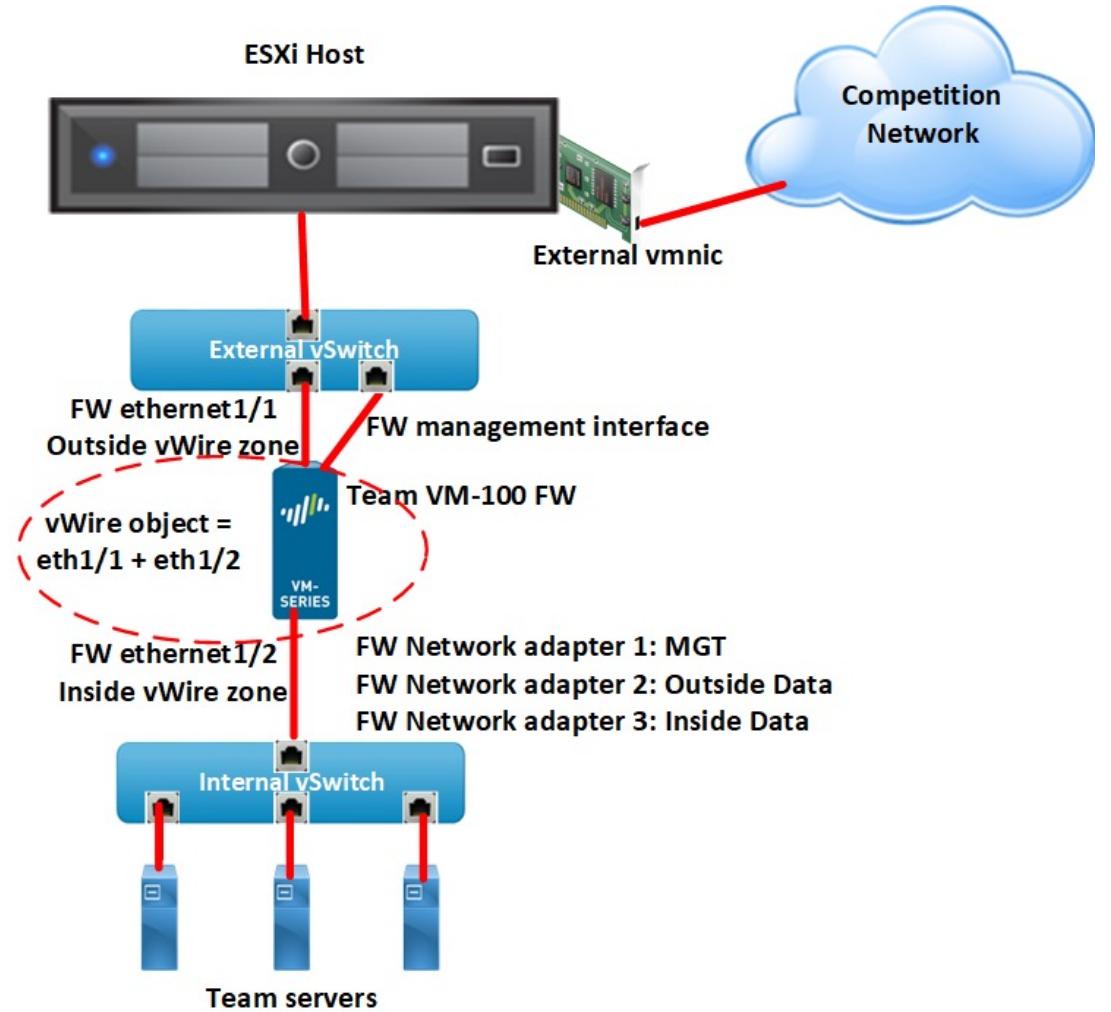
3 Network Deployment Options:

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

Network Deployment Option 1: Virtual Wire (Vwire)

- Rapid deployment: the easiest and quickest set up
 - 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 malware pivoting

Network Deployment (Option 1): Vwire Architecture



Network Deployment (Option 1): Vwire Security Policies

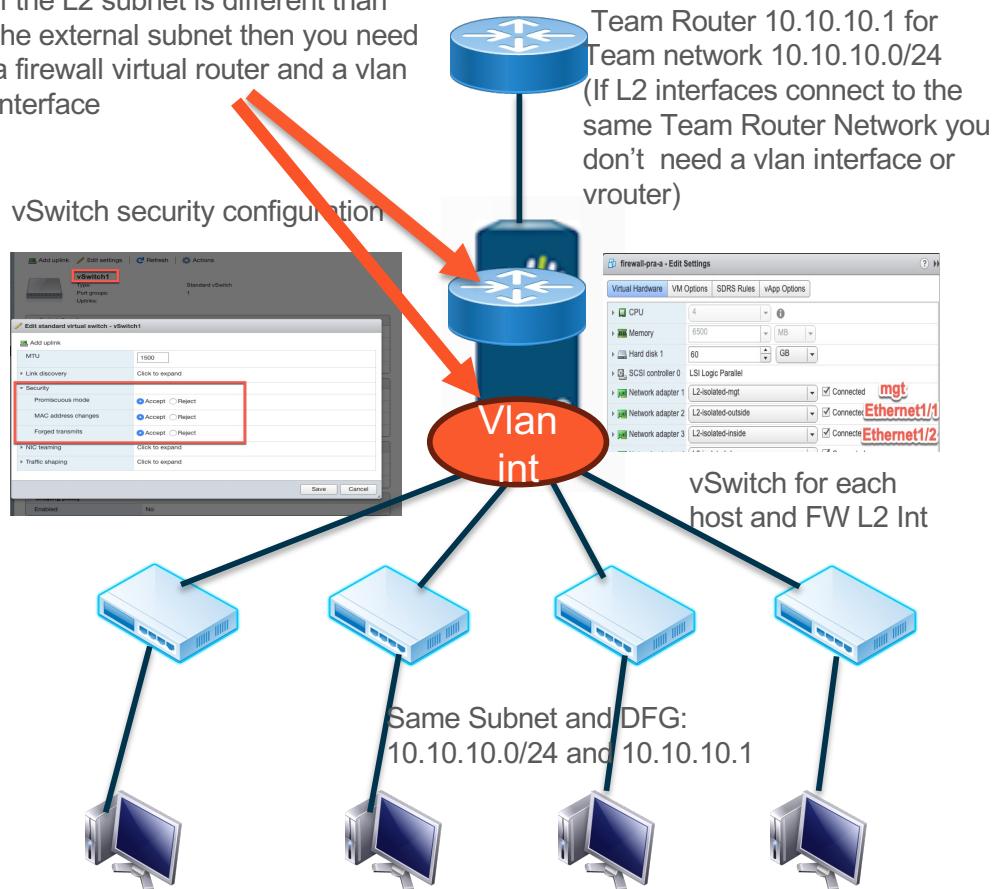
- Configure an inbound and outbound block rule to block unknown and bad urls
- Configure inbound allow rule(s) for scored services
 - Make rules as specific as possible by using allowed applications and destination IP addresses
- Configure outbound allow rule(s)
 - Make rules as specific as possible 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

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 zone
6. If connecting to different networks, connect the FW VLAN int and your FW external L3 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 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. On the left, a sidebar menu lists various monitoring categories such as Logs, 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, and Reports. A red box highlights the 'Manage Custom Reports' option under Reports. The main content area displays a 'Custom Report' dialog box. Inside, the 'Report Setting' tab is active, showing fields for Name ('Inside to outside Apps'), Description, Database ('Traffic Log'), Time Frame ('Last Hour'), Sort ('Bytes'), and Group By ('App Category'). To the right, there are two sections: '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 also highlighted with a red box. At the bottom of the dialog are 'Filter Builder' and 'Cancel' buttons.

Custom Security Profile: Anti Virus

The image displays two side-by-side screenshots of the Palo Alto Networks UI for configuring an Anti Virus profile.

Left Screenshot (Antivirus Profile):

- General:** Name: AV Profile, Description: [empty].
- Actions:** Action | Signature Exceptions | WildFire Inline ML.
- Protocol Actions:** A table showing actions for various protocols:

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:** An empty table with columns: APPLICATION and ACTION.
- Buttons:** OK, Cancel.

Annotations: Two red boxes highlight specific sections:

- A red box surrounds the "For North-South Traffic Set Actions to Drop" and "East-West Set Actions to reset-both" sections.
- A red box surrounds the "Enable inline Machine Learning to stop 0 Day attacks" section in the right screenshot.

Right Screenshot (Antivirus Profile):

- General:** Name: AV Profile, Description: [empty].
- Actions:** Action | Signature Exceptions | WildFire Inline ML.
- Available Models:** A table listing available machine learning 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:** An empty table with columns: PARTIAL HASH, FILENAME, DESCRIPTION.
- Buttons:** OK, Cancel.

Annotations: A red box surrounds the "Enable inline Machine Learning to stop 0 Day attacks" section.

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	NAME	DESCRIPTION	TYPE	STATUS
default-paloalto-dns			sinkhole	disable
Ad Tracking Domains			default (informational)	default (allow)
Command and Control Domains			default (high)	sinkhole
Dynamic DNS Hosted Domains			default (informational)	default (allow)
Grayware Domains			default (low)	sinkhole
Malware Domains			default (medium)	sinkhole

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 screen. At the top, there are fields for 'Name' (set to 'VP Profile') and 'Description'. Below these are tabs for 'Rules' (selected) and 'Exceptions'. The main area contains a table with columns: RULE NAME, THREAT NAME, CVE, HOST TYPE, SEVERITY, ACTION, and PACKET CAPTURE. There are three rows in the table: one empty row with an empty checkbox, a row for 'Drop-Crit-Hi' with a checked checkbox, and a row for 'Alert-All' with a checked checkbox. Below the table, there are descriptive text boxes with instructions for traffic types. At the bottom, there are buttons for 'Add', 'Delete', and 'Move' operations, along with 'OK' and 'Cancel' buttons.

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
command-and-control	block	block
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

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

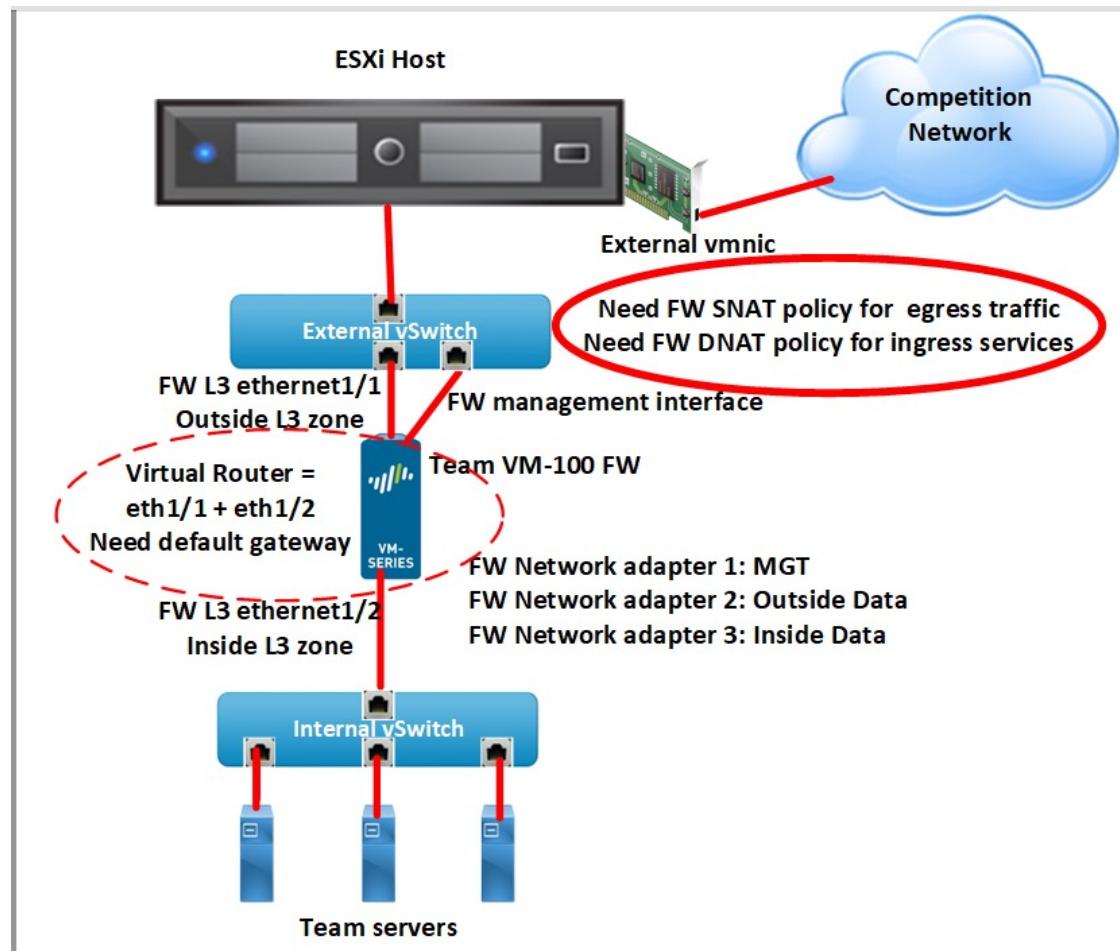
The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. A red box highlights the 'Security Profile Groups' section in the left sidebar. A second red box highlights the 'Name' field in the 'Security Profile Group' dialog, which contains the value 'North-South SG'. The dialog also lists 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

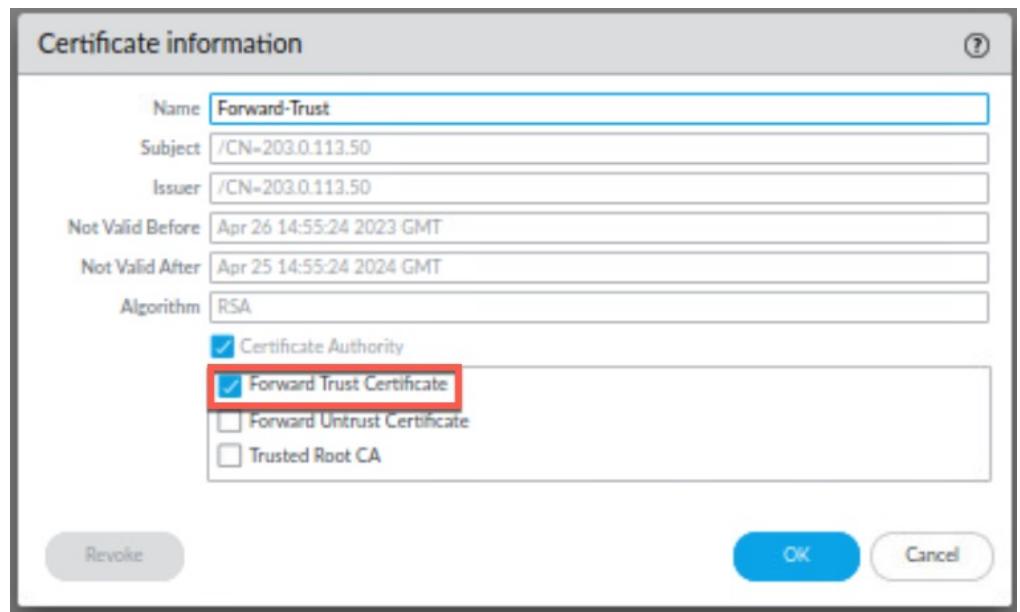
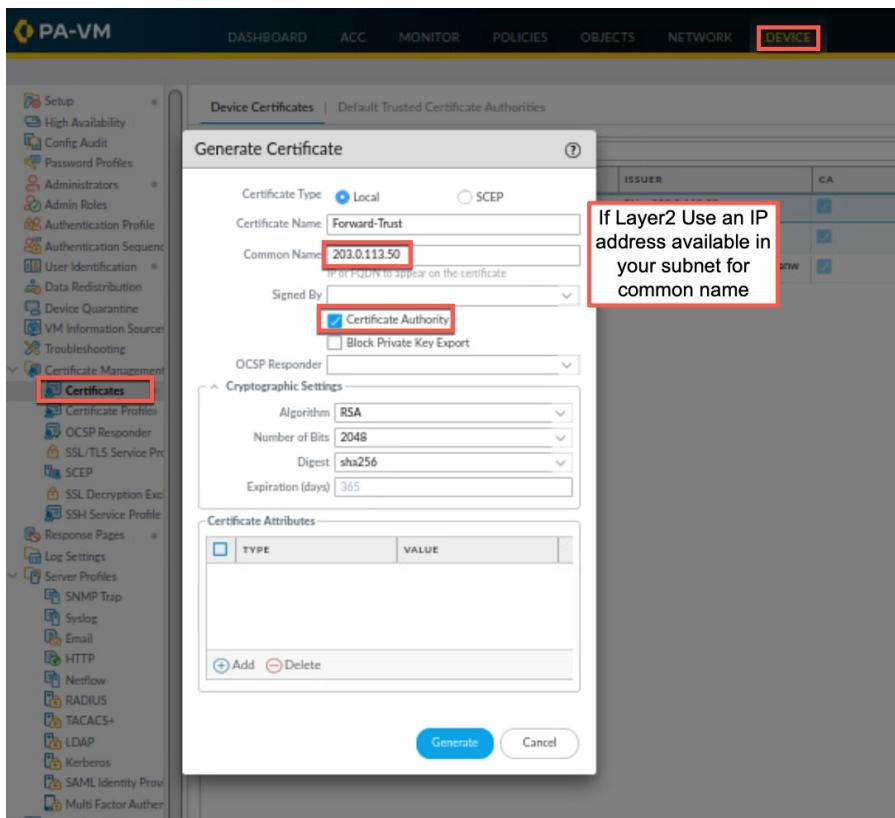
The screenshot shows the Palo Alto VM interface with the following details:

- 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) web 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

- Header:** Certificate information
- Form 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 Palo Alto Networks PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, **OBJECTS** (which is highlighted with a red box), NETWORK, and DEVICE. On the left, a sidebar lists various objects like Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, Devices, GlobalProtect (with HIP Objects and HIP Profiles), External Dynamic Lists, Custom Objects (Data Patterns, Spyware, Vulnerability, URL Category), Security Profilers (Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, WildFire Analysis, Data Filtering, DoS Protection, Mobile Network Protection, SCTP Protection), Security Profile Groups, Log Forwarding, Authentication, and a section for Decryption. Under Decryption, there is a 'Decryption Profile' item which is also highlighted with a red box. The main content area is titled 'Decryption Profile' and shows a configuration for 'Decrypt Profile'. It includes sections for 'SSL Decryption' (set to 'No Decryption'), 'SSL Forward Proxy' (SSL Inbound Inspection and SSL Protocol Settings), 'Server Certificate Verification' (checkboxes for 'Block sessions with expired certificates', 'Block sessions with untrusted issuers', and 'Block sessions with unknown certificate status' are checked and highlighted with a red box), 'Unsupported Mode Checks' (checkboxes for 'Block sessions with unsupported versions' and 'Block sessions with unsupported cipher suites' are checked and highlighted with a red box), 'Failure Checks' (checkboxes for 'Block sessions if resources not available', 'Block sessions if HSM not available', and 'Block downgrade on no resource' are unchecked), and 'Client Extension' (checkbox for 'Strip ALPN' is unchecked). 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.' At the bottom right are 'OK' and 'Cancel' buttons.

This screenshot shows a detailed view of the 'Decryption Profile' configuration dialog. The 'Name' field is set to 'Decrypt Profile'. The 'SSL Decryption' dropdown is set to 'No Decryption' (highlighted with a red box) and 'SSH Proxy'. The 'Server Certificate Verification' section contains two checked checkboxes: 'Block sessions with expired certificates' and 'Block sessions with untrusted issuers' (highlighted with a red box). A note below the checkboxes 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.' To the right of this note, a callout box with a red border contains the text: 'You want to block bad certs even for traffic you aren't decrypting'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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 with a red box), OBJECTS, NETWORK, and DEVICE. The left sidebar includes options like Security, NAT, QoS, Policy Based Forwarding, **Decryption** (highlighted with a red box), Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN.
- Top Right Window:** Titled "Decryption Policy Rule". It has tabs: General, Source, Destination, Service/URL Category (highlighted with a red box), and Options. Under "Service/URL Category", a list shows "service-https" selected (highlighted with a red box). 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, and Options (highlighted with a red box). Under "Action", "Decrypt" is selected (highlighted with a red box). Under "Type", "SSL Forward Proxy" is selected (highlighted with a red box). Under "Decryption Profile", "Decrypt Profile" is selected (highlighted with a red box).

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), Certificate Profiles, OCSP Responder, SSL/TLS Service Prc, SCEP, SSL Decryption Exc, SSH Service Profile, Response Pages, Log Settings, Server Profiles (with SNMP Trap, Syslog, Email, HTTP, and Mailflow selected), and Network.

The main content area displays "Device Certificates | Default Trusted Certificate Authorities". A table lists certificates:

NAME	SUBJECT	ISSUER
Forward-Trust	CN = 203.0.113.50	CN = 203.0.113.50
Forward-untrust	CN = forward-untrust	CN = forward-untrust
commerce-server	/C-US/ST=FL/O=nccdc/OU=panw	/C-US/ST=FL/O=nccdc/OU=panw

A modal dialog titled "Import Certificate" is open. It has the following fields:

- Certificate Type: Local (radio button selected)
- Certificate Name: commerce-server (highlighted with a red box)
- Certificate File: C:\fakepath\certificate.pem (highlighted with a red box)
- File Format: Base64 Encoded Certificate (PEM)
- Checkboxes:
 - Private key resides on Hardware Security Module
 - Import Private Key (selected)
 - Block Private Key Export
- Key File: C:\fakepath\privatekey.pem (highlighted with a red box)
- Passphrase: *****
- Confirm Passphrase: *****

At the bottom are OK and Cancel buttons.

Configure Inbound Decryption for Your DMZ Server

The screenshot displays the Palo Alto Networks Management Console interface. The top navigation bar includes 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 'Description' field is empty. The 'Audit Comment' field contains the placeholder 'Audit Comment Archive'. At the bottom right of the modal are 'OK' and 'Cancel' buttons.

The right side of the screen shows a detailed view of the 'Inbound-decryption' policy rule configuration. The 'Options' tab is selected. The 'Action' section has 'Decrypt' selected (radio button checked). The 'Type' is set to '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 Unsuccessful SSL Handshake' checkbox is checked. The 'Log Forwarding' dropdown is set to 'None'. At the bottom right 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

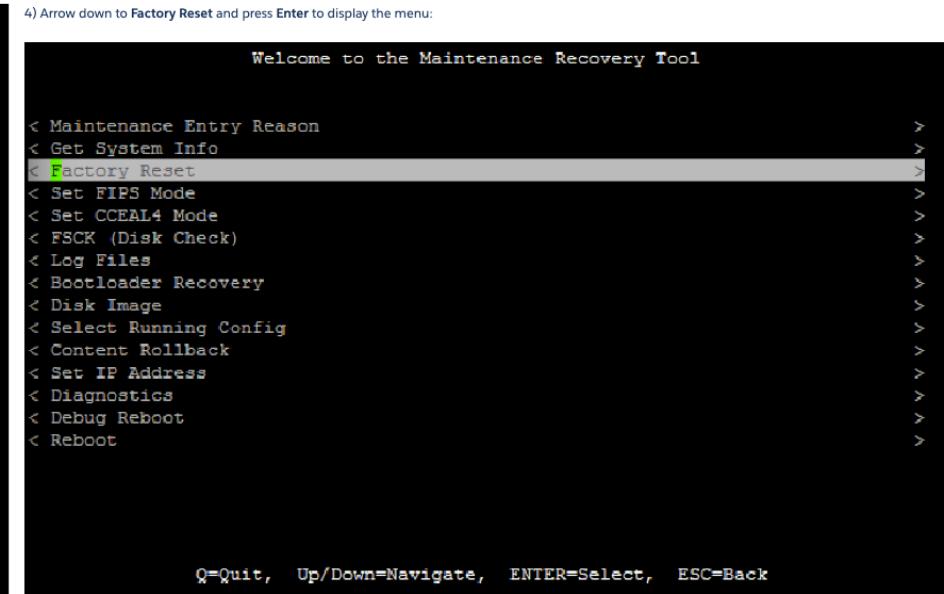
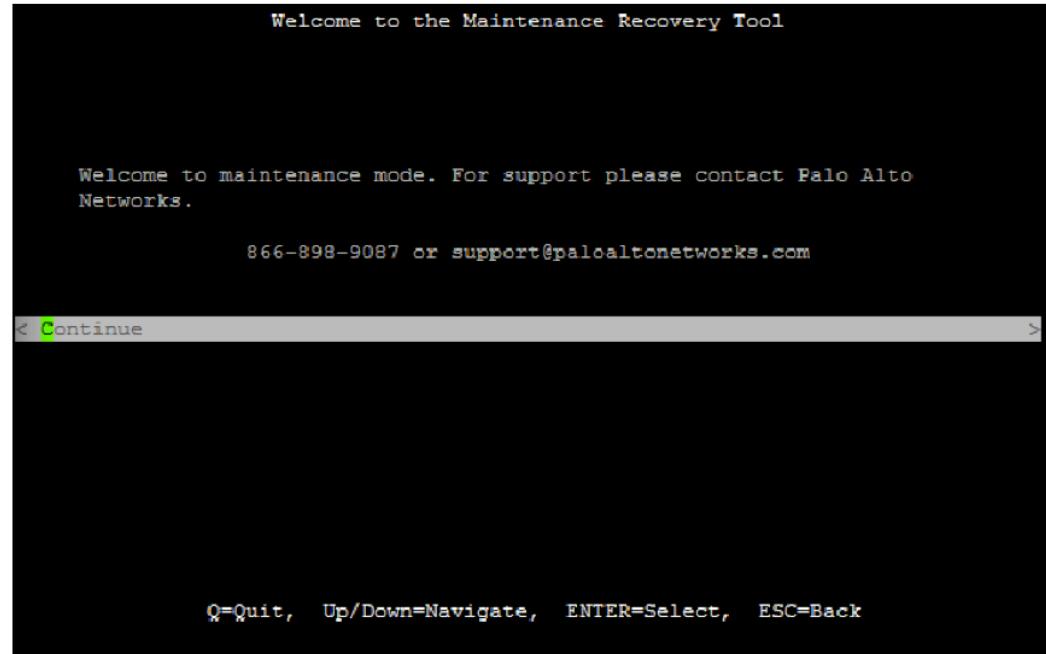
URL Article for hardware appliances:

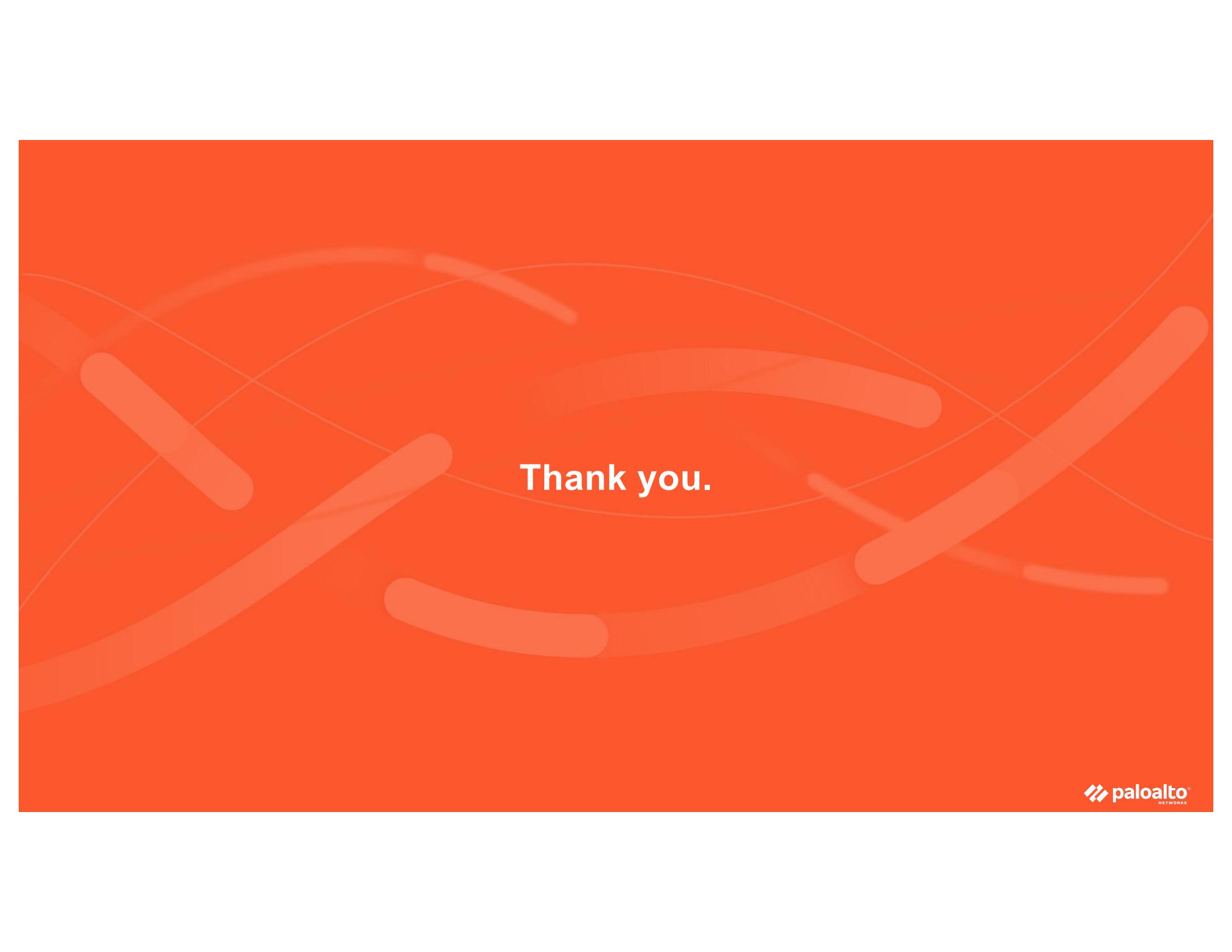
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldXCAS>

Youtube video for Virtual Appliance: https://www.youtube.com/watch?v=47H_sSjMMJw

- 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

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





Thank you.