CCDC Quick Start Guide for NGFW Deployment and Configuration

Jim Boardman – Cybersecurity Academy
Tom Trevethan – Cybersecurity Academy

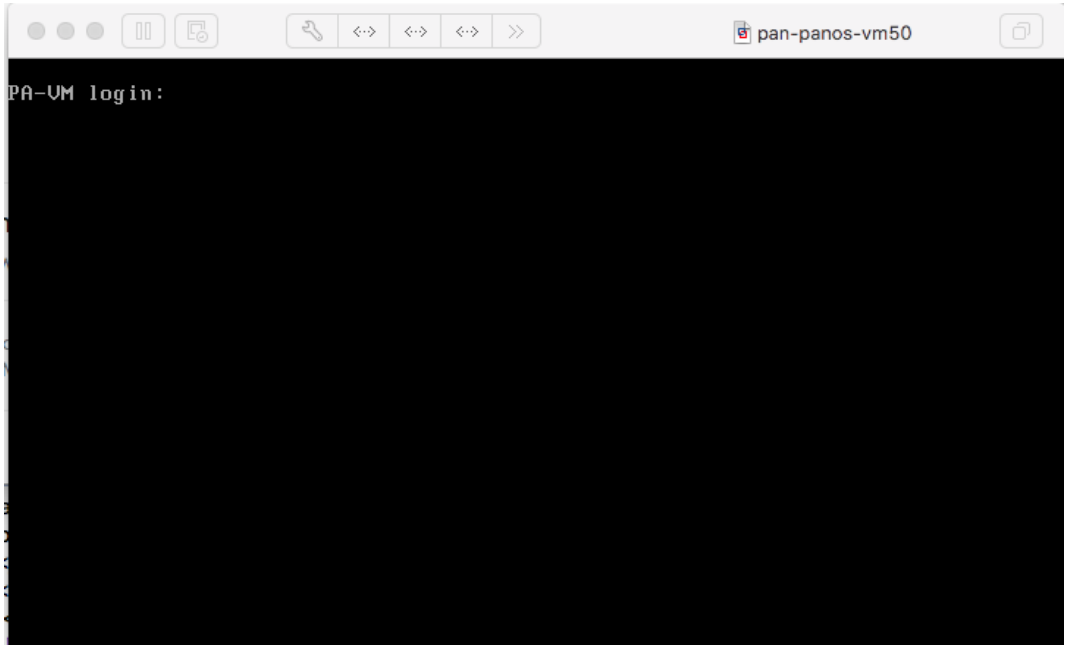
Quick Start - Critical Steps to Secure and Deploy the Firewall Appliance in order to Protect the Network

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

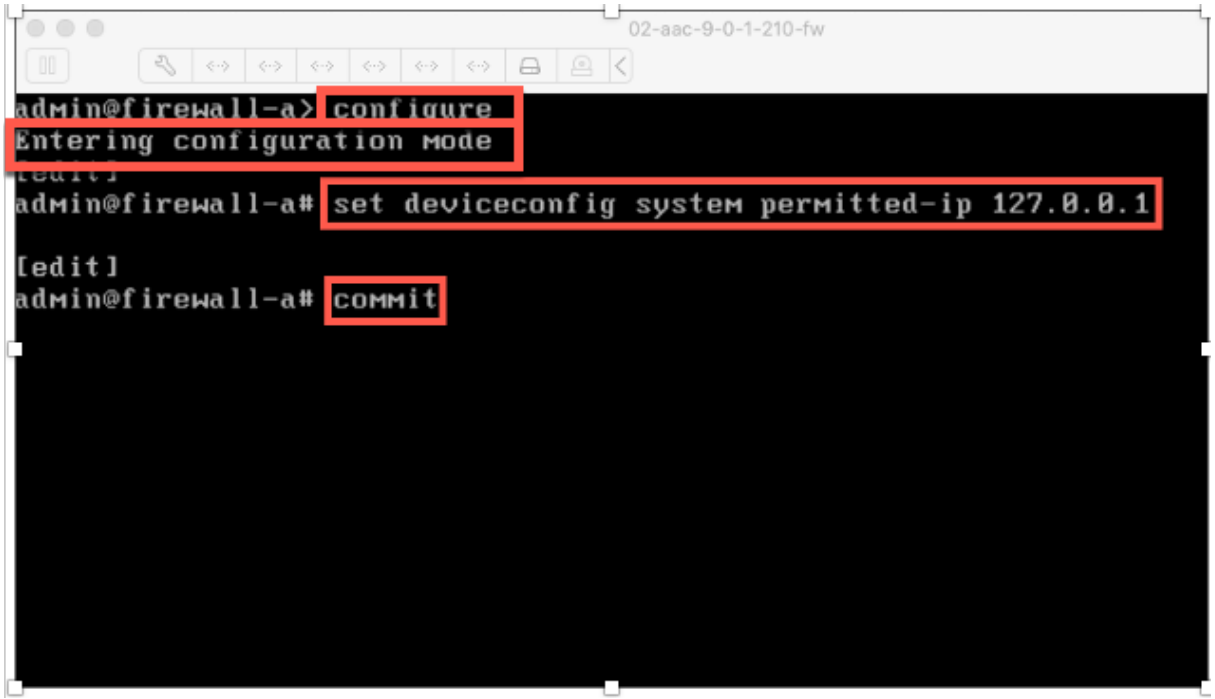
- Hypervisor Console Port
  - Default UN: admin
  - Default PWD: admin



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

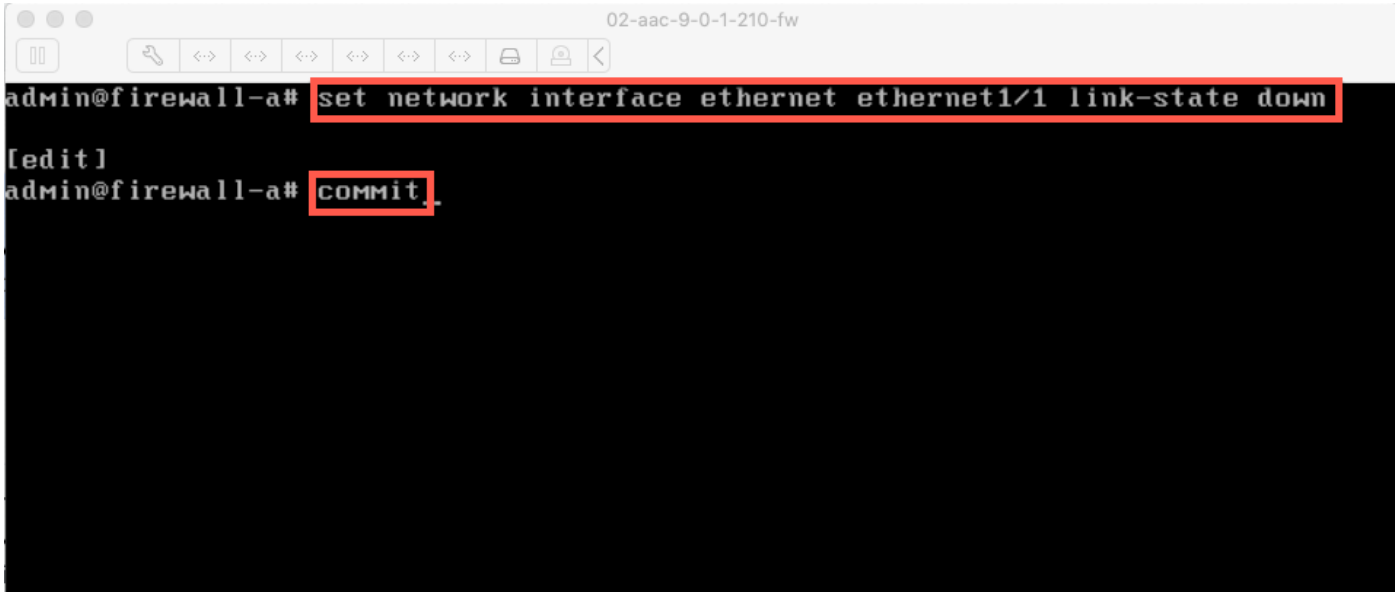
- Configure Mode **#set deviceconfig system permitted-ip 127.0.0.1**

#Commit



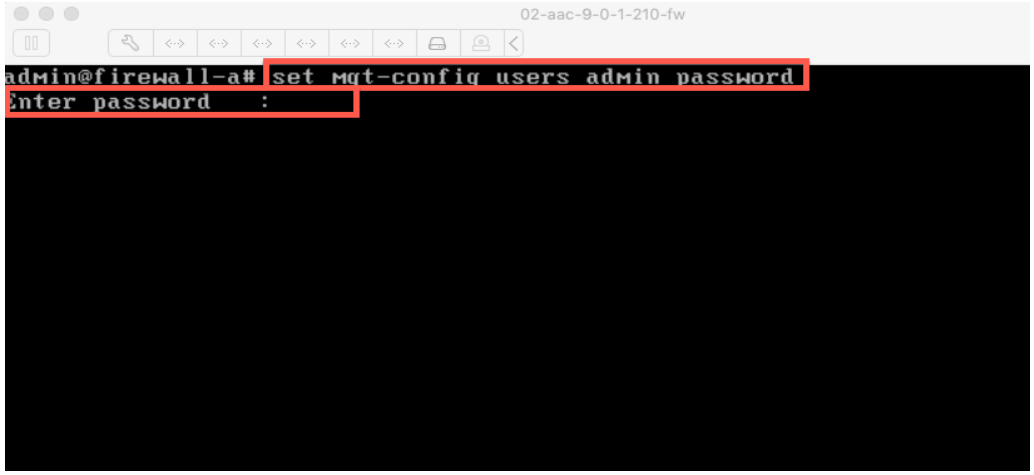
Securing the Virtual FW Appliance: Turn Off Data External Interface Temporarily if connected – Red Team Could Be Managing FW Via Data Interface

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



Securing the Virtual FW Appliance: Change the Admin Password

- Change default admin password
  - Operations Mode > **configure**
  - Configure Mode # **set mgt-confg 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

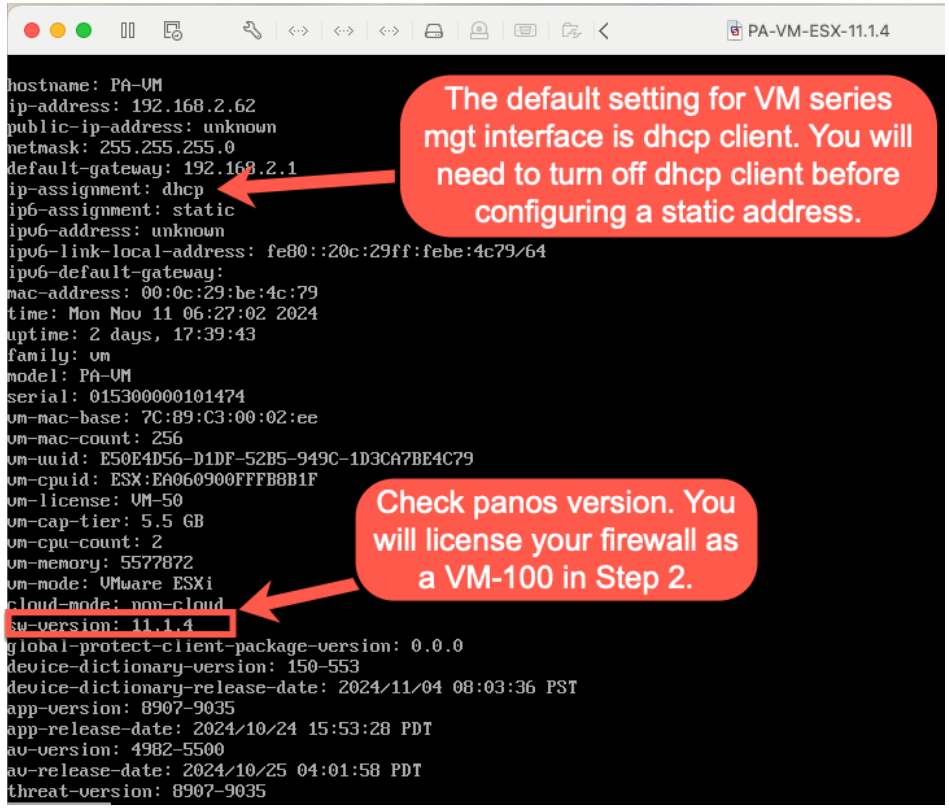


Securing the Virtual FW Appliance: Review System Info

- 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
```



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

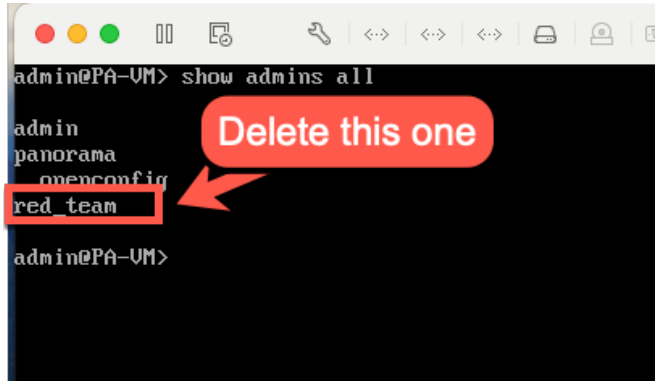
- Secure the FW management interface for allowed services
  - Only allow secure services: ssh, https, ping (for troubleshooting)
  - Configure mode: **#set deviceconfig system service disable-https no**
    #commit

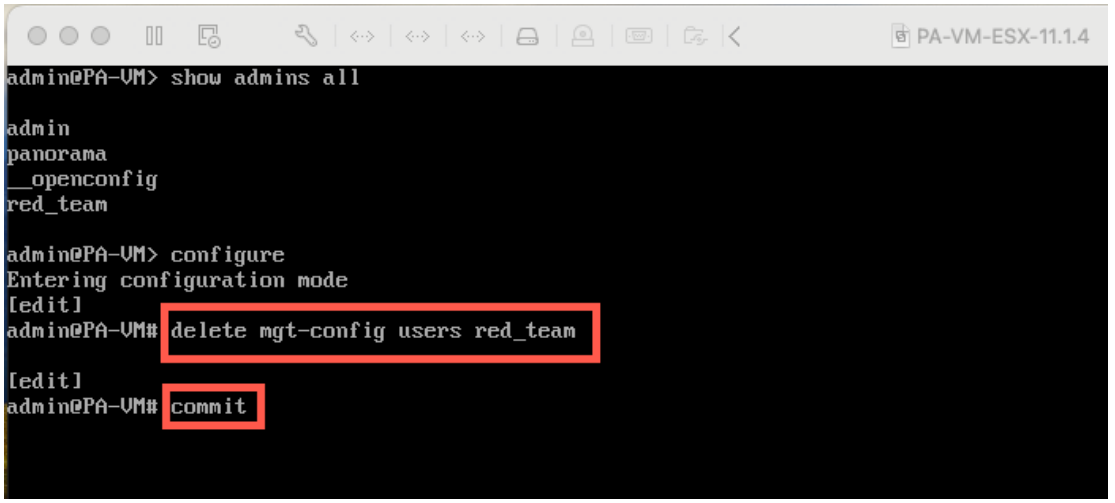
```
admin@PA-VM> show system services

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

```
admin@PA-VM> configure
Entering configuration mode
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

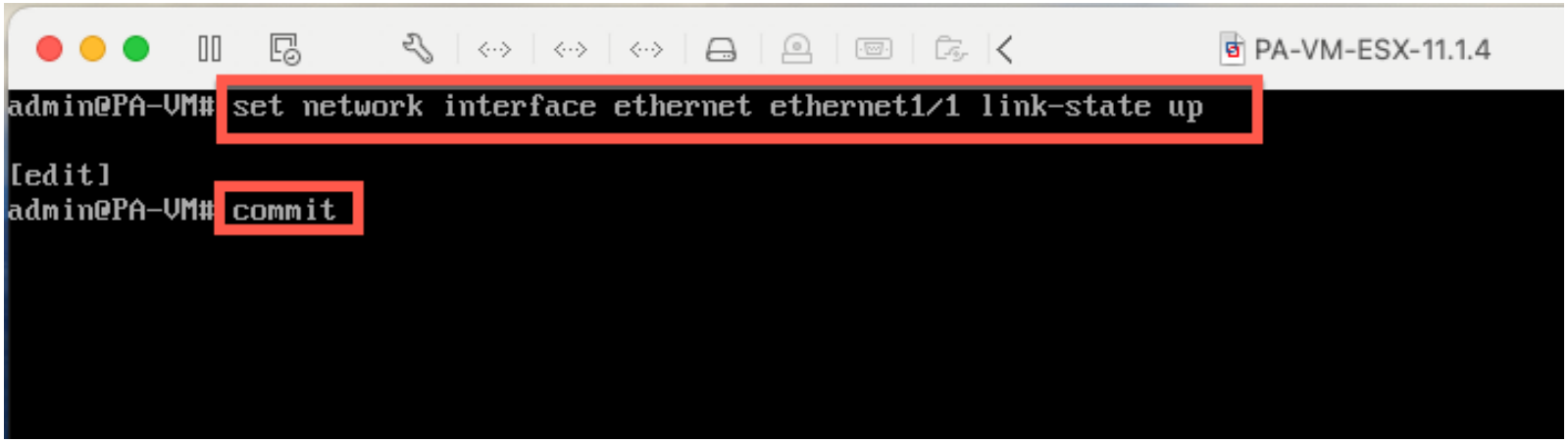
- Make sure there are only two admin accounts unless directed otherwise: (admin and panorama - - default configuration)
  - > **show admins all**
  - # **delete mgt-config users redteam and # commit**





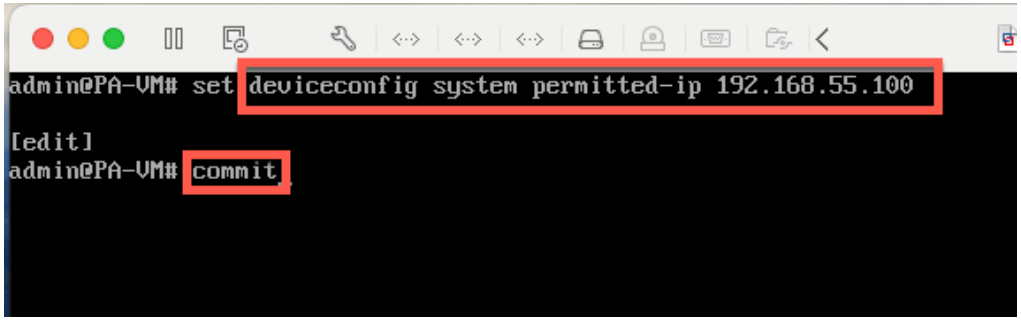
Secure FW Appliance: Turn Data Interfaces Back On If Turned Off

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

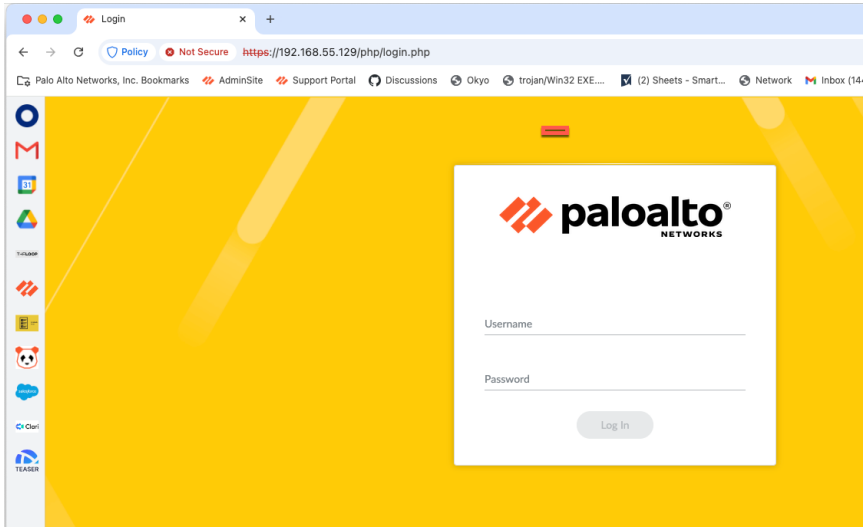


Securing the FW Appliance: Turn Management Interface Back On

- Only allow management Interface access from your team's computer
  - Configuration Mode# **set deviceconfig system permitted-ip x.x.x.x**

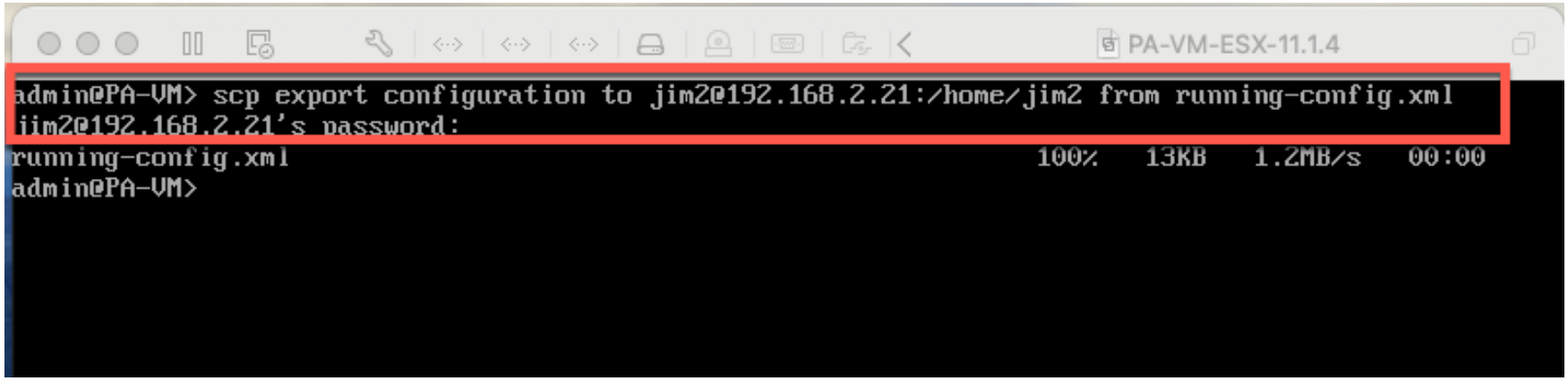


- Manage your FW appliance via mgt interface Web-UI



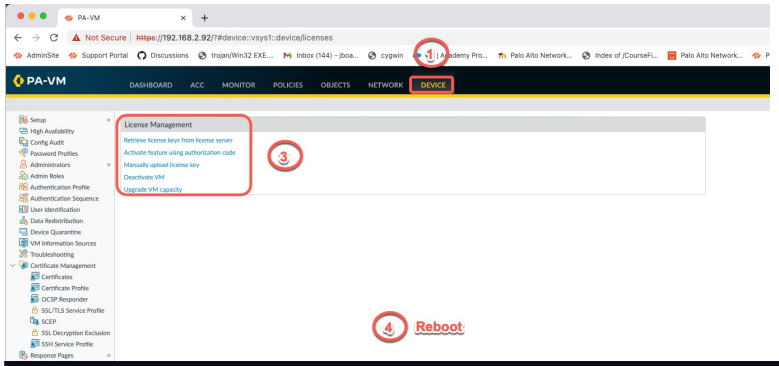
Securing the FW: Back Up Your FW Config and/or Take Snapshot of Virtual Firewall Appliance

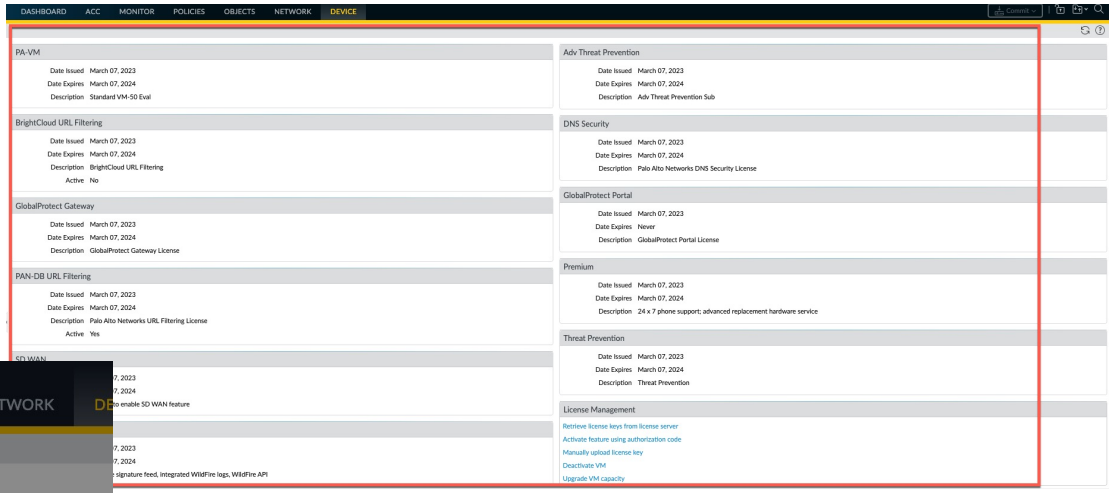
- Operations Mode >**scp export configuration to username@host:/home/secops from running-config.xml**

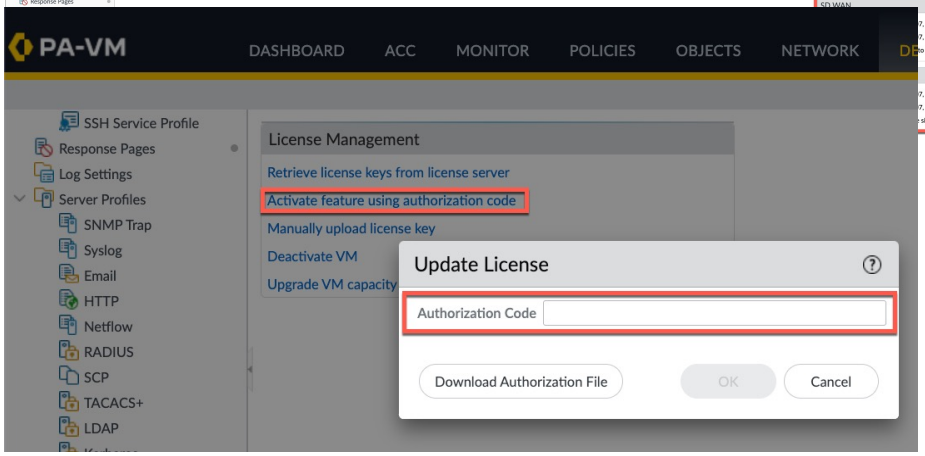


Step 2:
License the firewall appliance

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

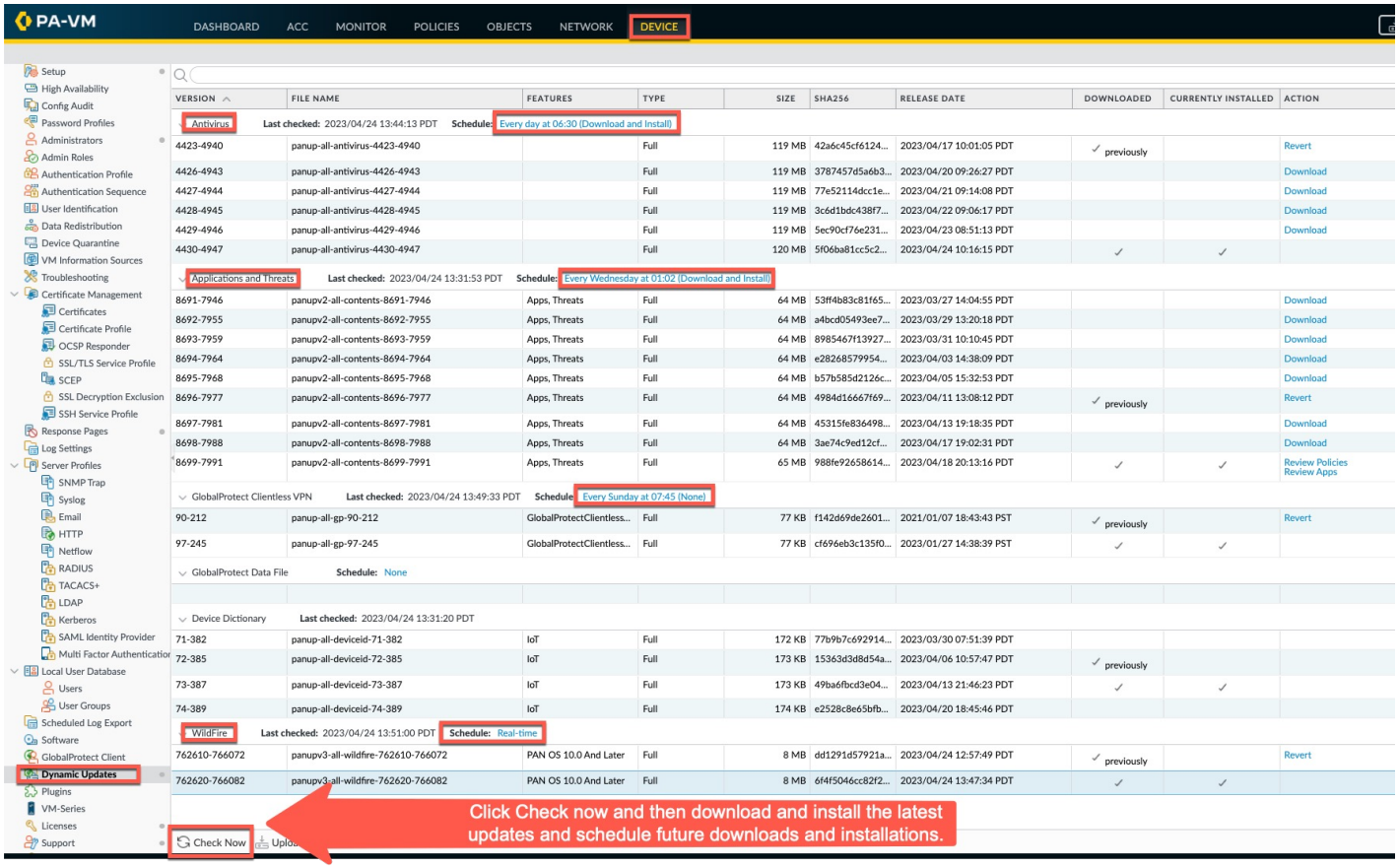






Step 3:
Download the latest malware signatures for the firewall appliance

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



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

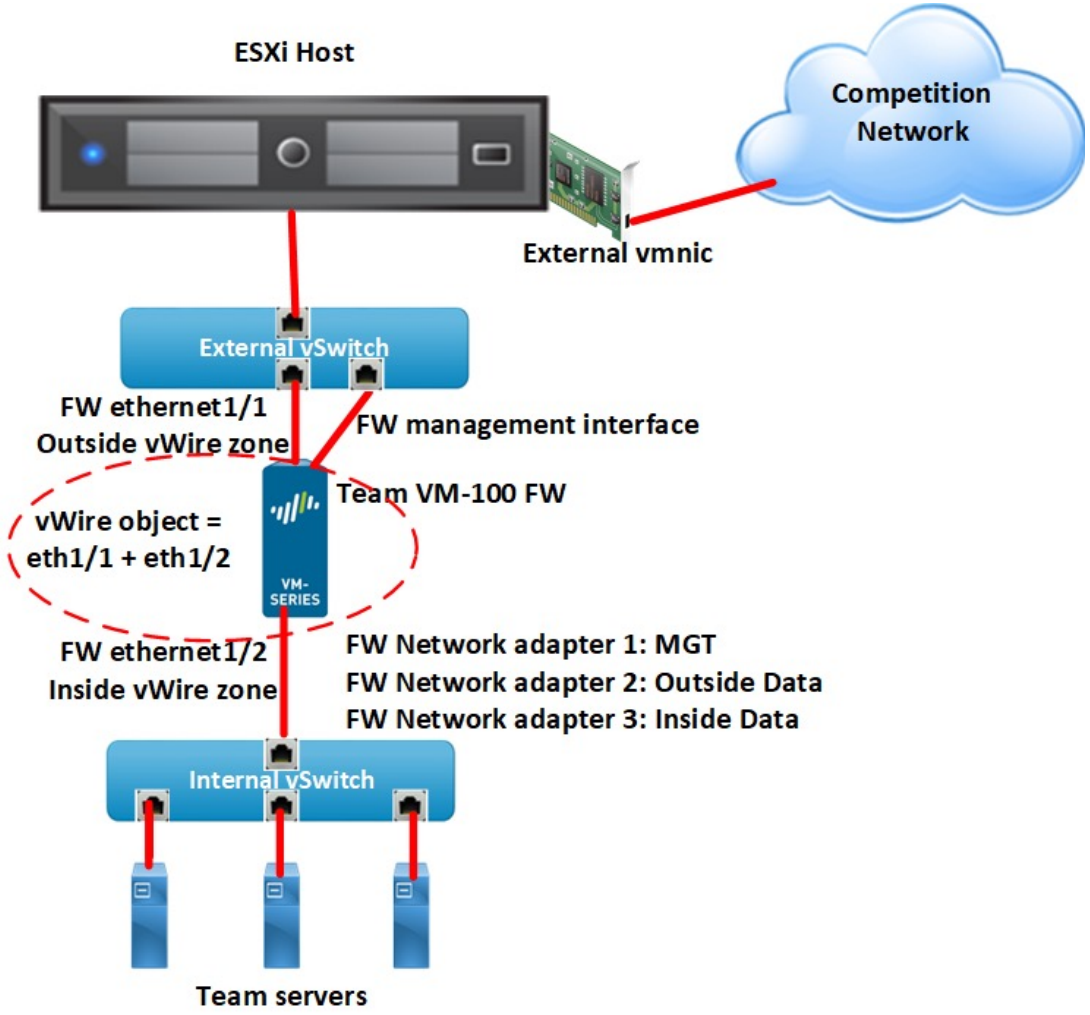
3 Network Deployment Options:

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



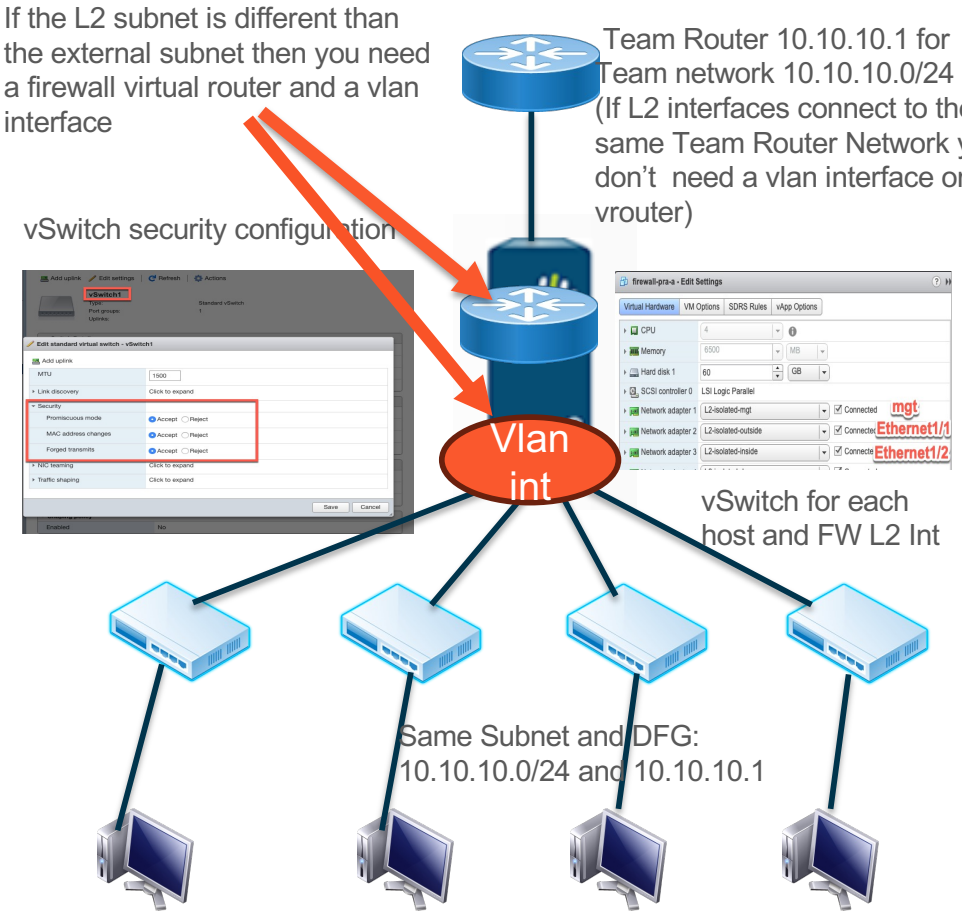
Network Deployment (Option 1): Vwire Security Policies

- 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



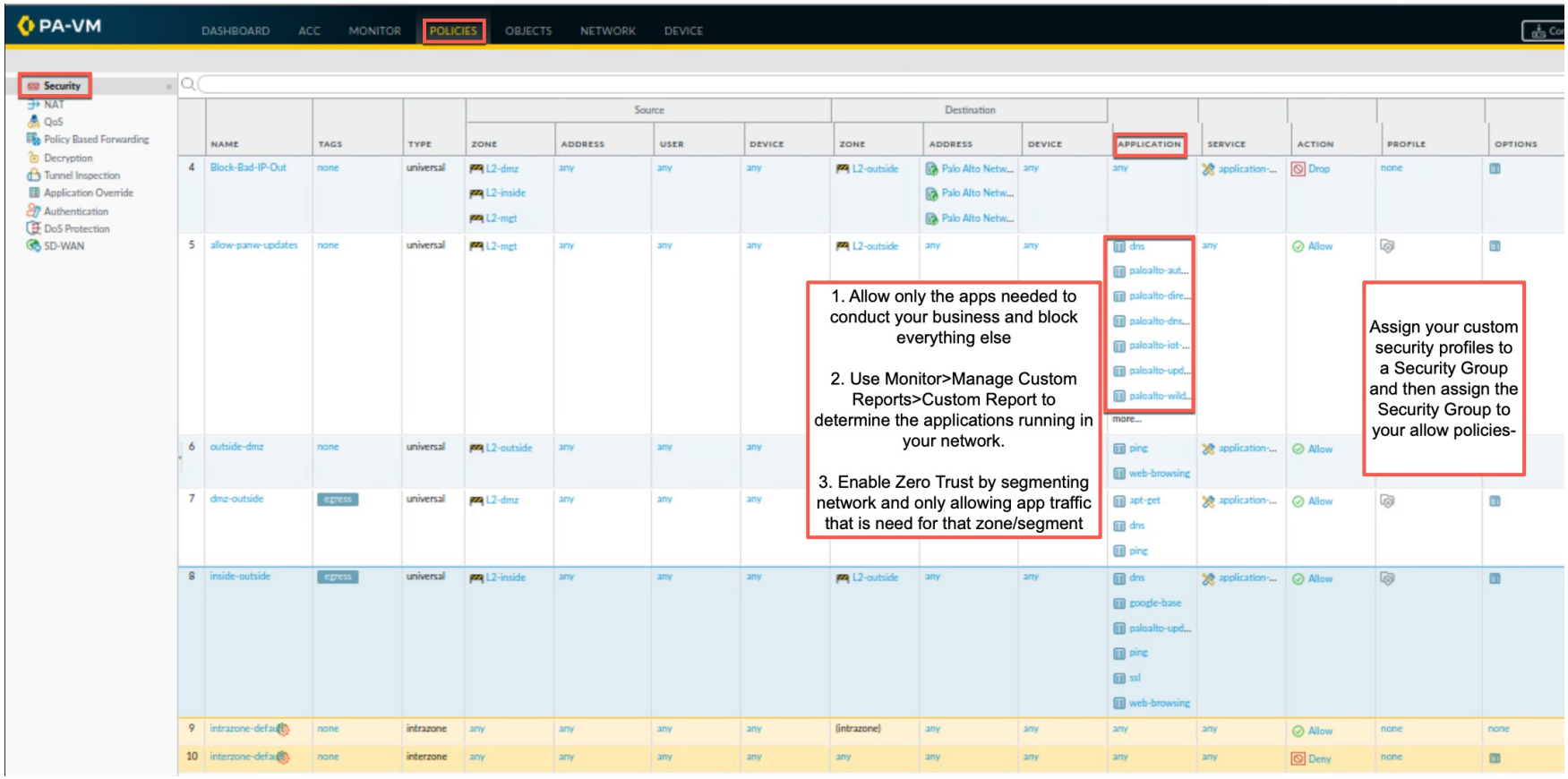
L2 Configuration Steps

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

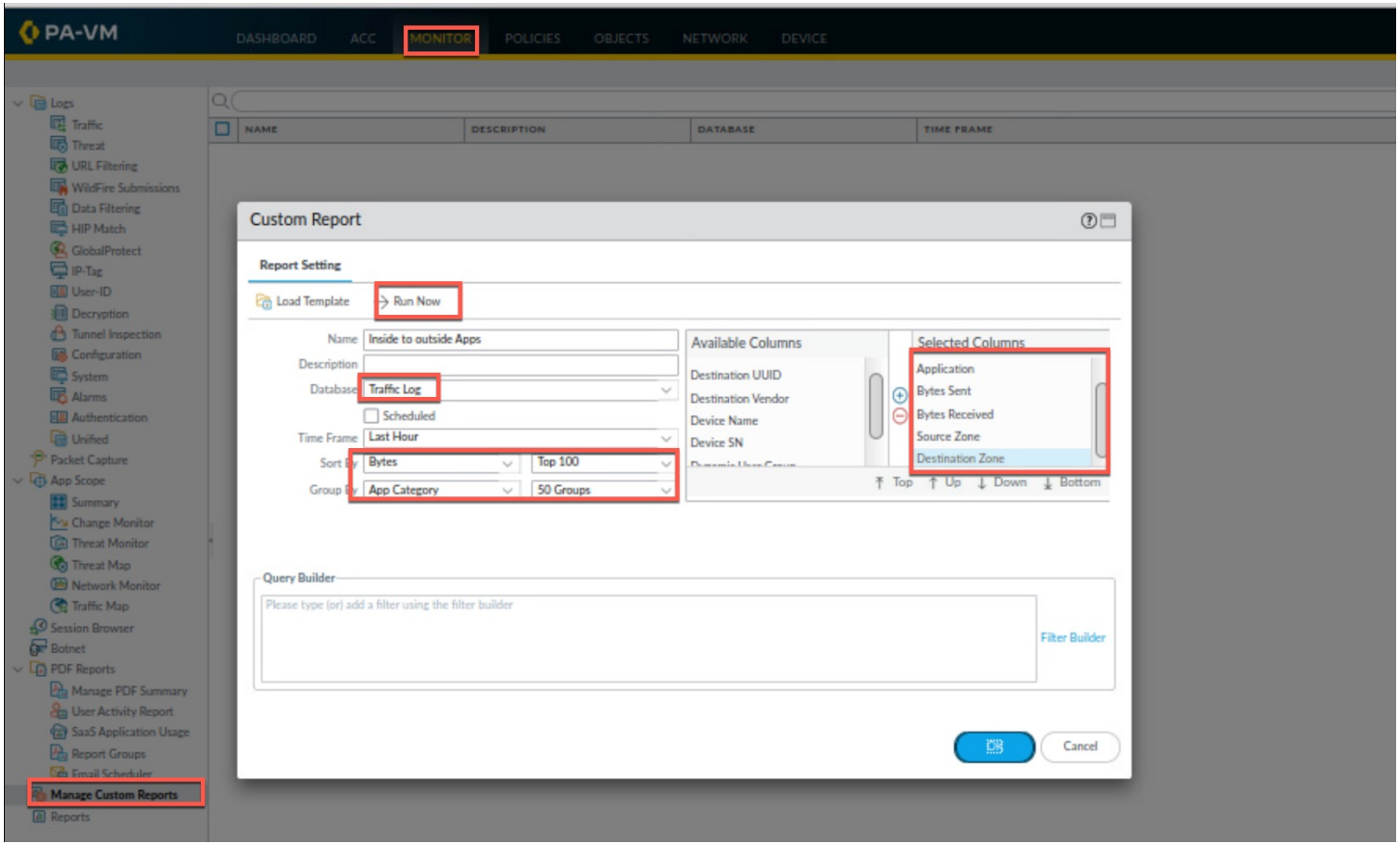
Network Deployment L2 (Option 2): Security Policies

- 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

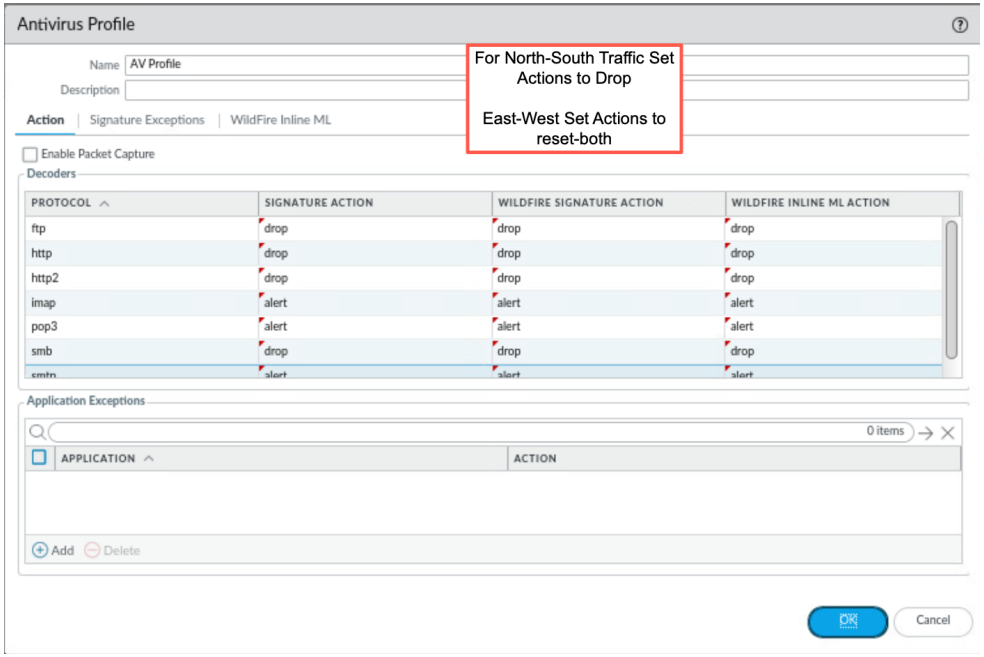
Network Deployment L2 (Option 2): Security Policies

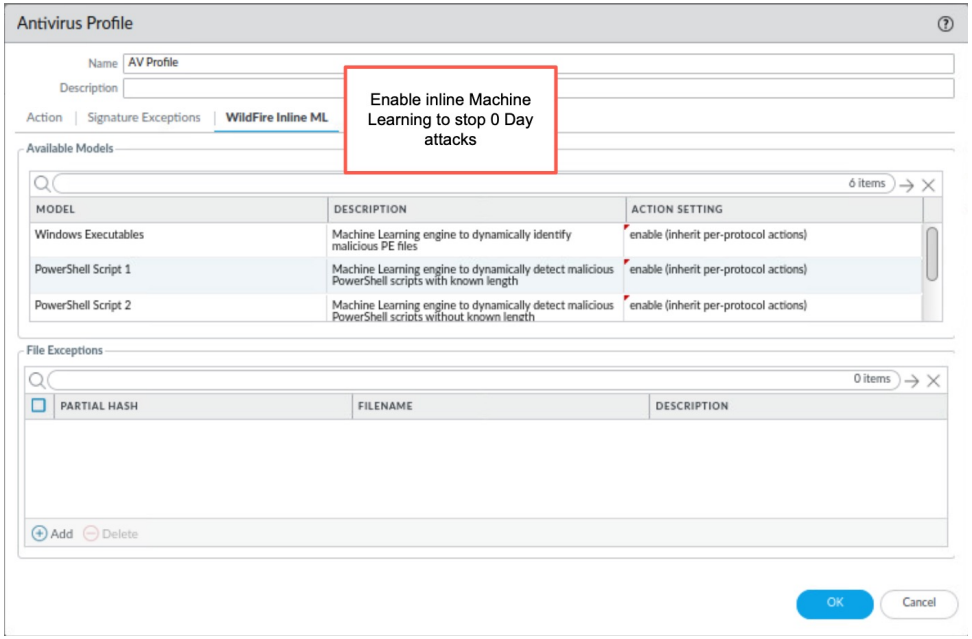


Use Custom Reports to Determine What Apps Are in Your Network

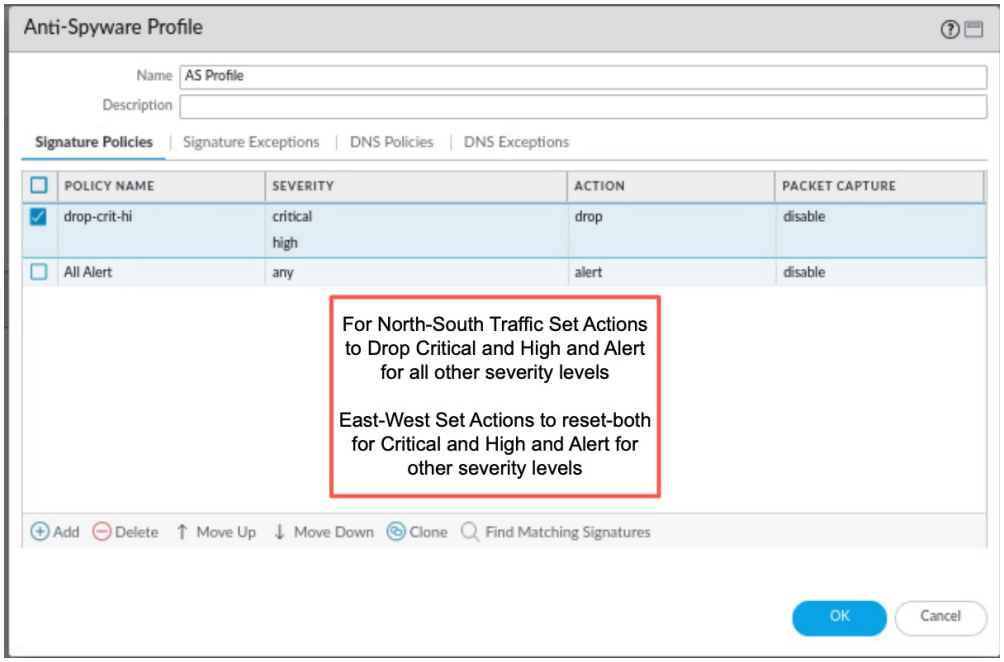


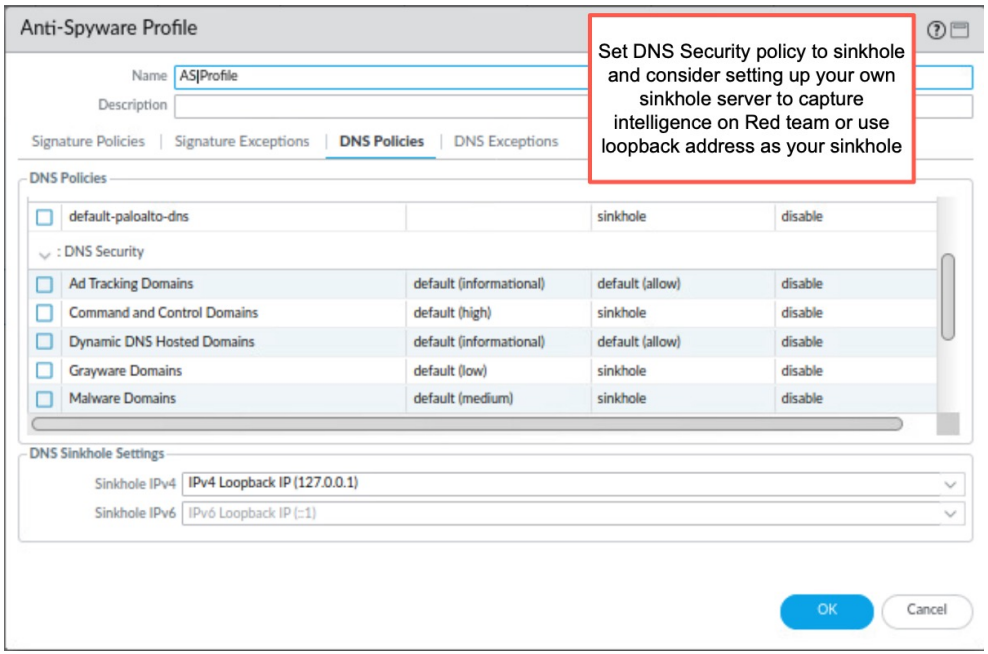
Custom Security Profile: Anti Virus



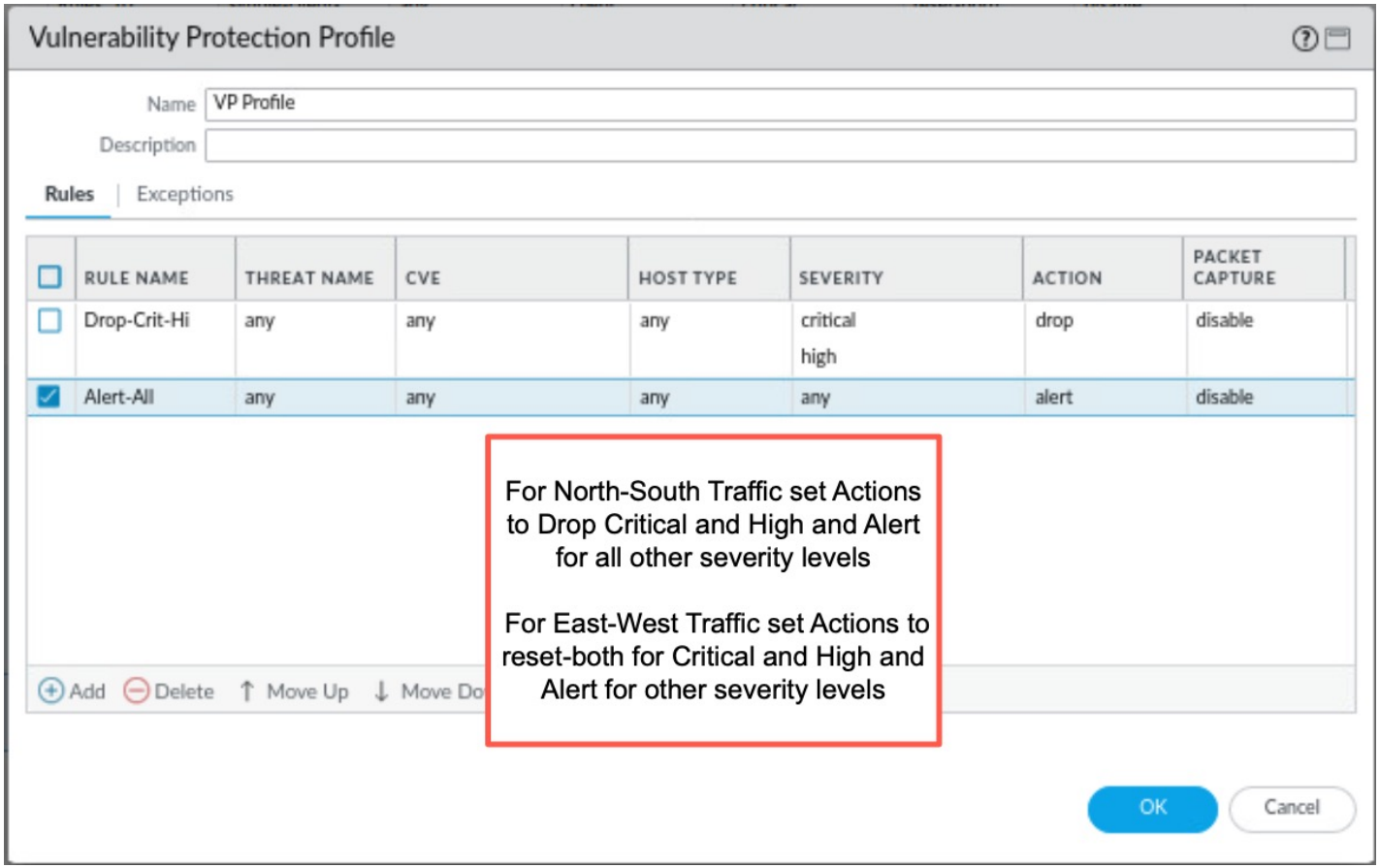


Custom Security Profile: Anti Spyware

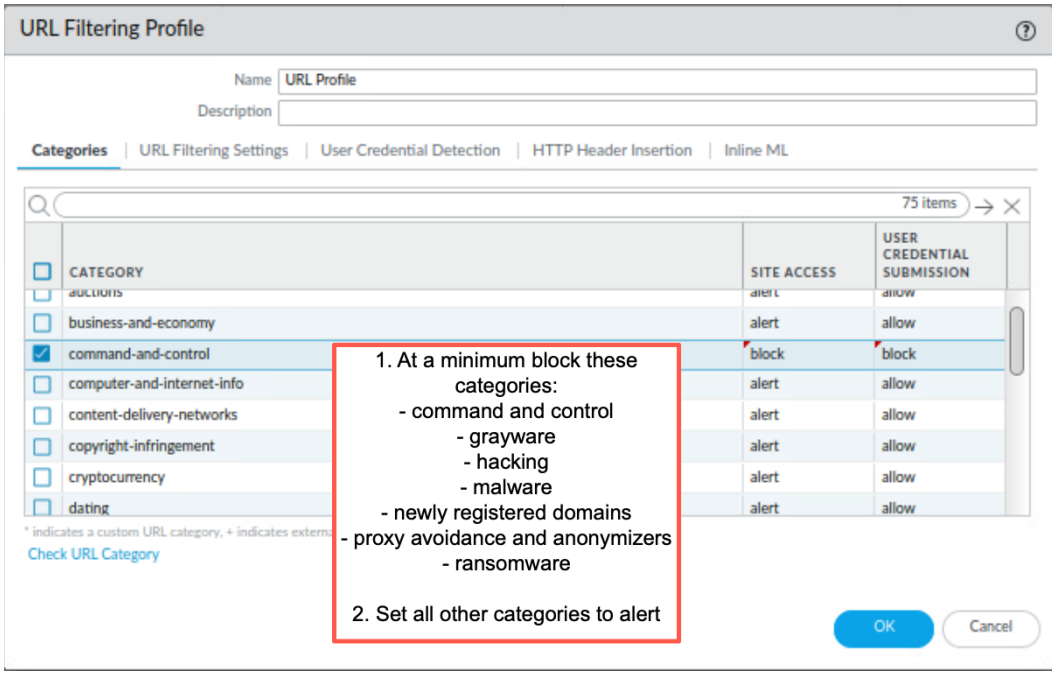


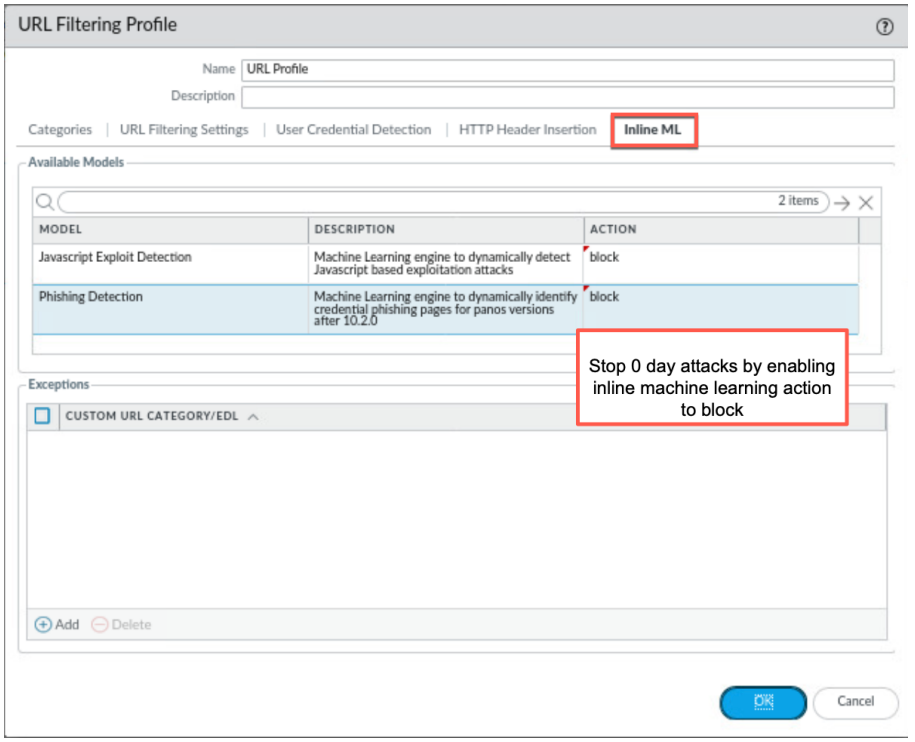


Custom Security Profile: Vulnerability Protection

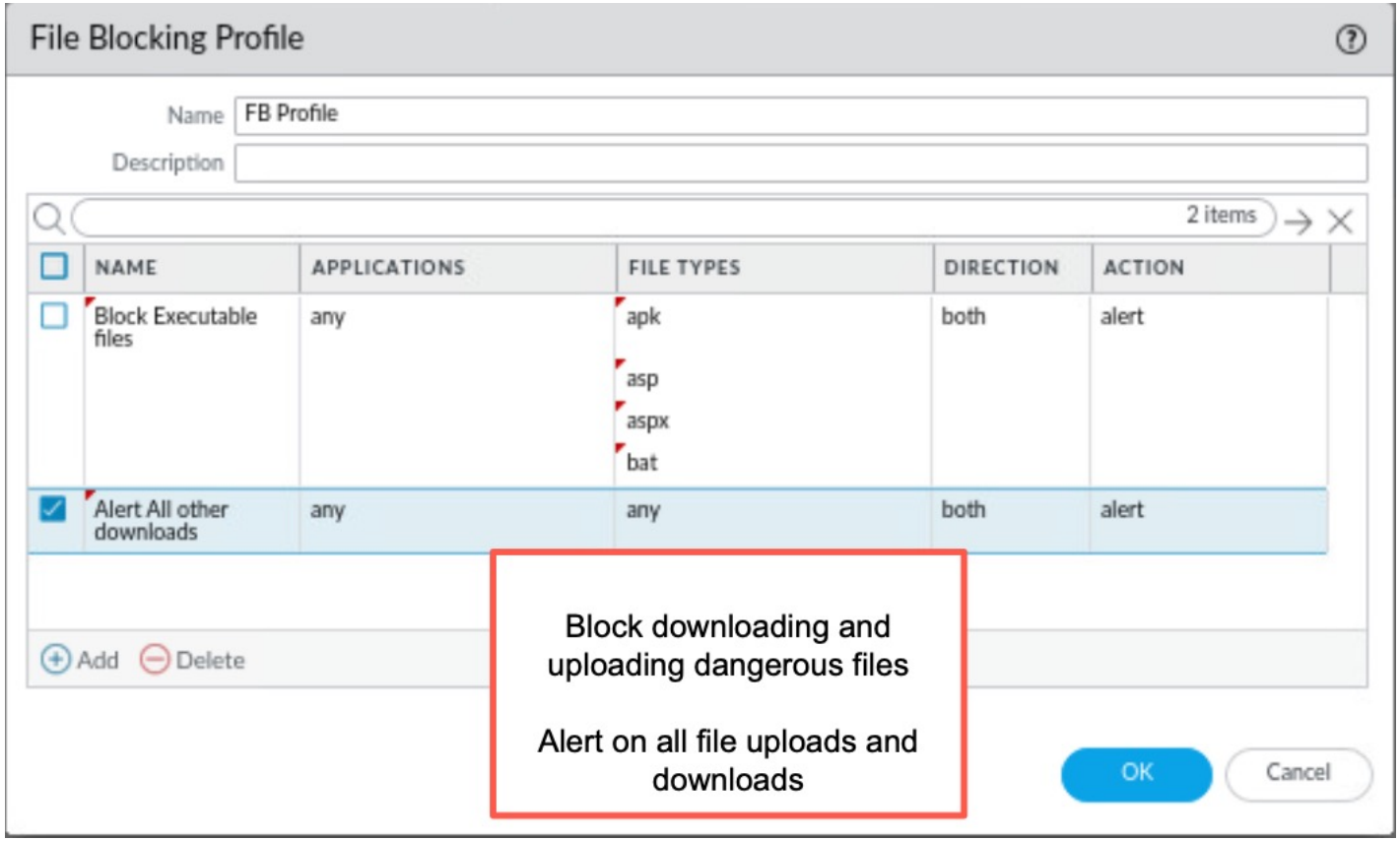


Custom Security Profile: URL Filtering

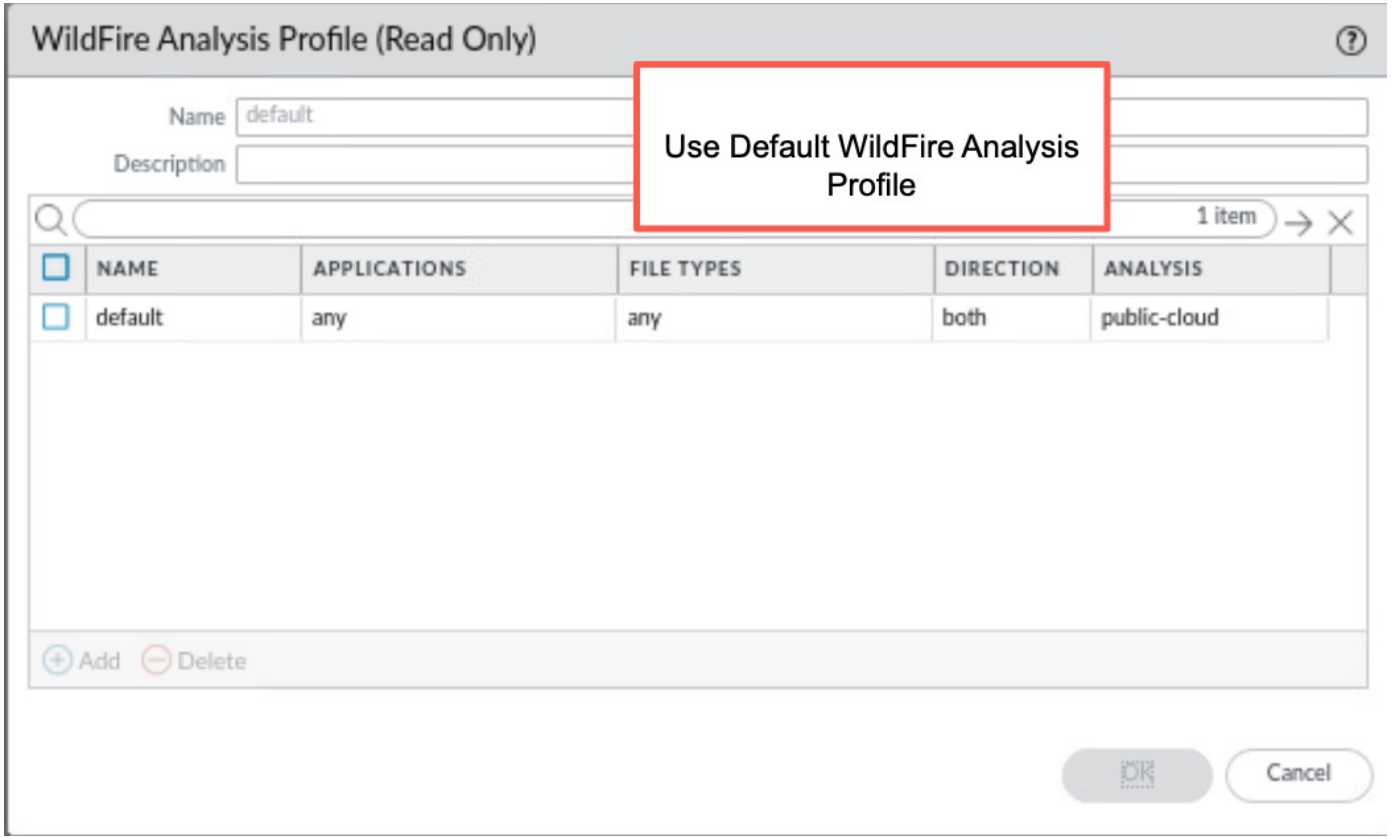




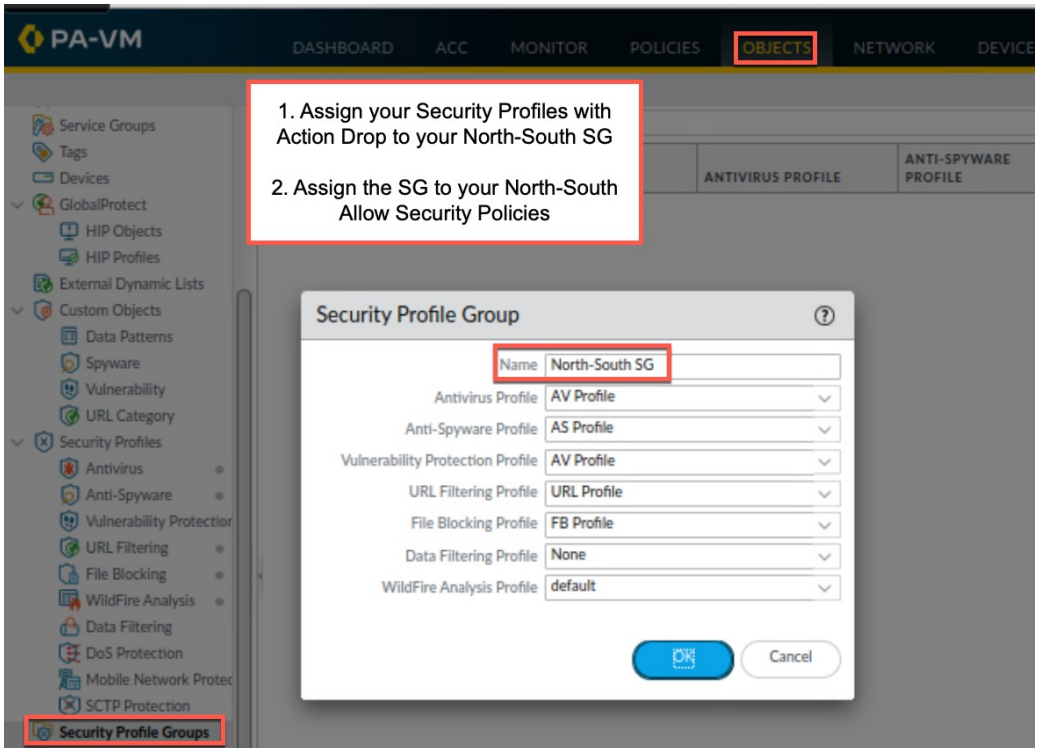
Custom Security Profile: File Blocking

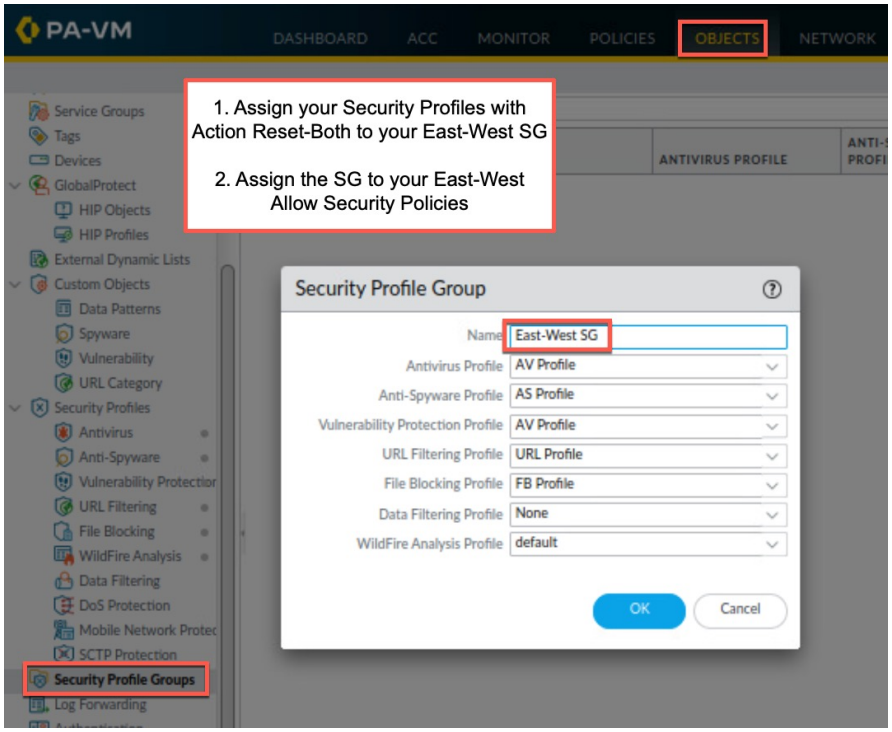


Custom Security Profile: WildFire Analysis



Custom Security Groups

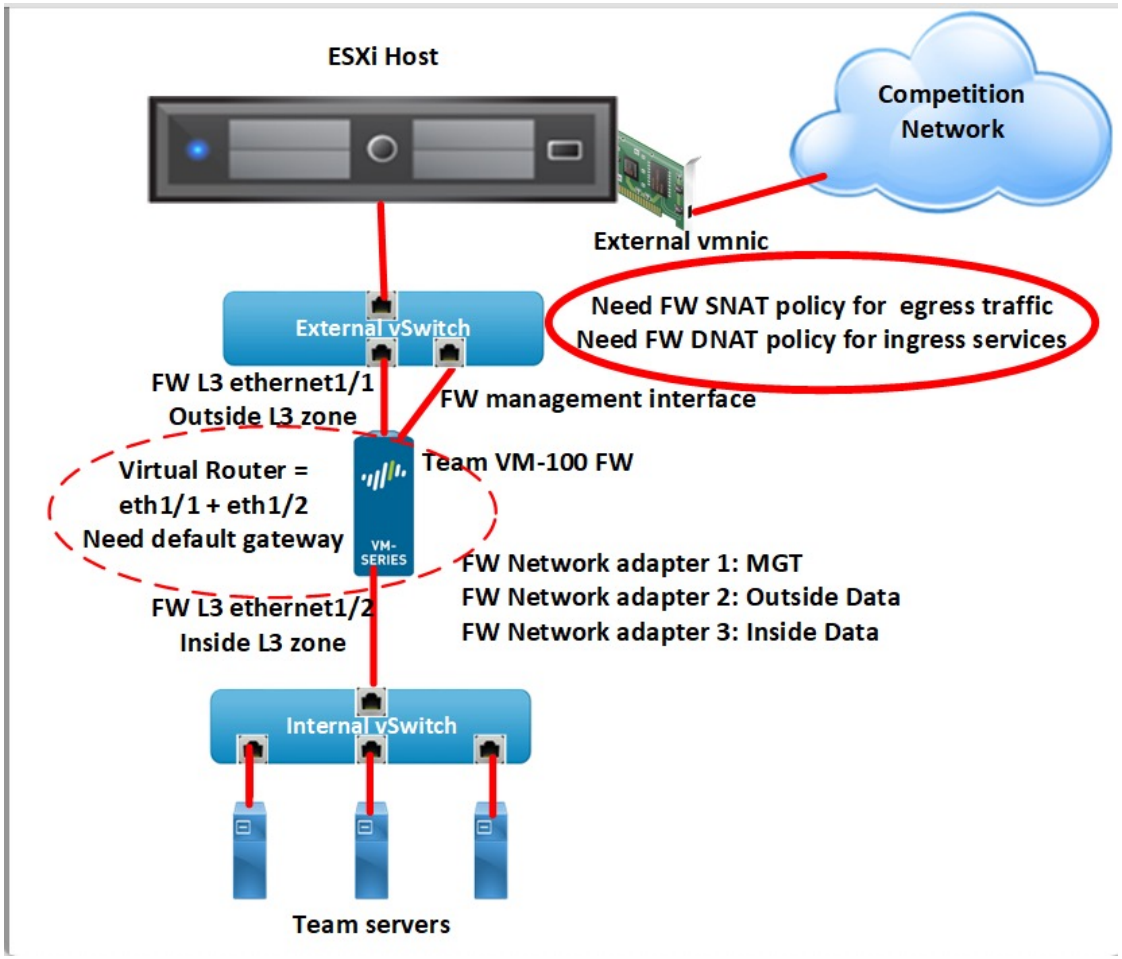




Network Deployment Option 3: Layer 3 (L3)

- **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

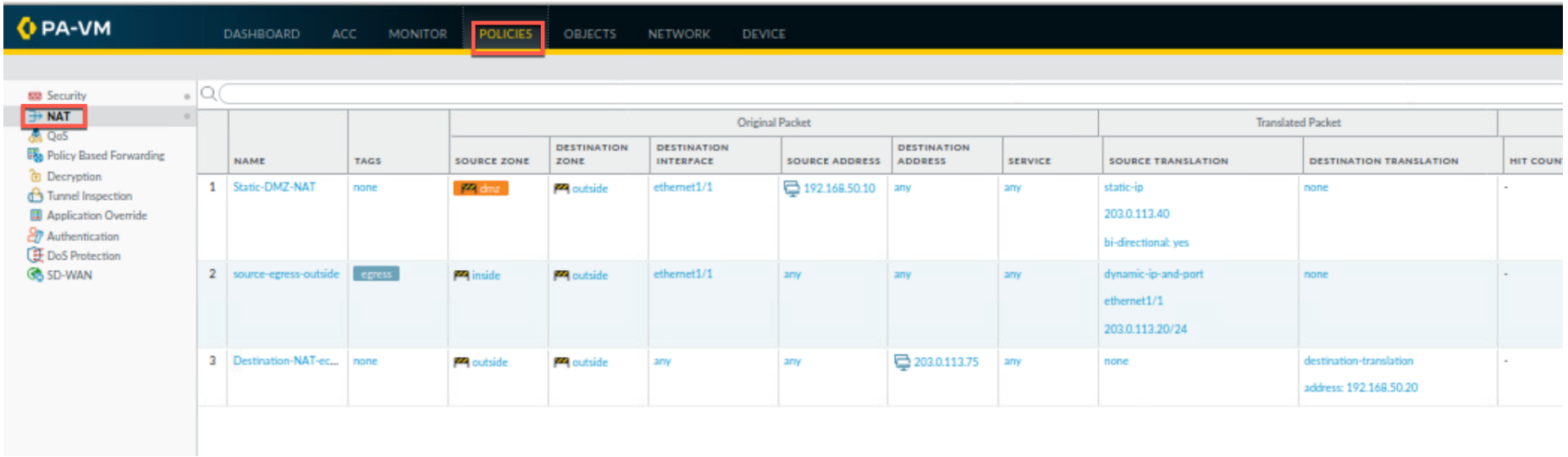
Network Deployment L3 (Option 3): Network Architecture



Network Deployment L3 (Option 3): Security Policies

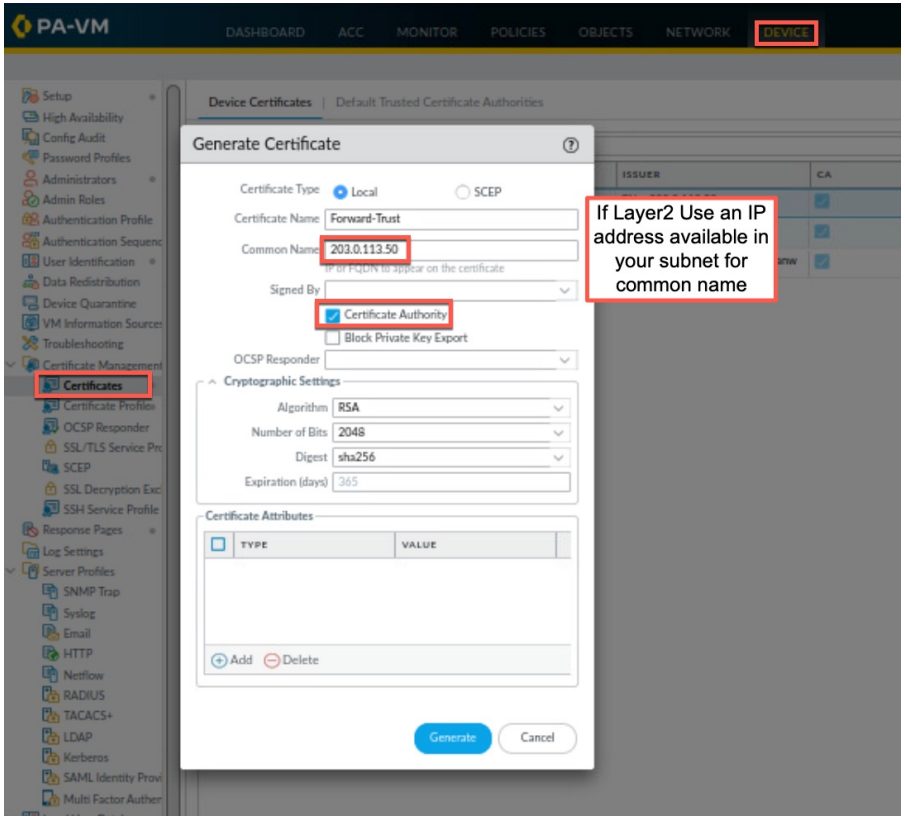
- Configure an inbound and outbound block rule to block unknown and bad urls
- Configure inbound allow rule(s) corresponding to your DNAT policy(ies) for scored services
  - Make rules as specific as possible by using allowed applications and destination IP addresses
- Configure East-West rule(s) for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

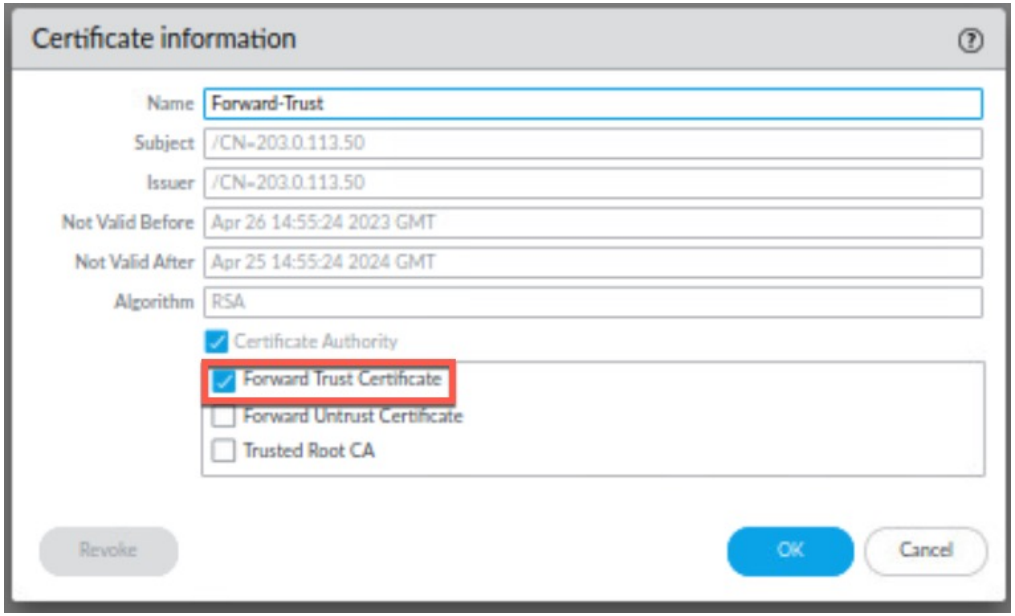
Network Deployment L3 (Option 3): NAT Policies



Step 5: Turn on Decryption

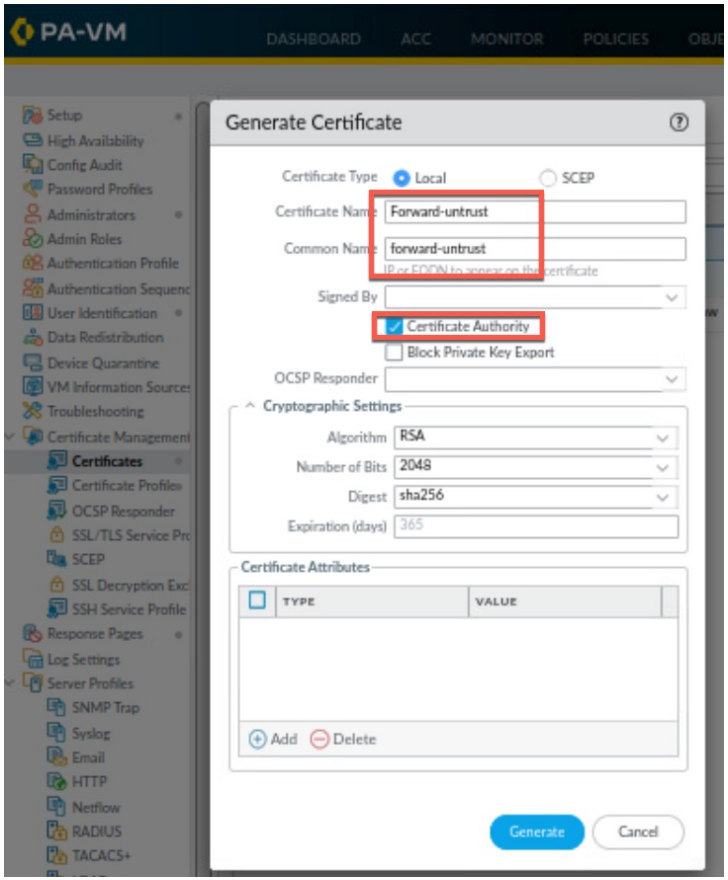
Forward Trust Decryption for Outbound traffic: Create Trust Certificate

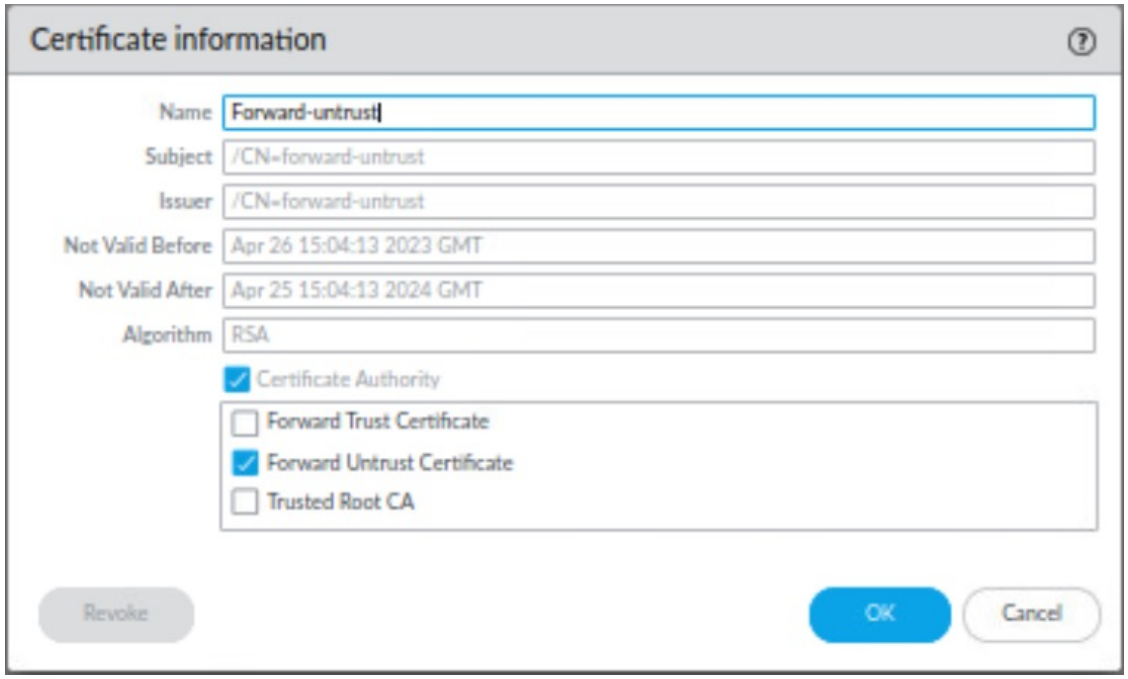




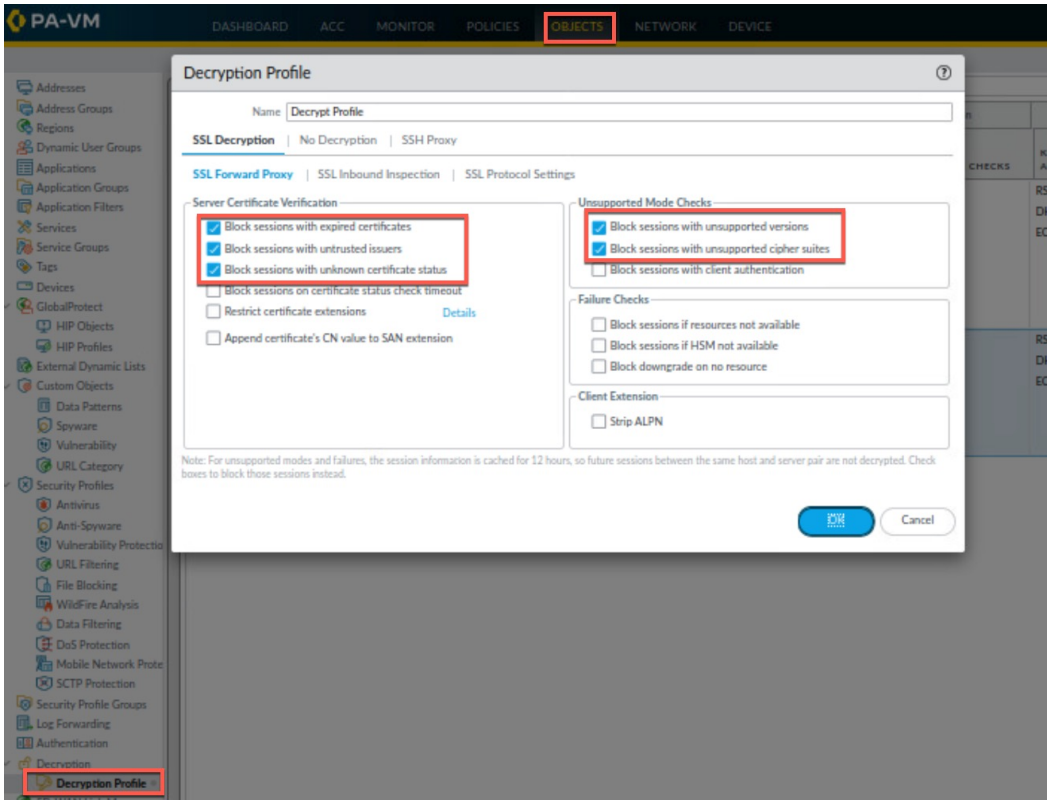
 |

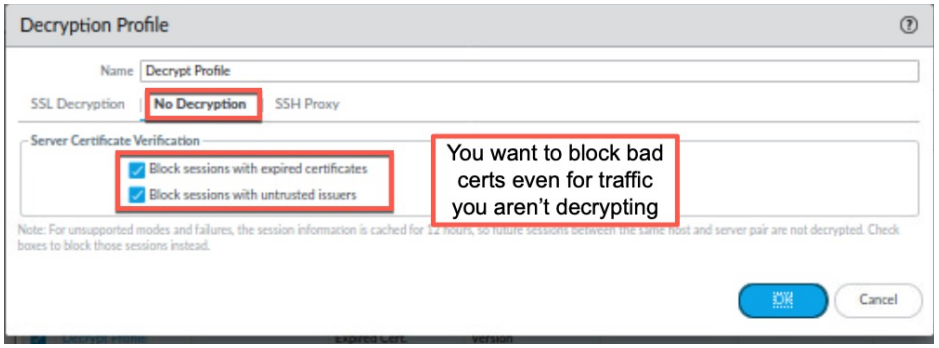
Forward Trust Decryption for Outbound traffic: Create Untrust Certificate



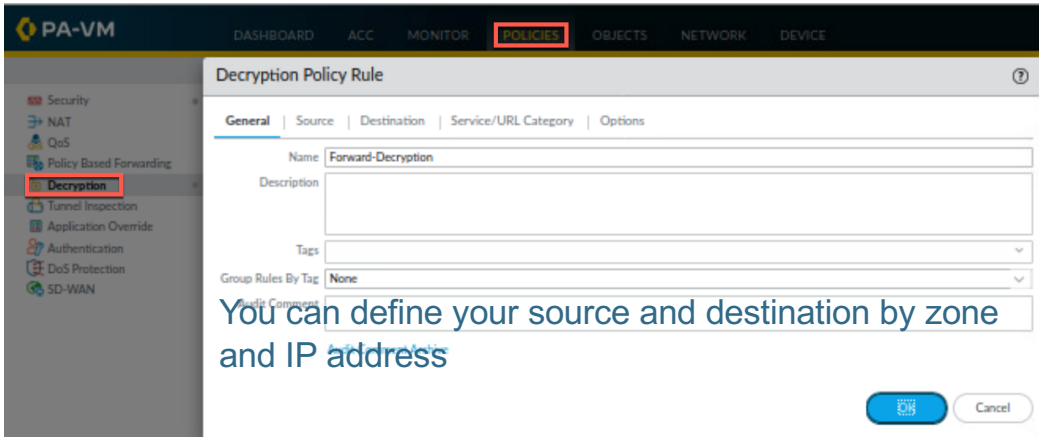


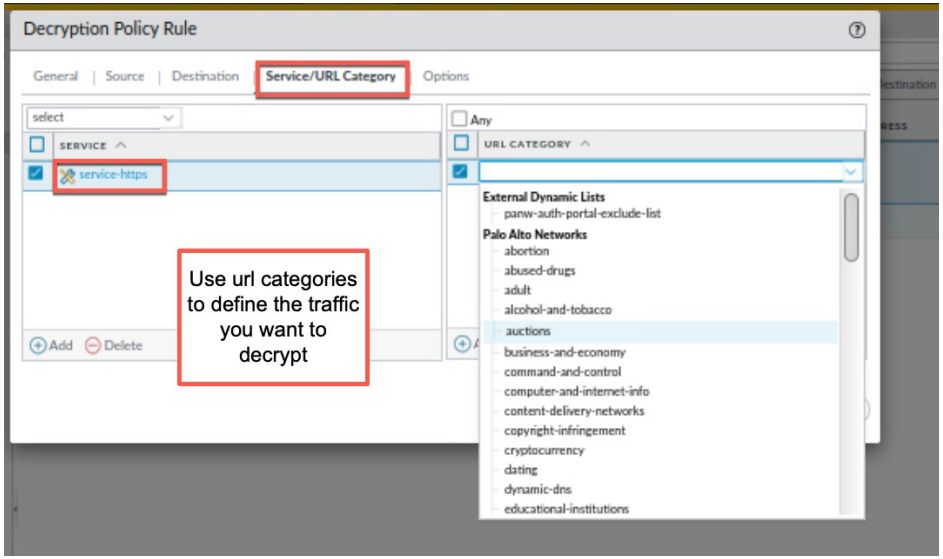
Configure Decryption Profile

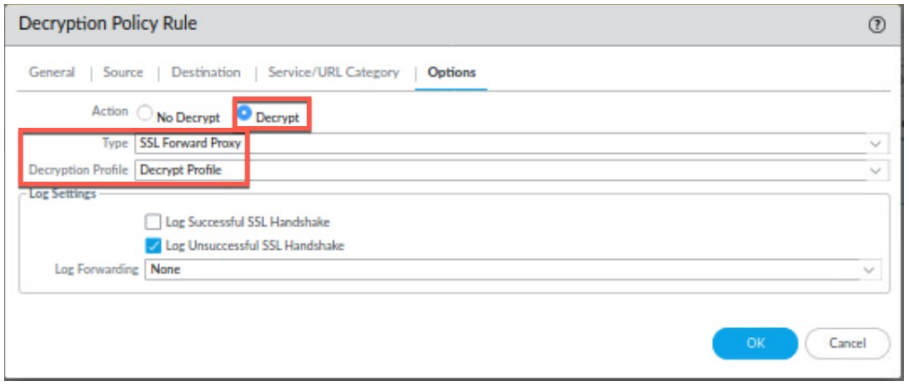




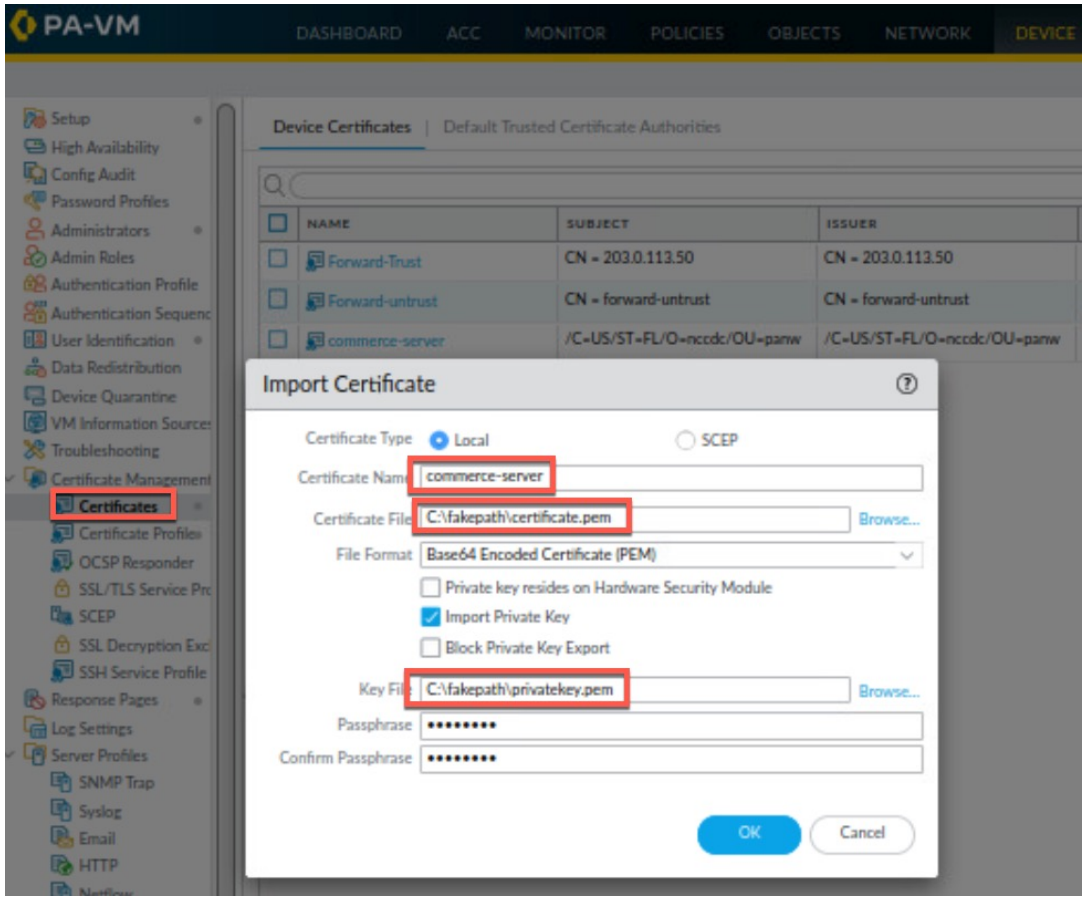
Configure Forward Decryption Policy for Outbound Traffic



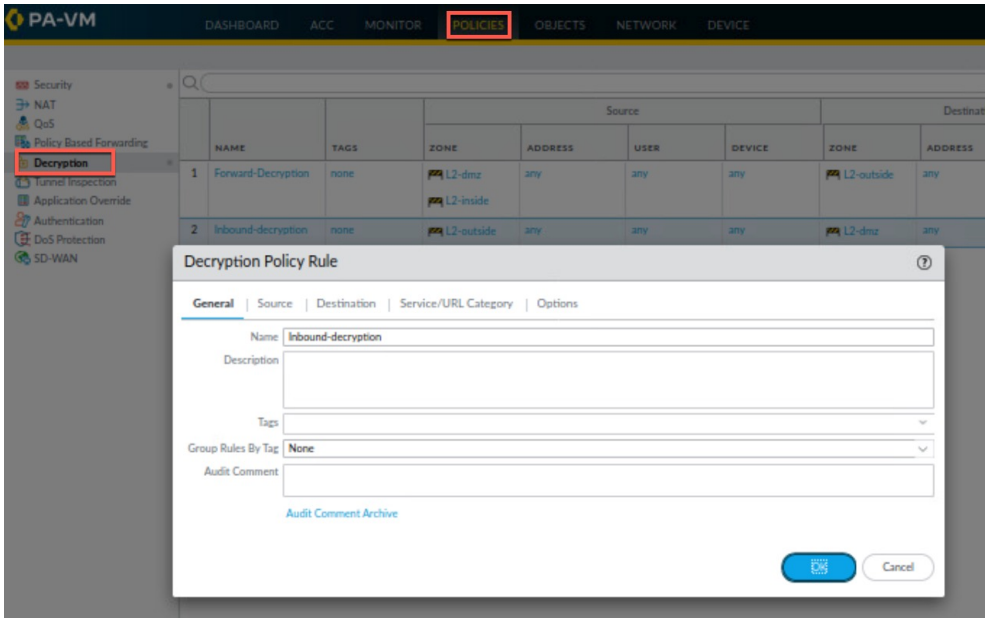


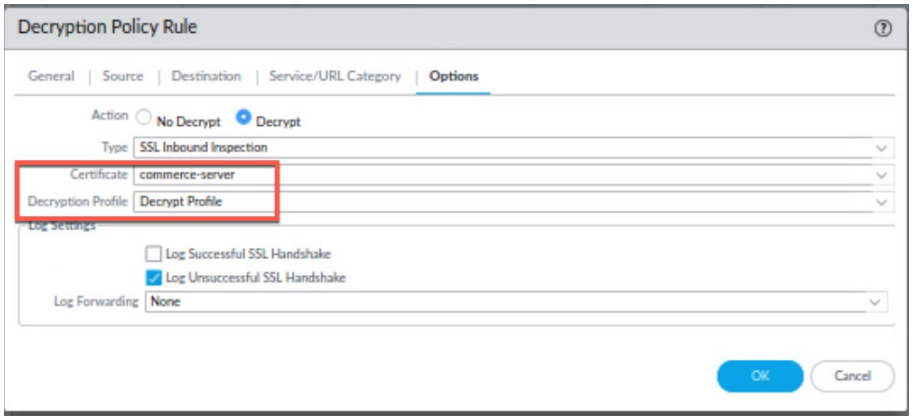


Inbound Decryption: Import Certificates From Your DMZ Server



Configure Inbound Decryption for Your DMZ Server





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

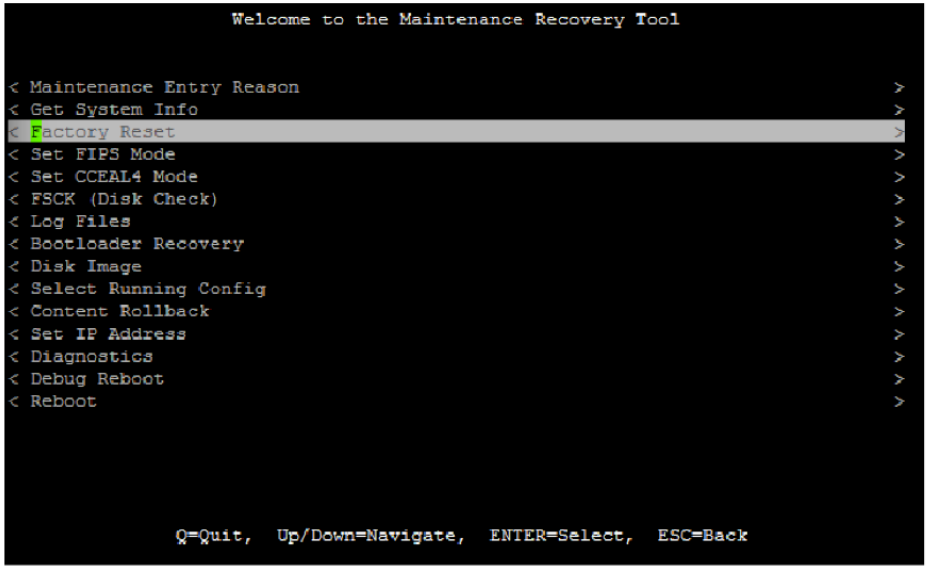
URL Articile for hardware appliances:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldXCAS

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:

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



Thank you.

paloalto NETWORKS