



Palo Alto Install And Setup SOP

By: Lcpl Hundley, Lcpl Regan

3rd PLT DCO-IDM

LU: 20240228

General intent of this document is to give guidance to DCO-IDM personnel who are inexperienced with the Palo Alto firewall .

PALO ALTO Firewall Synopsis.....	2
VM Initial Configuration.....	3
Firewall Walkthrough.....	14
Backup and Restore Configuration.....	23
Upgrade.....	26
-----Repeatable Process-----.....	28
Gateways and IP addresses.....	30
Network Zones.....	31
Policy (Security Rules).....	31
Policy (NAT Rules).....	36
A. Source NAT.....	37
B. U-Turn NAT.....	38
C. Bi-Directional NAT.....	39
Tunnels On Palo Alto.....	40
IKE & IPSec Crypto.....	42
IKE Gateway.....	44
IPSec Tunnels.....	46



PALO ALTO Firewall Synopsis

The Virtualized VM- Series Palo Alto Firewall uses PAN-OSTM, a security-specific operating system that enables intra-virtual machine traffic, protects against known and unknown threats, and integrates flexibly in the virtualized environments. Below are the following limitations to keep in mind during deployment and use of the toolset:

- ❖ Only 10 ports can be configured. One for management traffic and up to 9 can be used for data traffic.
- ❖ Forged transmit and promiscuous mode must be enabled on the ESXi vSwitch port groups connected to Layer 2 and vwire interfaces on the VM-Series firewall.
- ❖ Hypervisor-assigned MAC addresses are enabled by default. If neither promiscuous mode nor hypervisor-assigned MAC address is enabled, the firewall does not receive any traffic.

At their most basic, firewalls are filtering devices that operate on layer 3 and filter traffic based on variables like to/from IP, port, and protocol. Second generation, or stateful firewalls, keep a record of which ports are utilized by a given connection, examine some of the traffic, and make a determination whether to allow the connection based on its ruleset. Third generation firewalls, or application firewalls, control input, output, and access to/from an application or service based on a defined ruleset.

Like a proxy filters web traffic, a firewall filters known-bad traffic using a defined Access Control List (ACL). It is important to note that ACLs are limited in their ability to provide security against even moderately sophisticated actors as it is trivial to change IP addresses from attack to attack, or even during an attack.

The team will usually implement a firewall between the supported command's network and the team's DMSS toolkit.



VM Initial Install and Configuration

❖ Step 1:

On the ESXi Virtual Machines Tab select “Create / Register VM”

The screenshot shows the ESXi Host Client interface. The left sidebar contains a Navigator with categories: Host, Storage, and Networking. The main area displays the 'Virtual Machines' tab for the host 'localhost.localdomain'. A table lists existing VMs with columns for Name, Status, Used space, Guest OS, Host name, Host CPU, and Host memory. A yellow arrow points to the '+ Create / Register VM' button at the top of the VM list.

Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
DC1	Normal	17.51 GB	Microsoft Windows Server 20...	Unknown	20 MHz	2.68 GB
DC2	Normal	17.48 GB	Microsoft Windows Server 20...	Unknown	23 MHz	2.64 GB
SecOnion	Normal	176.25 GB	Oracle Linux 9 (64-bit)	seconion3rd	1.8 GHz	66.29 GB
PaloAlto	Normal	20.57 GB	CentOS 4/5/6/7 (64-bit)	FW-19	696 MHz	7.44 GB
SecAgent1	Normal	18.8 GB	Microsoft Windows 10 (64-bit)	Unknown	40 MHz	5.69 GB
SecAgent2	Normal	19.98 GB	Microsoft Windows 10 (64-bit)	Unknown	37 MHz	6.82 GB
SecAgent3	Normal	8.08 GB	Microsoft Windows 10 (64-bit)	Unknown	53 MHz	6.58 GB

❖ Step 2:

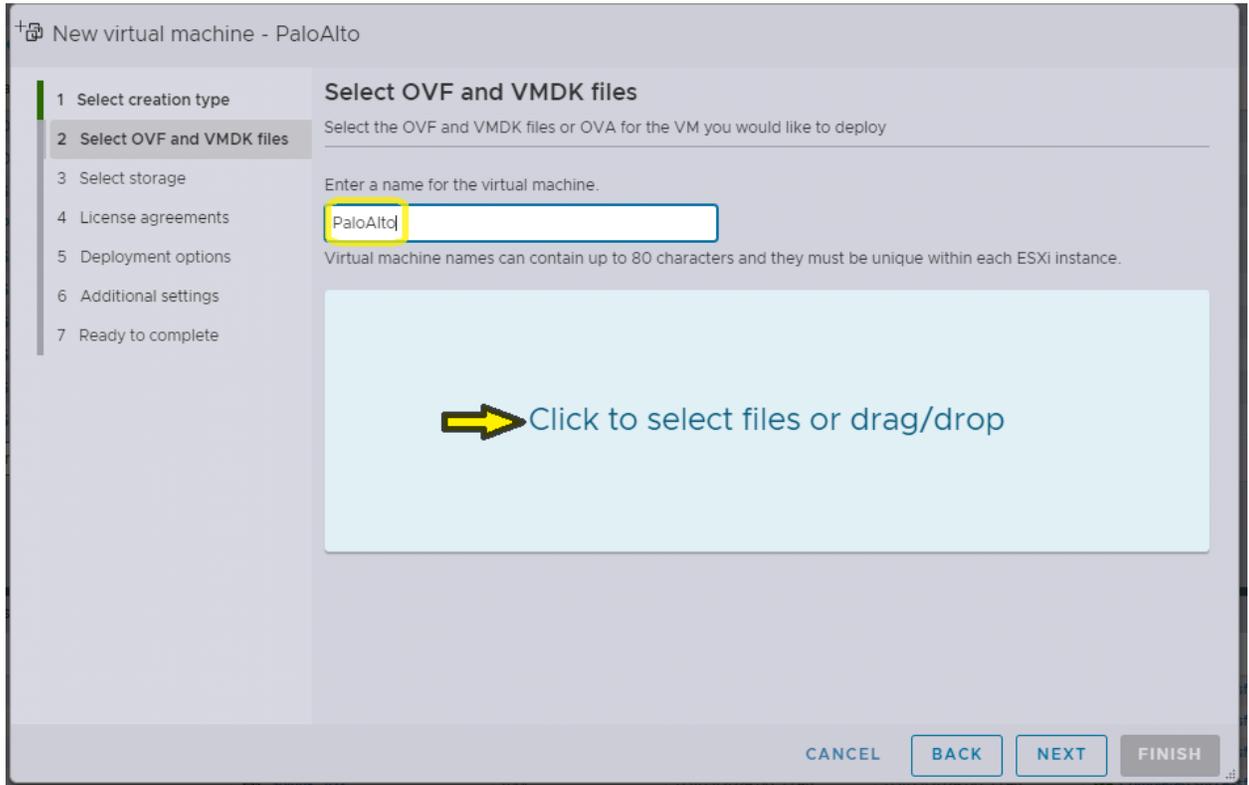
For Creation Type select “Deploy a virtual machine from an OVF or OVA file”

The screenshot shows the 'New virtual machine' wizard. The first step is 'Select creation type'. The main area asks 'How would you like to create a Virtual Machine?' and lists three options: 'Create a new virtual machine', 'Deploy a virtual machine from an OVF or OVA file', and 'Register an existing virtual machine'. A yellow arrow points to the 'Deploy a virtual machine from an OVF or OVA file' option. A text box explains: 'This option guides you through the process of creating a virtual machine from an OVF and VMDK files.' The bottom of the screen has buttons for CANCEL, BACK, NEXT, and FINISH.



❖ **Step 3:**

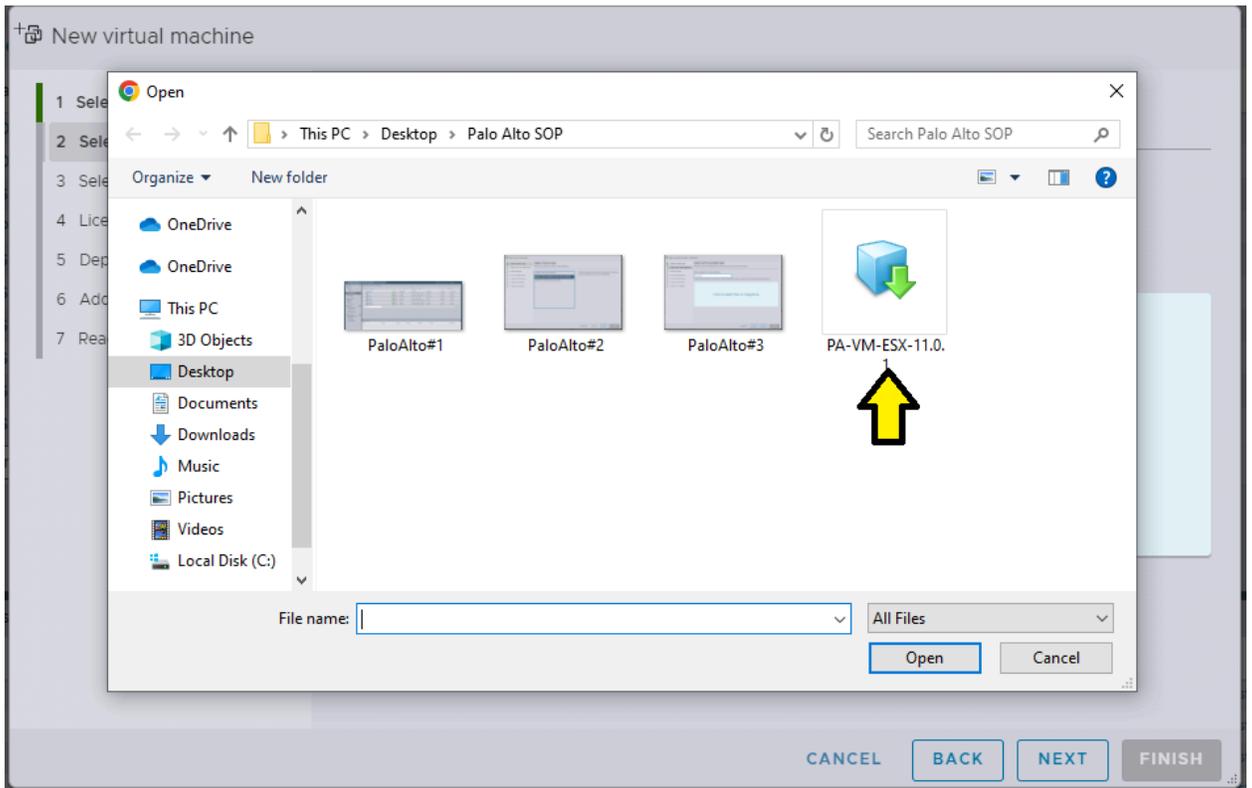
Assign the Virtual machine a name, in this instance name it along the lines of PaloAlto. Then Select “Click to select files or drag/drop”



❖ **Step 4:**

Find and select the Palo Alto OVA file. Notable locations are

- Data Lockers
- The workstation file system/network share
- Datastore on Local Hypervisor





❖ **Step 5:**

Before you open the VM make sure to shut it down fully and open the edit tab

The screenshot shows the PaloAlto VM interface. At the top, there are several control buttons: Console, Monitor, Power on, Shut down (highlighted with a yellow box), Suspend, Restart, Edit (highlighted with a yellow arrow), Refresh, and Actions. Below the buttons, the VM's general information is displayed, including Guest OS (CentOS 4/5/6/7 (64-bit)), Compatibility (ESXi 5.5 virtual machine), VMware Tools (Yes), CPUs (2), Memory (8 GB), and Host name (FW-19). On the right side, there are performance graphs for CPU (696 MHz), MEMORY (7.44 GB), and STORAGE (20.57 GB). The bottom section shows the Hardware Configuration, including CPU (2 vCPUs), Memory (8 GB), Hard disk 1 (5.32 TB), and three Network adapters (Domain Services, Domain Services, and Firewall External).

❖ **Step 6:**

Change memory size to 8 GB and hard disk space can be figured to your needs, Aswell make sure your network adapters are set to domain services for the first 2 network adapters and firewall external for the 3rd adapter

The screenshot shows the 'Edit settings - PaloAlto (ESXi 5.5 virtual machine)' window. The 'Virtual Hardware' tab is selected. The settings are as follows:

- CPU: 2
- Memory: 8 GB (highlighted with a yellow box)
- Hard disk 1: 5.32 TB (highlighted with a yellow box)
- SCSI Controller 0: LSI Logic Parallel
- Network Adapter 1: Domain Services (highlighted with a yellow arrow)
- Network Adapter 2: Domain Services (highlighted with a yellow arrow)
- Network Adapter 3: Firewall External (highlighted with a yellow arrow)
- CD/DVD Drive 1: (empty)
- Video Card: Specify custom settings

At the bottom right, there are 'CANCEL' and 'SAVE' buttons.



❖ **Step 7:**

The login and password are **admin/admin**

Note you might have to enter the login and password several times

Then you will get the option to change the password to the shop standard password

```
PaloAltoTest
PÅ-UM login: admin
Password:
Last login: Tue Mar  5 01:00:36 on tty1
Enter old password :
Enter new password :
Confirm password  :
Password changed

Number of failed attempts since last successful login: 0

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



❖ Step 8:

Before you enter any configurations make sure your mac addresses match your ESXI network adapter mac addresses. Commands on Palo alto for seeing mac addresses are **show interface all** And **show interface management**

```
admin@FU-19> show interface all
total configured hardware interfaces: 2
name            id  speed/duplex/state  mac address
-----
ethernet1/1     16  10000/full/up      00:0c:29:1c:f0:62
ethernet1/2     17  10000/full/up      00:0c:29:1c:f0:6c

aggregation groups: 0

total configured logical interfaces: 2
name            id  usys zone  forwarding  tag  address
-----
ethernet1/1     16  1    INSIDE    ur:default  0    10.1.10.100/24
ethernet1/2     17  1    OUTSIDE   ur:default  0    20.20.10.10/24

admin@FU-19>

admin@FU-19> show interface management
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 10000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:0c:29:1c:f0:58

Ip address: 10.1.10.21
Netmask: 255.255.255.0
Default gateway: 10.1.10.1
Ipo6 address: unknown
Ipo6 link local address: fe80::20c:29ff:fe1c:f05b/64
Ipo6 default gateway:

Logical interface counters:
bytes received          16571409
bytes transmitted      314913407
packets received       105840
packets transmitted    103023
receive errors         0
transmit errors        0
receive packets dropped 0
transmit packets dropped 0
multicast packets received 9

admin@FU-19>
```

Domain Services vSwitch topology:

- Physical adapters: vmnic4, 1000 Mbps, Full
- Virtual Machines (1):
 - Palo Alto (MAC Address 00:0c:29:1c:f0:58)
 - Palo Alto (MAC Address 00:0c:29:1c:f0:62)
 - Splunk_ID1
 - Splunk_ID2
 - Splunk_SH
 - DC1
 - SecOnion
 - DC2
 - WinTest1
 - WinTest3
 - WinTest2
 - Arkime

Firewall External vSwitch topology:

- Physical adapters: vmnic4, 1000 Mbps, Full
- Virtual Machines (1):
 - Palo Alto (MAC Address 00:0c:29:1c:f0:6c)



❖ **Step 9:**

Type “configure” to enter configuration mode

```
admin@PA-UM>
admin@PA-UM>
admin@PA-UM> configure
Entering configuration mode
[edit]
admin@PA-UM#
```

❖ **Step 10:**

To set the Hostname type “set deviceconfig system hostname FW-19”

```
admin@PA-UM>
admin@PA-UM> configure
Entering configuration mode
[edit]
admin@PA-UM# clear
Unknown command: clear
[edit]
admin@PA-UM# cls
Unknown command: cls
[edit]
admin@PA-UM# set deviceconfig system hostname FW-19
```

❖ **Step 11:**

To assign the VM with a static ip and assign is DNS servers type “set deviceconfig system ip-address 10.1.10.28 netmask 255.255.255.0 default-gateway 10.1.10.1 dns-setting servers primary 10.1.10.14 secondary 10.1.10.15” (change ip addresses as needed)

```
admin@PA-UM> configure
Entering configuration mode
[edit]
admin@PA-UM# set device
> device-object device-object
> deviceconfig deviceconfig

admin@PA-UM# set deviceconfig system hostname FW-Test

[edit]
admin@PA-UM# set deviceconfig system ip-address 10.1.10.28 netmask 255.255.255.0 default-gateway 10.1.10.1 dns-setting servers primary 10.1.10.14 secondary 10.1.10.15

[edit]
admin@PA-UM# _
```

❖ **Step 12:**

The next part is to make the Vm’s ip address static so DHCP does not assign the ip, Type “set deviceconfig system type static”

```
admin@PA-UM> configure
Entering configuration mode
[edit]
admin@PA-UM# set device
> device-object device-object
> deviceconfig deviceconfig

admin@PA-UM# set deviceconfig system hostname FW-Test

[edit]
admin@PA-UM# set deviceconfig system ip-address 10.1.10.28 netmask 255.255.255.0 default-gateway 10.1.10.1 dns-setting servers primary 10.1.10.14 secondary 10.1.10.15

[edit]
admin@PA-UM# set device
> device-object device-object
> deviceconfig deviceconfig

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



❖ **Step 13:**

To save your configurations you just applied, type “Commit”

```
[edit]
admin@PA-UM# set deviceconfig system ip-address 10.1.10.28 netmask 255.255.255.0 default-gateway 10.1.10.1 dns-setting servers primary 10.1.10.14 secondary 10.1.10.15

[edit]
admin@PA-UM# set device
> device-object device-object
> deviceconfig deviceconfig

admin@PA-UM# set deviceconfig system type static

[edit]
admin@PA-UM# commit

Commit job 3 is in progress. Use Ctrl+C to return to command prompt
.....
```

❖ **Step 14:**

In you web browser type in the ip address of the palo alto you just configured and log in, Next you will navigate to the Device tab

The screenshot shows the Palo Alto Networks PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. The 'DEVICE' tab is selected and highlighted with a yellow arrow. The main content area is divided into several sections:

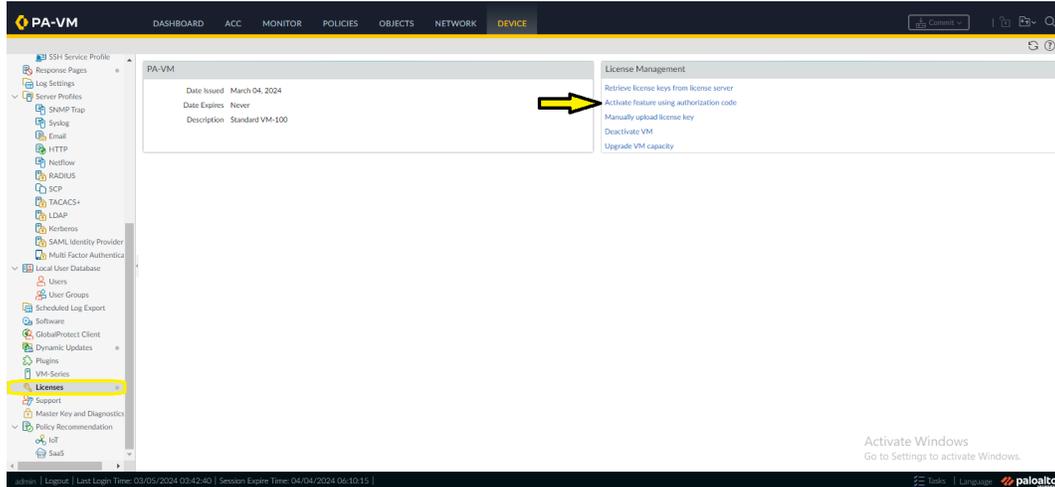
- Interfaces:** Shows a grid of interface status icons.
- General Information:** Displays device details such as Device Name (FW-19), MGT IP Address (10.1.10.21), MGT Netmask (255.255.255.0), MGT Default Gateway (10.1.10.1), MGT IPv6 Address (unknown), MGT IPv6 Link Local Address (fe80::20c:29ff:fe1c:05b/64), MGT IPv6 Default Gateway, MGT MAC Address (00:0c:29:1c:f0:5b), Model (PA-VM), Serial # (007051000255314), CPU ID (ESX:54060500FFB880F), UUID (564D4440-7D15-1D9D-355A-37CA9E1CF058), VM Cores (2), VM Memory (8158344), VM License (VM-100), VM Capacity Tier (6.5 GB), VM Mode (VMware ESXi), Software Version (11.0.1), GlobalProtect Agent (0.0.0), and Application Version (8644-7712).
- Logged In Admins:** A table showing active sessions for the 'admin' user from IP addresses 10.1.10.2 and 10.1.10.4.
- Data Logs:** Shows no data available.
- System Logs:** A table of system events including user logins, update server connections, and authentication events.
- Config Logs:** Shows no data available.
- Locks:** Shows no locks found.
- ACC Risk Factor (Last 60 minutes):** Shows no data found.

An 'Activate Windows' watermark is visible in the bottom right corner of the interface.



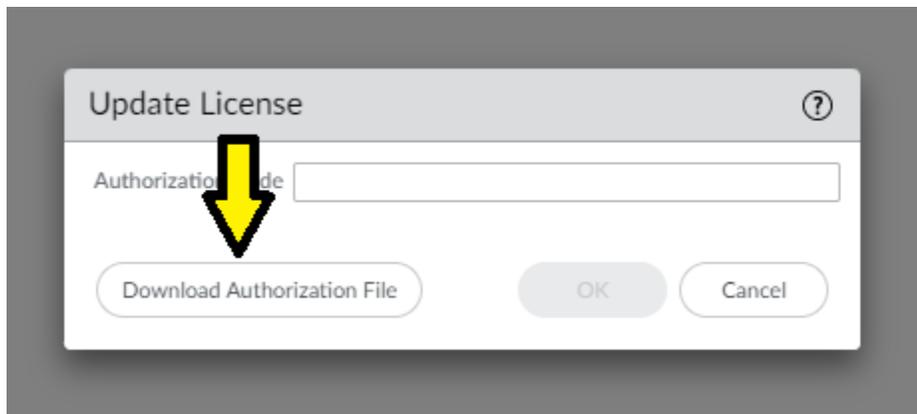
❖ **Step 15:**

Once in the device tab, in the left scroll pane scroll down till you see licenses. In the right pane under license Management select “Activate feature using authorization code”



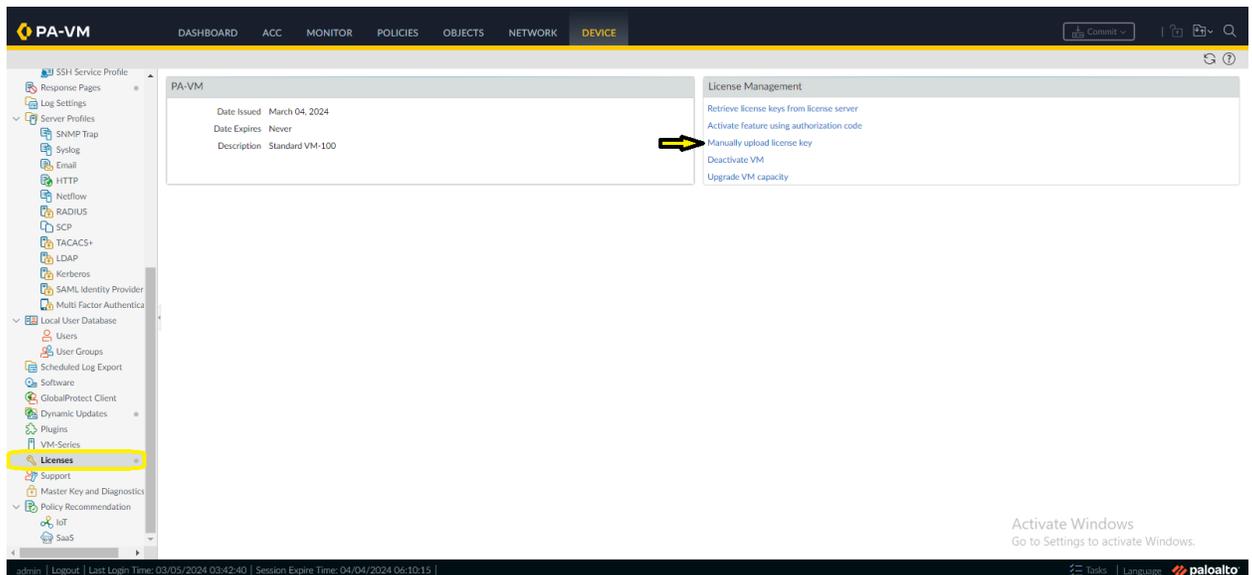
❖ **Step 16:**

Click “Download Authorization File”



❖ **Step 17:**

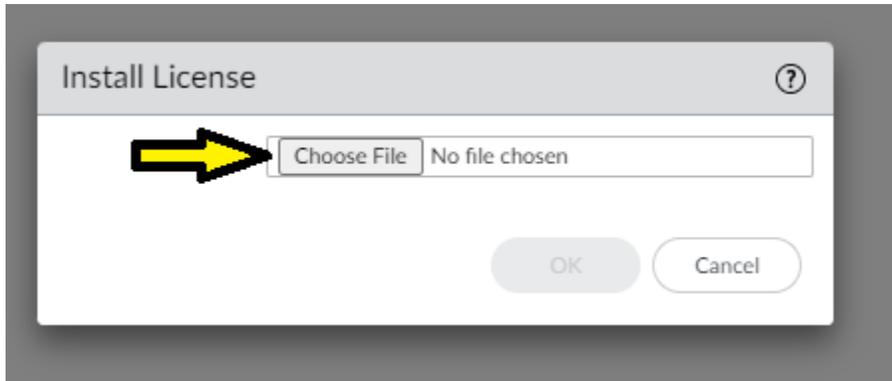
Now under License Management select “Manually upload license key”





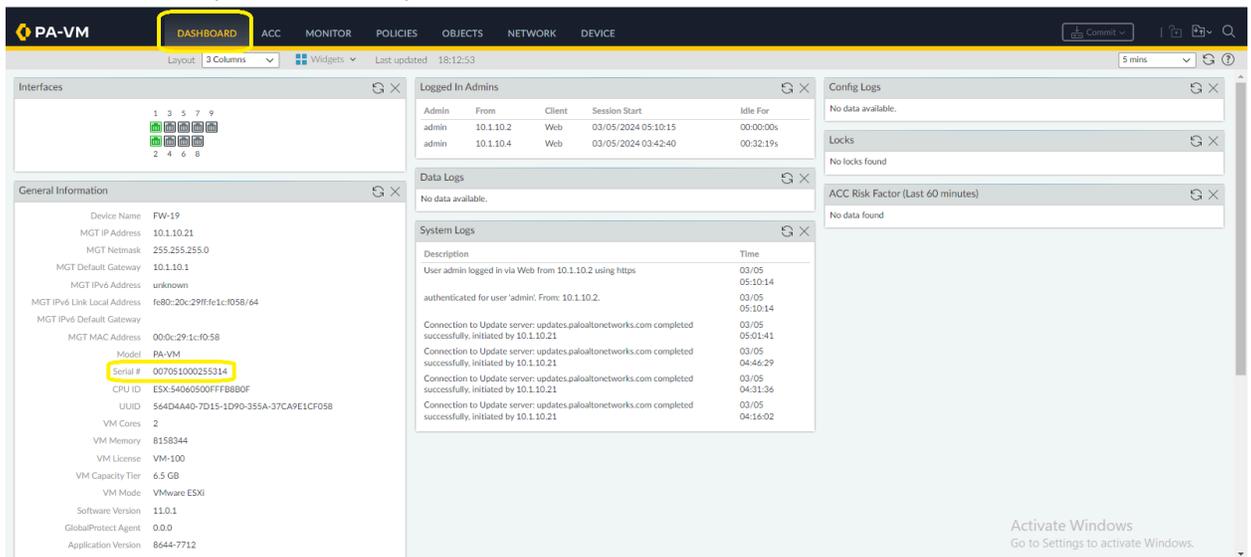
❖ **Step 18:**

Give authorization file to Palo Alto support point of contact (as of 3/6/2024 Ssgt Marshburn) then once given the .key file upload into



❖ **Step 19:**

Once the reboot finishes reconnect to the vm if needed and navigate to the Dashboard tab and look at the Serial# under General Information. There should be a number there if authorization was done correctly, if not it will say unknown.





❖ **Step 20:**

Navigate to the network tab select the Zones option on the left scroll pane, to add a zone select the add button at the bottom of the page.

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	ENABLE HEADER INSPECTION	PACKET BUFFER PROTECTION	LOG SETTING	User-ID		Device-ID			
							ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
INSIDE	layer3	ethernet1/1		<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
OUTSIDE	layer3	ethernet1/2		<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none

❖ **Step 21:**

Once in zone configuration, name the zone based off of network location (this example is for the Internal traffic why we named it Inside), Change the type to Layer 3. Then Select add and select the correct ethernet interface you want to assign this zone to.

Zone

Name:

Log Setting:

Type:

INTERFACES ^

- ethernet1/1

Add Delete

Zone Protection

Zone Protection Profile:

Enable Packet Buffer Protection

Enable L3 & L4 Header Inspection

User Identification ACL

Enable User Identification

INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will be identified.

EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will not be identified.

Device-ID ACL

Enable Device Identification

INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Devices from these addresses/subnets will be identified.

EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Devices from these addresses/subnets will not be identified.



❖ **Step 22:**

name the zone based off of network location (this example is for the External traffic why we named it Outside), Change the type to Layer 3. Then Select add and select the correct ethernet interface you want to assign this zone to.

The screenshot shows the 'Zone' configuration page in the Palo Alto Networks GUI. The 'Name' field is highlighted in yellow and contains the text 'OUTSIDE'. The 'Type' dropdown is also highlighted in yellow and set to 'Layer3'. Under the 'INTERFACES' section, 'ethernet1/2' is selected and highlighted in yellow. A yellow arrow points to the '+ Add' button below the interface list. The 'Zone Protection' section shows 'Zone Protection Profile' set to 'None', 'Enable Packet Buffer Protection' checked, and 'Enable L3 & L4 Header Inspection' unchecked. The 'User Identification ACL' and 'Device-ID ACL' sections are also visible, each with an 'INCLUDE LIST' and 'EXCLUDE LIST' section.

❖ **Step 23:**

Navigate to the Network tab and select the interfaces option on the left scroll pane, to configure the interfaces select the ethernet you need to configure.

The screenshot shows the 'Network' tab in the Palo Alto Networks GUI. The 'Interfaces' section is selected in the left sidebar. A table lists various interfaces, with 'ethernet1/2' highlighted by a yellow arrow. The table has the following columns: INTERFACE, INTERFACE TYPE, MANAGEMENT PROFILE, LINK STATE, IP ADDRESS, VIRTUAL ROUTER, TAG, VLAN / VIRTUAL-WIRE, SECURITY ZONE, SD-WAN INTERFACE PROFILE, UPSTREAM NAT, FEATURES, and COMMENT.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES	COMMENT
ethernet1/1		PING		10.1.10.100/24	default	Untagged	none	INSIDE		Disabled		
ethernet1/2		PING		20.20.10.10/24	default	Untagged	none	OUTSIDE		Disabled		
ethernet1/3				none	none	Untagged	none	none		Disabled		
ethernet1/4				none	none	Untagged	none	none		Disabled		
ethernet1/5				none	none	Untagged	none	none		Disabled		
ethernet1/6				none	none	Untagged	none	none		Disabled		
ethernet1/7				none	none	Untagged	none	none		Disabled		
ethernet1/8				none	none	Untagged	none	none		Disabled		
ethernet1/9				none	none	Untagged	none	none		Disabled		



❖ **Step 24:**

On the Interface management change the interface type to layer 3 and under config select the security zone that the interface IP scheme falls under (Ex. 10.1.10.100 falls under 10.1.10.0/24 zone) (Ex. Outside=Ethernet1/2, Inside=Ethernet1/1)

Ethernet Interface

Interface Name: ethernet1/2

Comment: [empty]

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default

Security Zone: OUTSIDE

OK Cancel

❖ **Step 25:**

Under the IPv4 Tab select the “Add” button and input the interface IP that the Scheme falls under (Ex. 10.1.10.100/24 falls under the inside Scheme or 20.20.10.10/24 falls under the outside scheme)

Ethernet Interface

Interface Name: ethernet1/1

Comment: [empty]

Interface Type: Layer3

Netflow Profile: None

Config | **IPv4** | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type: Static PPPoE DHCP Client

<input type="checkbox"/>	IP
<input type="checkbox"/>	10.1.10.100/24
<input checked="" type="checkbox"/>	your inside interface ip

+ Add - Delete ↑ Move Up ↓ Move Down

IP = /netmask. Ex. 192.168.2.254/24

OK Cancel



❖ **Step 26:**

Navigate to the Advanced tab and select “Management Profile”. In the drop down menu select “New Management profile”

❖ **Step 27:**

Give the Management profile its (Ex. Ping) then select the network service you need (Ex. Ping)



❖ **Step 28:**

Navigate to the “Virtual Routers” option in the “Network” tab. Select the “Add” Button at the bottom of the screen.

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

NAME	INTERFACES	CONFIGURATION	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
default	ethernet1/1 ethernet1/2	Static Routes: 2 ECMP status: Disabled						More Runtime Stats

Virtual Routers

Activate Windows
Go to Settings to activate Windows.

admin | Logout | Last Login Time: 03/05/2024 03:42:40 | Session Expire Time: 04/04/2024 06:10:15 | Tasks | Language | paloalto

❖ **Step 29:**

Select the add button and add all the interfaces previously configured.

Virtual Router - default

Router Settings

Name default

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

General | ECMP

INTERFACES ^

- ethernet1/1
- ethernet1/2

Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

Add Delete

OK Cancel



❖ **Step 30:**

Navigate to the “Policies Tab and open the “Security” option in the left scroll pane. Then click the “Add” button

NAME	TAGS	TYPE	ZONE	Source			Destination			APPLICATION	SERVICE	ACTION	PROFILE
				ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1 ANY	none	universal	any	any	any	any	any	any	any	any	Allow	none	
2 SSH to S0F	none	universal	INSIDE	10.1.10.100/24	any	any	OUTSIDE	20.20.10.10/24	any	any	SSH	Allow	none
3 Intrazone-default	none	Intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
4 Interzone-default	none	Interzone	any	any	any	any	any	any	any	any	any	Deny	none

❖ **Step 31:**

Policies are the firewall rules being implemented on palo alto. Name them according to what they allow/block

Rule type: leave as universal

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions

Name: Policy rule name

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

OK Cancel



❖ **Step 32:**

Source and destination refer to the traffic flow through the firewall.

source zone:

- if going from within your network to out. Source is **INSIDE**
- If originating from outside your network coming in. Source is **OUTSIDE**

The screenshot shows the 'Security Policy Rule' configuration window, specifically the 'Source' tab. The window has a title bar with a question mark icon. Below the title bar are tabs for 'General', 'Source', 'Destination', 'Application', 'Service/URL Category', and 'Actions'. The 'Source' tab is active and contains four columns for defining source criteria:

<input type="checkbox"/> Any	<input type="checkbox"/> Any	select	select
<input checked="" type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^	<input type="checkbox"/> SOURCE DEVICE ^
<input checked="" type="checkbox"/> INSIDE OUTSIDE			
+ Add - Delete	+ Add - Delete	+ Add - Delete	+ Add - Delete

At the bottom of the window, there is a 'Negate' checkbox and 'OK' and 'Cancel' buttons.



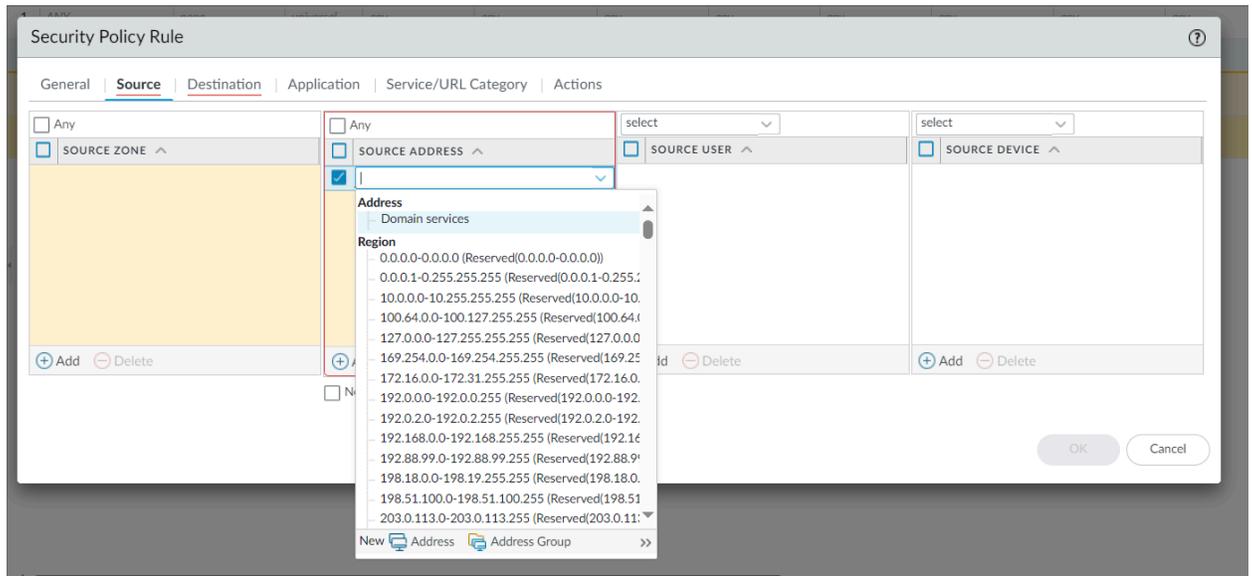
❖ **Step 33:**

Source Address:

- Interface IP associated with the zone selected
(Ex. Source zone=INSIDE ; Source Address=10.1.10.100)

Source User & Source Device:

- Leave blank

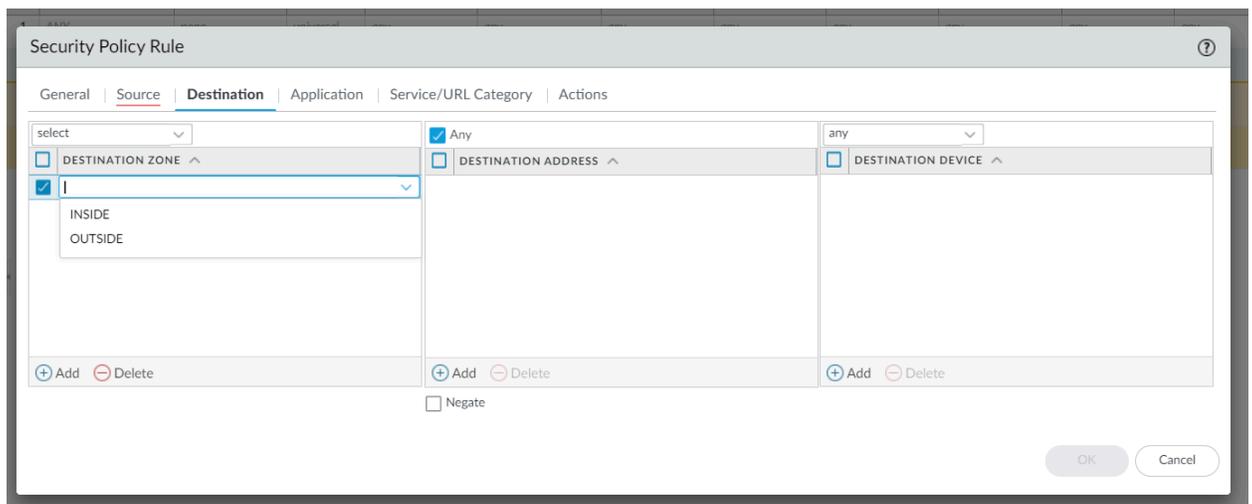


❖ **Step 34:**

Destination Zone:

The endpoint of the traffic you want to allow/block

- if going from within your network to out. Destination is OUTSIDE
- If originating from outside your network coming in. Destination is INSIDE





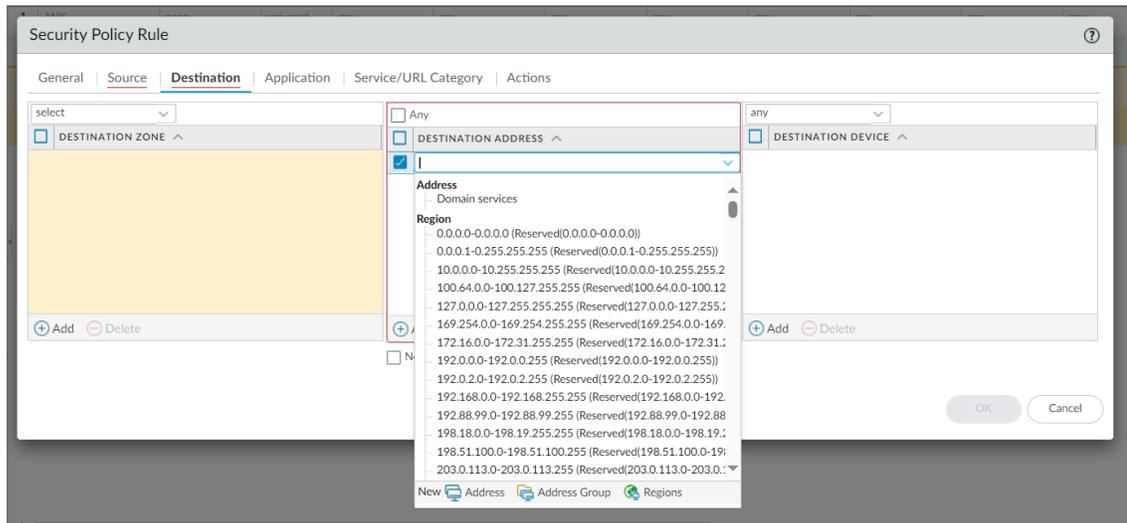
❖ **Step 35:**

Source Address:

- Network IP range of the source zone selected
(Ex. Source zone=OUTSIDE ; Destination Address=20.20.10.10)

Source User & Source Device:

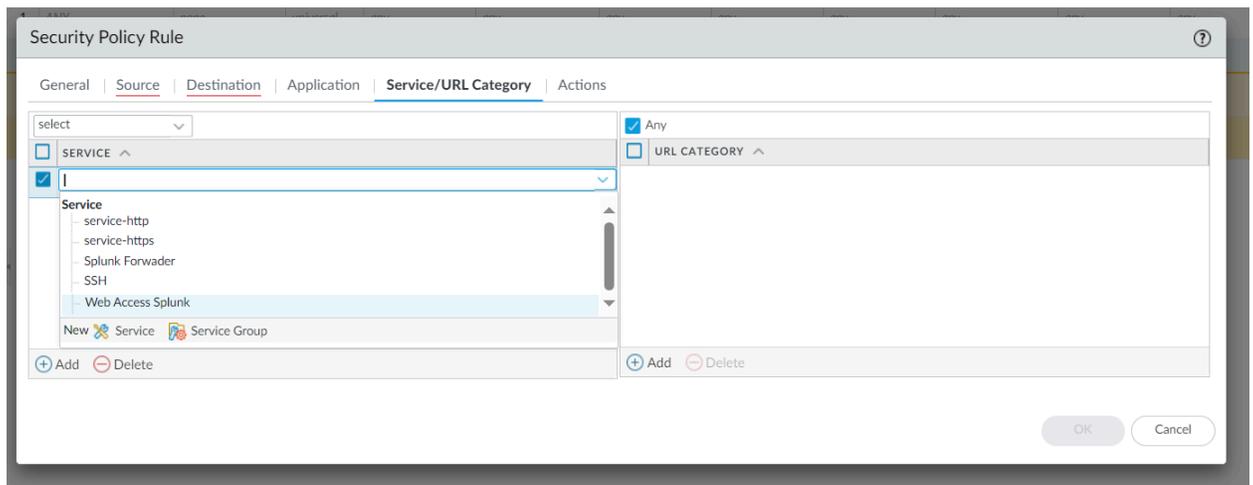
- Leave blank



❖ **Step 36:**

Services are another way of fingerprinting traffic as it passes through the firewall, Allowing/blocking ports and protocols.

- Select New Service
- URL Category: Leave default





❖ **Step 37:**

- Name your Service something recognizable (HTTPS / SSH)
- Specify if the Service uses the TCP or UDP protocol
- Specify Destination & Source ports assigned to the service (SSH -> Destination Port=22 , Source Port=1-65535)
1-65535 represents ANY

Service

Name:

Description:

Protocol: TCP UDP

Destination Port:

Source Port:

Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)

Session Timeout: Inherit from application Override

Tags:

OK Cancel

❖ **Step 38:**

Once all the configurations are done, Select the “Commit” Button in the top right hand corner. If you don't do this all your configurations will not be applied, erasing your work.

PA-VM | DASHBOARD | ACC | MONITOR | POLICIES | OBJECTS | NETWORK | DEVICE

Commit 5 mins

Layout: 3 Columns | Widgets | Last updated: 19:47:19

Interfaces

1	3	5	7	9
2	4	6	8	

General Information

Device Name: FW-19
MGT IP Address: 10.1.10.21
MGT Netmask: 255.255.255.0
MGT Default Gateway: 10.1.10.1
MGT IPv6 Address: unknown
MGT IPv6 Link Local Address: fe80::29ff:fc1c:058/64
MGT IPv6 Default Gateway:
MGT MAC Address: 00:0c:29:1c:f0:58
Model: PA-VM
Serial #: 007051000255314
CPU ID: ESX-54060500FFB880F
UUID: 564D4A40-7D15-1D90-355A-37CA9E1CF058
VM Cores: 2
VM Memory: 8158344
VM License: VM-100
VM Capacity Tier: 6.5 GB
VM Mode: VMware ESXi
Software Version: 11.0.1
GlobalProtect Agent: 0.0.0
Application Version: 8644-7712

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	Console	CLI	03/05/2024 06:22:26	00:20:48s
admin	10.1.10.2	Web	03/05/2024 05:10:15	00:00:00s

Data Logs

No data available.

System Logs

Description	Time
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 06:31:43
User admin logged in via CLI from Console	03/05 06:32:26
authenticated for user 'admin'. From Console or telnet.	03/05 06:22:25
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 06:16:23
Auto update agent found no new IoT updates	03/05 06:08:13
Failed to check IoT content upgrade info due to Unknown error	03/05 06:08:13
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 06:08:13
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 06:01:38
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 05:46:17

Config Logs

Command	Path	Admin	Time
delete	vsys vsys1 rulebase security rules Splunk Forwarder	admin	03/05 06:43:42
delete	vsys vsys1 rulebase security rules Splunk Rules	admin	03/05 06:43:36
delete	vsys vsys1 rulebase security rules SSH	admin	03/05 06:43:26
delete	vsys vsys1 rulebase security rules HTTPS	admin	03/05 06:43:22
edit	vsys vsys1 rulebase security rules ANY disabled	admin	03/05 06:07:58
move	vsys vsys1 rulebase security rules ANY	admin	03/05 06:07:45
move	vsys vsys1 rulebase security rules ANY	admin	03/05 06:07:42
set	vsys vsys1 rulebase security rules ANY	admin	03/05 06:07:42
move	vsys vsys1 rulebase security rules SSH.to.SOF	admin	03/05 06:06:25
move	vsys vsys1 rulebase security rules HTTPS	admin	03/05 06:06:19

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

No data found

Activate Windows
Go to Settings to activate Windows.

admin | Logout | Last Login Time: 03/05/2024 03:42:40 | Session Expire Time: 04/04/2024 06:10:15 | Tasks | Language | paloalto



- ❖ **Step 39:**
Select "commit"

Commit

Doing a commit will overwrite the running configuration with the commit scope.

Commit All Changes Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▶ policy-and-objects	Policy and Objects			
▶ device-and-network	Device and Network Configuration			

[Preview Changes](#) [Change Summary](#) [Validate Commit](#)

Note: This shows all the changes in login admin's accessible domain.

Description

