



## Palo Alto Install And Setup SOP

By: Lcpl Hundley, Lcpl Regan <u>3rd PLT DCO-IDM</u> <u>LU: 20240228</u>

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	
Firewall Walkthrough	
Backup and Restore Configuration	
Upgrade	
Repeatable Process	
Gateways and IP addresses	
Network Zones	31
Policy (Security Rules)	31
Policy (NAT Rules)	
A. Source NAT	
B. U-Turn NAT	
C. Bi-Directional NAT	
Tunnels On Palo Alto	40
IKE & IPSec Crypto	
IKE Gateway	
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"

☆ Navigator ✓ Host	«	🛱 localhost.localdomain - Virtual Machines						
Manage		* Create / Register VM   Console   Power on	() Power	off 🔢 Suspend   🤇	C Refresh Actions		Qs	earch
Monitor		Virtual machine ~ S	Status ~	Used space ~	Guest OS 🗸 🗸	Host name 🗸 🗸	Host CPU ~	Host memory ~
Virtual Machines	7	□ ੈ 🛱 DC1	📀 Normal	17.51 GB	Microsoft Windows Server 20	Unknown	20 MHz	2.68 GB
√ 🕲 PaloAlto		□ *@ DC2 (	📀 Normal	17.48 GB	Microsoft Windows Server 20	Unknown	23 MHz	2.64 GB
Monitor		SecOnion	📀 Normal	176.25 GB	Oracle Linux 9 (64-bit)	seconion3rd	1.8 GHz	66.29 GB
> 📴 SecOnion		PaloAlto 6	📀 Normal	20.57 GB	CentOS 4/5/6/7 (64-bit)	FW-19	696 MHz	7.44 GB
> 🔂 DC1		SecAgent1	📀 Normal	18.8 GB	Microsoft Windows 10 (64-bit)	Unknown	40 MHz	5.69 GB
> 🔂 DC2		SecAgent2	📀 Normal	19.98 GB	Microsoft Windows 10 (64-bit)	Unknown	37 MHz	6.82 GB
More VMs		SecAgent3	📀 Normal	8.08 GB	Microsoft Windows 10 (64-bit)	Unknown	53 MHz	6.58 GB
✓ E Storage ✓ C datastoreBig Monitor > C datastore1 More storage	2	Ouick filters v						7 items
V Networking Firewall External Sniffing vSwitch0	4							
More networks		Recent tasks						
					Charles	Desult 4		Commission of m

### \* Step 2:

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

+6	New virtual machine	
	1 Select creation type	Select creation type
	<ol> <li>Select OVF and VMDK files</li> <li>Select storage</li> <li>License agreements</li> <li>Deployment options</li> <li>Additional settings</li> <li>Ready to complete</li> </ol>	How would you like to create a Virtual Machine?         Create a new virtual machine         Deploy a virtual machine from an OVF or OVA file         Register an existing virtual machine
		CANCEL BACK NEXT FINISH





# 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

Sele Sele Lice Dep	$\leftrightarrow \rightarrow \checkmark \uparrow$	→ This ew folder	PC > Desktop > Pal	o Alto SOP		- 7.				
Sele Lice	Organize 👻 N	ew folder				• 0	Search Palo /	Alto SOP		ρ
Lice								-		2
5 Dep	OneDrive	^								
	lene One Drive			Normania Manageria Without Strategy Manageria Wi	Research MAR means MR PERSON N means National Statements means National Statements					
6 Add	💻 This PC				The second secon					
Rea	🧊 3D Objects		PaloAlto#1	PaloAlto#2	PaloAlto#3	PA-V	/M-ESX-11.0.			
	📃 Desktop						$\mathbf{\lambda}$			
	Documents						<b>4                                    </b>			
	👆 Downloads									
	👌 Music									
	Pictures									
	📕 Videos									
	🏪 Local Disk (C	)								
		File nan	ne:			~	All Files			~
							Open		Cancel	







#### Step 5:

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

PaloAlto				
📮 Console 🛛 Monitor 📄 🕨 Po	ower on 🕐 Shut down 🛛 🛿 Suspend 🛛 🛱 Restart	🖍 Edit   C Refresh	Actions	^
	PaloAlto       Guest OS     CentOS 4/5/6/7 (64-bit)       Compatibility     ESXI 5.5 virtual machine       VMware Tools     Yes       CPUs     2       Memory     8 GB       Host name     FW-19	Û		CPU (1) 696 MHZ (1) MEMORY 7.44 GB (1) STORAGE 20.57 GB (1)
- General Information		- Hardware Configuration		
√ ❷ Networking		> 💭 CPU	2 vCPUs	
Host name	FW-19	I Memory	8 GB	
IP addresses	1.1.10.110.21 2.2.fe80::200.29ff.felc:f058 3.3.fe80::270.76ff.fe69:66ff 4.4::127.131.11 5.5.fe80::270.76ff.fe69:66ff 6.6.10.10100	> 🕞 Hard disk 1 > 🛱 Network adapter 1 > 🗟 Network adapter 2 > 🗟 Network adapter 3	5.32 TB Domain Services (Connected) Domain Services (Connected) Firewall External (Connected)	

#### 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

Intual Hardware VM Options			
🖨 Add hard disk 🦳 🗒 Add netwo	rk adapter 🛛 🖪 Add other device		
CPU	2 ~ 1		
😇 Memory	8 GB 🗸		
Hard disk 1	5.32 TB 🗸		×
SCSI Controller 0	LSI Logic Parallel	~	
😇 Network Adapter 1	Domain Services	✓ Connect	×
😇 Network Adapter 2	Domain Services	✓ Connect	×
🔄 Network Adapter 3	Firewall External	✓ Connect	×
S CD/DVD Drive 1		~	×
Video Card	Specify custom settings	~	





## \* 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		Actions X
PA-VM 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 credentia our password prior to deployment. admin@PA-VM>	als. Please	e change y





#### 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** 







#### Step 9:

Type "configure" to enter configuration mode



#### Step 10:

To set the Hostname type "set deviceconfig system hostname FW-19"

admin@PA-VM>	
admin@PA-VM> configure	
Entering configuration mode	
[edit]	
admin@PA-VM# clear	
Unknown command: clear	
[edit]	
admin@PA-VM# cls	
Unknown command: cls	
realti	
admin@PA-VM# 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-VM# set deviceconfig system hostname FW-Test

#### [edit]

admin@PA-VM# 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-VM# \_

#### 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-VM> configure Entering configuration mode [edit] admin@PA-VM# set device > device-object device-object deviceconfig deviceconfig admin@PA-VM# set deviceconfig system hostname FW-Test [edit] admin@PA-VM# 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-VM# set device > device-object device-object deviceconfig deviceconfig admin@PA-VM# set deviceconfig system type static





#### Step 13:

To save your configurations you just applied, type "Commit"

#### [edit]

admin@PA-VM# 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-VM# set device > device-object device-object > deviceconfig deviceconfig

admin@PA-VM# set deviceconfig system type static



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

📢 PA-VM	DASHBOARD ACC MONITOR	POLICI	ES OBJECTS NETWORK DEVICE			📩 Commit 🗸 🛛   🔁 🗗 🗸 Q
	Layout 3 Columns 🗸 👫 Widgets 🗸	Last upd	lated 18:12:53			5 mins 🗸 🕤 🕐
Interfaces		$\mathbf{G}\times$	Logged In Admins	G×	Config Logs	S × Đ
	1 3 5 7 9 1 6 6 6 6 6 1 6 7 7 1 7 9 1 7		Admin         From         Client         Session Start           admin         10.1.10.2         Web         03/05/2024 05:10:15           admin         10.1.10.4         Web         03/05/2024 03:42:40	Idle For 00:00:00s 00:32:19s	No data available. Locks No locks found	Ø×
General Information		$G \times$	Data Logs	G ×	ACC Risk Factor (Last 60 minutes)	ß×
Device Name MGT IP Address	FW-19 10.1.10.21		System Logs	G ×	No data found	
MGT Netmask	255.255.255.0		Description	Time		
MGT Default Gateway	10.1.10.1 unknown		User admin logged in via Web from 10.1.10.2 using https	03/05 05:10:14		
MGT IPv6 Link Local Address	fe80::20c:29ff:fe1c:f058/64		authenticated for user 'admin'. From: 10.1.10.2.	03/05 05:10:14		
MGT IPv6 Default Gateway MGT MAC Address	00:0c:29:1c:f0:58		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 05:01:41		
Model	PA-VM		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 04:46:29		
CPU ID	ESX:54060500FFFB8B0F		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 04:31:36		
UUID VM Cores	564D4A40-7D15-1D90-355A-37CA9E1CF058 2		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 04:16:02		
VM Memory	8158344					
VM License VM Capacity Tier	VM-100					
VM Capacity Her	VMware ESXi					
Software Version	11.0.1					
GlobalProtect Agent	0.0.0				Activ	ate Windows
Application Version	8644-7712				Go to S	ettings to activate Windows.





#### ✤ 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"

🚺 PA-VM	DASHBOARD ACC MO	NITOR POLICIES	OBJECTS	NETWORK	DEVICE			Commit ~	în 18ar Q
NR COLORIS DUCIN									5 ()
Response Pages •	PA-VM						License Management		
Log Settings	Date Issued March 04, 202	14					Retrieve license keys from license server		
V Lever Profiles	Date Expires Never						Activate feature using authorization code		
System	Description Standard VM-	100				-	Manually upload license key		
Email							Deactivate VM		
🚯 НТТР							Upgrade VM capacity		
Netflow									
RADIUS									
L SCP									
LDAP									
Kerberos									
SAML Identity Provider									
Multi Factor Authentica									
✓ III Local User Database									
Control User Groups									
Scheduled Log Export									
💁 Software									
Contect Client									
Dynamic Updates •									
NA Series									
S Licenses									
Support									
Master Key and Diagnostics									
V B Policy Recommendation									
of lot								Activate Windows	
Chick Wr								Go to Settings to activate V	Vindows.
admin   Logout   Last Login Time: (	13/05/2024 03:42:40   Session Expire Ti	ime: 04/04/2024 06:10:	15					Z= Tasks   Langua	👷 🥠 paloalto

#### \* Step 16:

Click "Download Authorization File"

Update License	(!)
Authorization	
Download Authorization File	OK Cancel

#### \* Step 17:

Now under License Management select "Manually upload license key"

🔶 PA-VM	DASHBOARD ACC	MONITOR POLIC	IES OBJECTS	NETWORK	DEVICE		Commit ~	ि मि∽ Q
								S ()
Response Pages	PA-VM					License Management		
Log Settings	Data laward Marsh (	24.2024				Retrieve license kevs from license server		
Server Profiles	Date issued March o	.4, 2024				Activate feature using authorization code		
SNMP Trap	Date expires Never	1104-100				Manually upload license key		
Syslog	Description Standar	3 VM-100				 Deactivate VM		
Email						Upgrade VM capacity		
B Notflow								
RADIUS								
C) SCP								
TACACS+								
LDAP								
terberos								
SAML Identity Provider								
Multi Factor Authentica								
V 🔝 Local User Database								
Users								
School and a second								
Continuero								
GlobalProtect Client								
Ovnamic Updates								
Plugins								
VM-Series								
🔍 Licenses 🔹								
27 Support								
🔂 Master Key and Diagnostics								
Policy Recommendation								
of IoT							Activate Windows	
SaaS 👻							Go to Settings to activate	Windows.
admin   Logout   Last Login Time: C	3/05/2024 03:42:40   Session Ex	pire Time: 04/04/2024 06	:10:15				🚝 Tasks   Lang	uage 🛷 paloalto





#### ✤ 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.

🚺 PA-VM	DASHBOARD ACC MONITOR	POLICI	S OBJECTS NETWORK DEVICE			Ecommit -   🐨 🗣 - Q
	Layout 3 Columns V Widgets V	Last upd	ated 18:12:53			5 mins 🗸 Ġ 🕐
Interfaces		$\mathbb{G}\times$	Logged In Admins	G×	Config Logs	G ×
	1 3 5 7 9 <b>(b)</b> (b) (b) (b) <b>(c)</b> (b) (c) <b>(c)</b> (c) (c) (c) <b>(c)</b> (c) (c) (c) <b>(c)</b> (c) (c) (c) (c) <b>(c)</b> (c) (c) (c) (c) <b>(c)</b> (c) (c) (c) (c) (c) <b>(c)</b> (c) (c) (c) (c) (c) (c) (c) <b>(c)</b> (c)		Admin         From         Client         Session Start           admin         10.1.10.2         Web         03/05/2024 05:10:15           admin         10.1.10.4         Web         03/05/2024 03:42:40	Idle For 00:00:00s 00:32:19s	No data available.	G×
			Data Loge	D V	No locks found	
General Information		$\mathbf{G}\times$	No data available.	G ^	ACC Risk Factor (Last 60 minutes)	G×
Device Name	FW-19				No data found	
MGT IP Address	10.1.10.21		System Logs	G×		'
MGT Netmask	255.255.255.0		Description	Time		
MGT Default Gateway	10.1.10.1		User admin logged in via Web from 10.1.10.2 using https	03/05		
MGT IPv6 Address	unknown		authenticated for user 'admin' From: 10.1.10.2	05:10:14		
MGT IPv6 Link Local Address	fe80::20c:29ff:fe1c:f058/64		authenticated for user authin, Profile 10.1.10.2.	05:10:14		
MGT IPv6 Default Gateway	00-029-110-58		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 05:01:41		
Model	PA-VM		Connection to Update server: updates.paloaltonetworks.com completed	03/05		
Serial #	007051000255314		Connection to Update server: updates.paloaltonetworks.com completed	03/05		
CPU ID	ESX:54060500FFFB8B0F		successfully, initiated by 10.1.10.21	04:31:36		
UUID	564D4A40-7D15-1D90-355A-37CA9E1CF058		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 04:16:02		
VM Cores	2					
VM Memory	8158344					
VM Coposity Tier	VM-100					
VM Mode	VMware ESXI					
Software Version	1101					
GlobalProtect Agent	0.0				Ac	tivate Windows
Application Version	8644-7712					to Settings to activate Windows.





#### ✤ 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.

PA-VM		DASHBOARD	ACC M	ONITOR POLICIES	OBJECTS	NETWORK	DEVICE					l	<u> </u>	
														G (
interfaces	• Q													2 items →
🚧 Zones	0									User-ID			Device-ID	
VLANs     Virtual Wires     Virtual Routers		NAME	ТҮРЕ	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	ENABLE HEADER	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED
1PSec Tunnels		INSIDE	layer3	ethernet1/1						any	none		any	none
SRE Tunnels		OUTSIDE	layer3	ethernet1/2						any	none		any	none
DNS Proxy     Proxy     GlobalProtect     @ Portals     @ Gateways     Gateways     MDM     Clientless Apps														
Clientless App Groups	s a													
<ul> <li>GlobalProtect IPSec C</li> <li></li></ul>	Cryptc 0 0													
Interface Mgmt     Zone Protection     Zone Protection     QoS Profile     LLDP Profile     He BFD Profile     SD-WAN Interface Profile     SD-WAN Interface Profile	•	Ŷ										Activate	Nindows	
-	, 🕀	Add 🕞 Delete	DPDF/CSV									Go to Settin	gs to activate W	lindows.

#### \* 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.

Name	INSIDE	- User Identification ACL	Device-ID ACL
Log Setting	None 🗸	Enable User Identification	Enable Device Identification
Туре	Layer3 🗸		
INTERFACES ^		Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24	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	+ Add Delete
յե		Users from these addresses/subnets will be identified.	Devices from these addresses/subnets will be identified.
Add Delete	e None	Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24	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
	Enable Packet     Buffer Protection     Enable L3 & L4     Header Inspection	Add      Delete Users from these addresses/subnets will not be identified	Add      Delete
			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.

Name OUTSIDE	User Identification ACL	Device-ID ACL
Log Setting None ~	Enable User Identification	Enable Device Identification
Type Layer3		
INTERFACES ^ ethernet1/2	Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24	Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add O Delete	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  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
Enable Packet     Buffer Protection     Enable L3 & L4     Header Inspection	← Add ← Delete Users from these addresses/subnets will not be identified.	Add      Delete  Devices from these addresses/subnets will not be identified.

#### \* 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.

🚺 PA-VM	DASHBOARD		R POLICIES	ОВЈ	ECTS NETWO	DRK DEVICE	:						(	↓ Commit ∨	î⊨ ⊞~ Q
															S ()
Interfaces	Ethernet VLAN	Loopback   Tur	nnel   SD-WAN												
VLANs	Q.(														$_{9 \text{ items}} \rightarrow \times$
Virtual Wires     Virtual Routers     IPSec Tunnels	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		
GRE Tunnels	cm ethernet1/1	<del></del>	PING		10.1.10.100/24	default	Untagged	none	INSIDE		Disabled				
S DNS Proxy	📾 ethernet1/2		PING		20.20.10.10/24	default	Untagged	none	OUTSIDE		Disabled				
Proxy	ethernet1/3	-		m	none	none	Untagged	none	none		Disabled				
GlobalProtect	ethernet1/4			m	none	none	Untagged	none	none		Disabled				
Gateways	cm ethernet1/5			面	none	none	Untagged	none	none		Disabled				
C MDM	ethernet1/6				none	none	Untagged	none	none		Disabled				
Clientless Apps	ethernet1/7			m	none	none	Untagged	none	none		Disabled				
& QoS	and ethernet1/8			m	none	none	Untagged	none	none		Disabled				
😸 LLDP	ethernet1/9				none	none	Untagged	none	none		Disabled				
Network Profiles	and ethernet1/ 7						ontoggeo				Distored				
GlobalProtect IPSec Cryptc     H IKE Gateways															
👌 IPSec Crypto 🔹 🔹															
IKE Crypto															
Monitor e															
Renace Man															
& QoS Profile															
2 LLDP Profile															
🕀 BFD Profile 🔹 🔹													Activate	Mindaus	
SD-WAN Interface Profile													Activate	vvindows	All and accord
) b	+ Add Subinterface	- Delete Delete	F/CSV											ngs to activate i	
admin   Logout   Last Login Time: 0	03/05/2024 03:42:40   S	ession Expire Time: 0	4/04/2024 06:10:1	.5										🚝 Tasks   Langu	📰 и paloalto
														<b>V</b>	betweets





#### ✤ 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)

YPE	Ethernet Interfa	ice (?	) RE
	Interface Name	ethemet1/2	bled
	Comment		bled
	iterface Type	Layer3	bled
	tflow Profile	None	bled
l	Config IPv4	IPv6   SD-WAN   Advanced	bled
	Assign Interface To		bled
	Virtual Router	default 🗸	bled
l	Security Zone		bled
			bled
l		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 Inter	ace	?
Interface Name	ethernet1/1	
Comment		
Interface	Layer3	$\sim$
Netflow Parce	None	$\sim$
Config   IPv4	IPv6   SD-WAN   Advanced	
Type IP 10.1.10.100/2 Vour inside inte	Enable SD-WAN  Static PPPoE DHCP Client	
+ Add - Dele	te ↑ Move Up ↓ Move Down 192.168.2.254/24	
	ОК Сал	:el





#### \* Step 26:

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

6	Ethernet Interf	ace	(?)	REAM
FACE TYPE	Interfece Mene	adh e a sid 14		aled
	Interrace Name	ethemet1/1		Jieu
3	Comment			oled
	Interface Type	Layer3	×	oled
	Netflow Profile	None	~	hole
	Config   IPv4	IPv6   SD-WAN   Advanced		oled
	Link Settings			oled
	Link Speed a	uto Link Duplex auto Link State auto	~	oled
	Other Info A	RP Entries   ND Entries   NDP Proxy   LLDP   DDNS   Cluster	-	bled
	Management Pr	ofile PING	~	bled
	Ν	ITU None		
	Adjust TCP MS	5 — PING		
	IPv4 M	New 👼 Management Profile		
	IPv6 MSS Adjus	tment 60		
		Untagged Subinterface		
		ок	Cancel	

#### \* Step 27:

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

Interface Management Profile     Name Ping     Administrative Management Services     HTTP   HTTPS   Telnet   SSH   twork Services   Ping   HTTP OCSP   SNMP   Response Pages   User-ID   User-ID Syslog Listener-SSL   User-ID Syslog Listener-UDP                  • Add          • Delete    Ex. IPv4 192.168.1.0/24 or IPv6 2001:db8:1231::1 or 2001:db8:1231::164	-wan		0
Name Ping     Administrative Management Services     HTTP   HTTPS   Telnet   SSH   Work Services   Ping   HTTP OCSP   SNMP   Cost Systog Listener-SSL   User-ID Systog Listener-SSL   User-ID Systog Listener-UDP     Delete   Ex IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 201:db8:123:1::1 or 2001:db8:123:1::1 or 2001:db8:10:0 or 2001:db8:0	Interface Management Profile		(?)
Administrative Management Services     HTTP   HTTPS   Telnet   SSH   work Services   Ping   HTTP OCSP   SNMP   Response Pages   User-ID   User-ID Syslog Listener-SSL   User-ID Syslog Listener-UDP     Add C Delete   Ex: IPv4 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/d4	Name Ping		
<ul> <li>HITP</li> <li>HITPS</li> <li>Telnet</li> <li>SSH</li> <li>twork Services</li> <li>Ping</li> <li>HTTP OCSP</li> <li>SNMP</li> <li>Response Pages</li> <li>User-ID</li> <li>User-ID Syslog Listener-SSL</li> <li>User-ID Syslog Listener-UDP</li> <li></li></ul>	Administrative Management Services	PERMITTED IP ADDRESSES	
In this   Telnet   SSH   twork Services   Ping   HTTP OCSP   SNMP   Response Pages   User-ID   User-ID   User-ID Syslog Listener-SSL   User-ID Syslog Listener-UDP     Image: Add Delete   Ex. IPv4 192.168.1.0 r192.168.1.0/24 or IPv6   201:db8:123:1::1 or 2001:db8:123:1::/64			
<pre>     renter     SSH     SSH     rowork Services     Ping     HTTP OCSP     SNMP     Response Pages     User-ID     User-ID Syslog Listener-SSL     User-ID Syslog Listener-UDP</pre>			
Voork Services   Ping   HTTP OCSP   SNMP   Response Pages   User-ID   User-ID Syslog Listener-SSL   User-ID Syslog Listener-UDP     Image: Add Delete   Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 201:db8:123:1::1 or 2001:db8:123:1::/64			
✔ ing			
<ul> <li>Ping</li> <li>HTTP OCSP</li> <li>SNMP</li> <li>Response Pages</li> <li>User-ID</li> <li>User-ID Syslog Listener-SSL</li> <li>User-ID Syslog Listener-UDP</li> <li></li></ul>	twork Services		
HTTP OCSP SNMP Response Pages User-ID User-ID Syslog Listener-SSL User-ID Syslog Listener-UDP → Add → Delete Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64 OK Cancel	Ping		
SNMP         Response Pages         User-ID         User-ID Syslog Listener-SSL         User-ID Syslog Listener-UDP            • Add	HTTP OCSP		
□ Response Pages         □ User-ID         □ User-ID Syslog Listener-SSL         □ User-ID Syslog Listener-UDP	SNMP		
□ User-ID       Syslog Listener-SSL         □ User-ID Syslog Listener-UDP	Response Pages		
□ User-ID Syslog Listener-UDP         → Add → Delete         Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6         2001:db8:123:1::1 or 2001:db8:123:1::/64	User-ID		
Oser-ID Sysiog Listener-ODP	User-ID Syslog Listener-SSL		
<ul> <li>→ Add → Delete</li> <li>Ex. IPv4 192.168.1.0 r 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64</li> <li>OK Cancel</li> </ul>	User-ID Syslog Listener-ODP		
→ Add       → Delete         Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6         2001:db8:123:1::1 or 2001:db8:123:1::/64         OK			
Ex. IPv4 192.168.1.1 or 192.168.10/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64 OK Cancel		+ Add - Delete	
OK Cancel		Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64	
		ОК	Cancel





### \* 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 POLIC	IES OBJECTS NE	TWORK DEVICE				Commit	✓ 1 1 1 1 2 < Q
									G ()
interfaces	• Q								1 item $\rightarrow$ $\times$
Zones	NAME	INTERFACES	CONFIGURATION	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
VLANs	default	ethernet1/1	Static Routes: 2						More Runtime Stats
Virtual Wires     Wirtual Poutore		ethernet1/2	ECMP status: Disabled						
r⊎ IPSec Tunnels	-								
SRE Tunnels									
₹ DHCP									
🕎 DNS Proxy									
🔤 Proxy									
V 😫 GlobalProtect									
O Portals									
Gateways									
Clientless Apps									
Clientless App Groups									
A QoS									
R LLDP									
V 🕞 Network Profiles									
🔒 GlobalProtect IPSec Cr	petc								
☆ IKE Gateways									
IPSec Crypto	•								
HKE Crypto	•								
Monitor	•								
Topo Protoction	•								
2010 Profile									
LLDP Profile									
He BFD Profile	• <b>_</b>							A 12 1 147 1	
SD-WAN Interface Profile	V							Activate Windov	/S
4	, 🕀 Add \ominus Delete 🕲 PDF.	/CSV							
admin   Logout   Last Login Tin	e: 03/05/2024 03:42:40 Session	Expire Time: 04/04/2024 06	:10:15					Z⊟ Tasks	Language 🛛 🦇 paloalto

## \* Step 29:

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

Router Settings   Static Routes   Redistribution Profile   RIP   OSPF   OSPF   OSPFV3   BGP   Multicast     Multicast     Add Oplete     Name defauld     General ECMP     Add Oplete     Add Oplete     Name defauld     Add Oplete     Name defauld     Construction     Static IPv3 Int 30   OSPFv3 Ext 110   Interpretation     Static IPv3 Int 30        Add Oplete	Virtual Router - de	fault			0 🗆
Static Routes Redistribution Profile RIP OSPF OSPFv3 BGP Multicast Multicast OSPFv3 L Comparison OSPFv3 L	Router Settings	Name default			
Redistribution Profile RIP OSPF OSPFV3 BGP Multicast Multicast Administrative Distances Static 10 OSPF V3 10 OSPF V3 10 10 OSPF V3 10 10 0 0 0 0 0 0 0 0 0 0 0 0 0	Static Routes	General ECMP			
RIP OSPF OSPFV3 BGP Multicast  Administrative Distances  Static 10  Static IPv6 10  OSPF Int 30  OSPF Ext 110  OSPF At 110  OSPF Sxt 110  IBGP 200  EBGP 20  RIP 120  RIP 120	Redistribution Profile				
OSPF       ethernet1/1       static       10         OSPFV3       ethernet1/2       0SPF int       30         Multicast       0SPF Ext       110       0SPF int         OSPF 201       30       0SPF Ext       110         OSPF 201       30       0SPF int       30         OSPF 201       10       intermet1/2       0SPF int         Image: Provide the intermet	RIP	INTERFACES A	<ul> <li>Administrative Distance</li> </ul>	ances	
OSPF       10         OSPFv3       BGP         Multicast       0         OSPF int       30         BGP       200         It in the intervent in the interve		ethernet1/1	Static	10	
OSPFv3       0         BGP       0SPF Int       30         Multicast       0       0SPF Ext       110         OSPFV3 Ext       110       0         IBGP       200       0       0         RIP       120       120       120		ethernet1/2	Static IPv6	10	
BGP       Multicast       OSPF Ext       110         Multicast       0       OSPF Y3 Int       30         OSPF Y3 Ext       110       0         IBGP       200       0         EBGP       20       0         RIP       120       120	OSPFv3		OSPF Int	30	
Multicast           Multicast         OSPFv3 Int         30           OSPFv3 Ext         110         IBGP           IBGP         200         IBGP           RIP         120         ID	BGP		OSPF Ext	110	
OSPFV3 Ext       110         IBGP       200         EBGP       20         RIP       120	Multicast		OSPFv3 Int	30	
IBGP       200         EBGP       20         RIP       120			OSPFv3 Ext	110	
EBGP 20 RIP 120 Add ⊙ Delete			IBGP	200	
Image: Weight of the second secon			EBGP	20	
			RIP	120	
<ul> <li>✓ Add ⊖ Delete</li> </ul>					
→ Add					
↔ Add ⊖ Delete		V			
		(+) Add (-) Delete			
OK Cancel					OK Cancel





### \* Step 30:

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

OPA-VM		DASHBOARD A	ACC MONITO	R POLI	CIES OBJECT	S NETWORK	DEVICE						Con	mit 🗸 🛛 🗎 🗇	ta~ C
															GO
Security	• Q(													4	items )→
→ NAT						Sou	irce			Destination					
Policy Based Forwarding		NAME	TAGS	туре	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFIL
Decryption     Decryption	1	ANY	none	universal	any	any	any	any	any	any	any	any	any	Allow	none
Application Override	2	SSH.to.SOF	none	universal		10.1.10.100/24	any	any		20.20.10.10/24	any	any	💥 SSH	⊘ Allow	none
DoS Protection	3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	⊘ Allow	none
🚱 SD-WAN	4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	O Deny	none
Ilicy Optimizer  New App Viewer  Rules Without App Contro  Unused App  Rules Usage  Visues in 30 days  Cussed in 90 days  Cussed	- 0 Is 0 9 See 0 0	-													
ject : Addresses	, -	Add  Delete	Clone 🔞 Overrid	le @ Reven	t 🕢 Enable 🚫	Disable Move -	PDF/CSV	] Highlight Unused	Rules 🗍 View Rule	base as Groups Re	set Rule Hit Coun	Act	ivate Wind o Settings to a Test Policy Match	OWS ctivate Window	

#### \* 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 (1	Ð
General Sour	rce   Destination   Application   Service/URLCategory   Actions	
Name	Policy rule name	٦.
Rule Type	universal (default)	· ]
Description		
Tags		
Group Rules By Tag	None	r
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

Security Policy Rule			0			
General Source Destination Service/URL Category Actions						
Any	Any	select ~	select			
SOURCE ZONE	SOURCE ADDRESS A	SOURCE USER A	SOURCE DEVICE A			
INSIDE						
OUTSIDE						
(+) Add (-) Delete	+ Add - Delete	+ Add Oelete	🛨 Add 😑 Delete			
	Negate					
			OK Cancel			





## 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

Security Policy Rule	Luniuszal Lanu Lanu	lanı lanı lan	()
General Source Destination	Application Service/URL Category Acti	ons	
Any	Any	select 🗸	select 🗸
SOURCE ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DEVICE
		~	
	Address		
	Region           0.0.0.0-0.0.0.0 (Reserved(0.0.0.0-0.0.           -0.0.0.1-0.255.255.255 (Reserved(0.0.00.0.           -10.0.0-10.255.255.255 (Reserved(1.0.0.0.0-0.0.           -100.04.0.0-100.127.255.255 (Reserved(1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0	0.0)) 0.1-0.255.2 10.0.0.0-10. ed(100.64.4 d(127.0.0.0	
🕂 Add \ominus Delete	(⊕), - 169.254.0.0-169.254.255.255 (Reser	ved(169.25 Id ODelete	
_	<ul> <li>N2.16.00-1/2.31.253.253 (Reserved)(192)</li> <li>192.00.0-192.00.255 (Reserved)(192)</li> <li>192.00.2-192.02.255 (Reserved)(192)</li> <li>192.168.00-192.168.255.255 (Reserve</li> <li>192.88.99.0-192.88.99.255 (Reserve</li> <li>198.18.00-198.19.255.255 (Reserve</li> <li>198.51.100.0-198.51.100.255 (Reserve</li> <li>203.0.113.255 (Reserve</li> <li>New  Address  Address Group</li> </ul>	0,1/2,100. 2,00,0-192. 0,2,0-192. ved(192,1£ d(192,88.9* d(198,810. ved(198,51) d(203,0,11.♥ ≫	OK Cancel

#### ✤ 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

Security Policy Rule		any any any	()
General Source Destination Application Servi	ce/URL Category Actions		
select 🗸	Any	any 🗸	
DESTINATION ZONE	DESTINATION ADDRESS	DESTINATION DEVICE	
INSIDE OUTSIDE			
+ Add O Delete	(+) Add (-) Delete	+ Add O Delete	
	Negate	ОК	Cancel





## 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

Security Policy Rule		0
General   Source   Destination   Application   Service	e/URL Category Actions	
select 🗸	Any	any 🗸
DESTINATION ZONE	DESTINATION ADDRESS	
Add      Delete	Address         Domain services           Bogion         0.0.0.0-0.0.0.0 (Reserved(0.0.0.0-0.0.0.0))         0.0.0.1-0.255.255 (Reserved(10.0.0.1-0.255.255.255))           10.0.0.0.10.255.255 (Reserved(10.0.0.0-10.255.255.255)         10.0.0.0-10.255.255 (Reserved(10.0.0.0-10.255.255.255)           10.0.0.0.10.255.255 (Reserved(127.0.0.0-127.255.255)         110.0.0-127.255.255 (Reserved(127.0.0.0-127.255.255)           110.0.0.127.255.255 (Reserved(127.0.0.0-127.255.255)         1127.0.0.0-127.255.255 (Reserved(127.0.0.0-127.255.10.0.0-172.31.255)           110.0.0.127.255.255 (Reserved(127.0.0.0-127.255.255)         1120.0.0-122.0.255)           112.0.0.0.127.255.255 (Reserved(127.0.0.0-127.255.10.0.0-172.31.255)         1120.0.0-127.231.255.255 (Reserved(129.0.0.0-127.231.255)           112.0.0.0.127.215.255 (Reserved(129.0.0.0-127.231.255)         1120.0.0.127.215.255 (Reserved(129.0.0.0-127.231.255)           112.0.0.0.127.215.255 (Reserved(129.0.0.0-127.231.255)         1120.20.255)           112.0.0.0.128.255 (Reserved(129.0.0.0-129.20.255))         1120.20.255)           112.168.0.128.190.2555 (Reserved(129.0.0.128.00-128.20.255))         1120.20.255)           112.168.0.128.19.2555 (Reserved(129.0.189.00-128.20.255))         1120.255 (Reserved(129.0.128.20.258))           112.168.0.128.110.0.255 (Reserved(1298.01.180.0-198.192.20.255))         1120.255 (Reserved(1298.01.180.20.20.250.255)           112.168.0.138.255 (Reserved(1298.01.180.0-198.192.20.255)         1120.255 (Reserved(1298.01.180.20.20.250.255)	Add  Delete OK Cancel

#### \* 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

General   Source   Destination   Application   Service/URL Category   Actions	
select v	Z Any
SERVICE A	URL CATEGORY A
Service - service-http - service-https - Splunk Forwader - SSH - Web Access Splunk New & Service Group	
Add ODelete	Add      Delete     OK     Cancel







- 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	0
Name	
Description	
Protocol	O TCP O UDP
Destination Port	[>=0]
Source Port	[>= 0]
	Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)
Session Timeout	O 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	POLICI	ES OBJECTS NETWORK DEVICE				Commit 🗸	1 în №a• Q
	Layout 3 Columns 🗸 🖬 Widgets 🗸	Last upo	lated 19:47:19				5 mi	ns v G 🕐
Interfaces		G×	Logged In Admins	G×	Config Logs		- ጎ ጉ	G×
	1 3 5 7 9 m m m m m m m m m 2 4 6 8		Admin         From         Client         Session Start           admin         Console         CLI         03/05/2024 06:22:26           admin         10.1.10.2         Web         03/05/2024 05:10:15	Idle For 00:20:48s 00:00:00s	Command delete delete	Path vsys vsys1 rulebase security rules Splunk Forwader vsys vsys1 rulebase security	Admin admin admin	Time 03/05 06:43:42 03/05
General Information		G×	Data Logs No data available.	G×	delete	rules Splunk Rules vsys vsys1 rulebase security rules SSH	admin	06:43:36 03/05 06:43:26
Device Name MGT IP Address	FW-19 10.1.10.21		System Logs	G X	delete	vsys vsys1 rulebase security rules HTTPS vsys vsys1 rulebase security	admin	03/05 06:43:22 03/05
MGT Netmask MGT Default Gateway	255.255.255.0 10.1.10.1		Description Connection to Update server: updates.paloaltonetworks.com completed	Time 03/05	move	rules ANY disabled vsys vsys1 rulebase security rules ANY	admin	06:07:58 03/05 06:07:45
MGT IPv6 Address MGT IPv6 Link Local Address	unknown fe80::20c:29ff:fe1c:f058/64		successfully, initiated by 10.1.10.21 User admin logged in via CLI from Console	06:31:43 03/05 06:22:26	move	vsys vsys1 rulebase security rules ANY	admin	03/05 06:07:42
MGT IPv6 Default Gateway MGT MAC Address	00:0c:29:1c:f0:58		authenticated for user 'admin'. From: Console or telnet.	03/05 06:22:25	set	vsys vsys1 rulebase security rules ANY vsys vsys1 rulebase security	admin	03/05 06:07:42 03/05
Model Serial #	PA-VM 007051000255314		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21 Auto update agent found no new IoT updates	03/05 06:16:23 03/05	move	rules SSH.to.SOF vsys vsys1 rulebase security rules HTTPS	admin	06:06:25 03/05 06:06:19
CPU ID UUID	ESX:54060500FFFB8B0F 564D4A40-7D15-1D90-355A-37CA9E1CF058		Failed to check IoT content upgrade info due to Unknown error	06:08:13 03/05 06:08:13	Locks			S ×
VM Cores VM Memory	2 8158344 VM-100		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.1.10.21	03/05 06:08:13	No locks found			
VM Capacity Tier VM Mode	6.5 GB VMware ESXi		connection to Update server: updates paloaltonetworks.com completed successfully, initiated by 10.1.10.21 Connection to Update server: updates paloaltonetworks.com completed upgates fills, initiated by 10.1.10.21	03/05 06:01:38 03/05	ACC Risk Factor (Last No data found	60 minutes)		ß×
Software Version GlobalProtect Agent	11.0.1 0.0.0		Successiony, initiated by 20.2.20.21	03961/		Activa	te Windows	
Application Version	8644-7712	/2024.04-	10-15			Go to Se	ettings to activate	Windows.





## Step 39:

Select "commit"

Commit							
Doing a commit will overwrite the running configuration with the commit scope.							
Commit All Changes Ocommit Changes Made By:(1) admin							
COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS			
<ul> <li>policy-and-objects</li> </ul>	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							
			Commit	Cancel			
				Cancer			