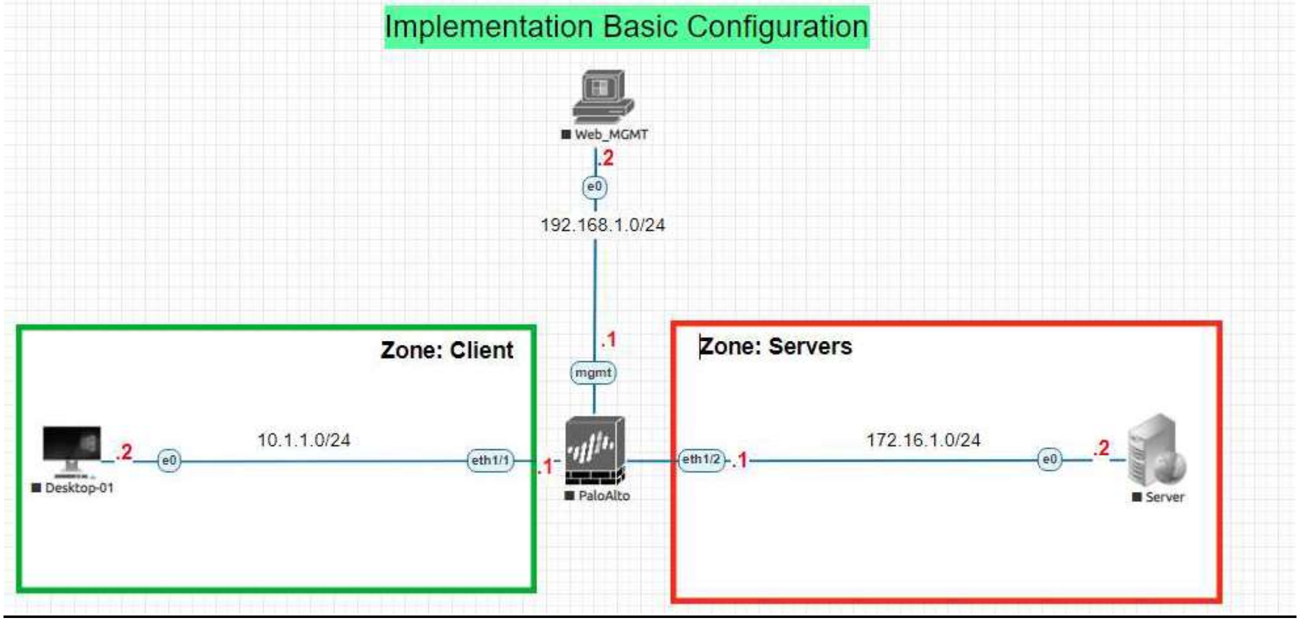
LAB – Implementation Basic Configuration

*** LAB Topology:**



LAB Objective:

- Build the network and configuration basic Firewall PaloAlto
- Configuration Policies at Firewalls PaloAlto:
  - Desktop-01 can ping to Server success.
  - Desktop-01 can ssh to Server success

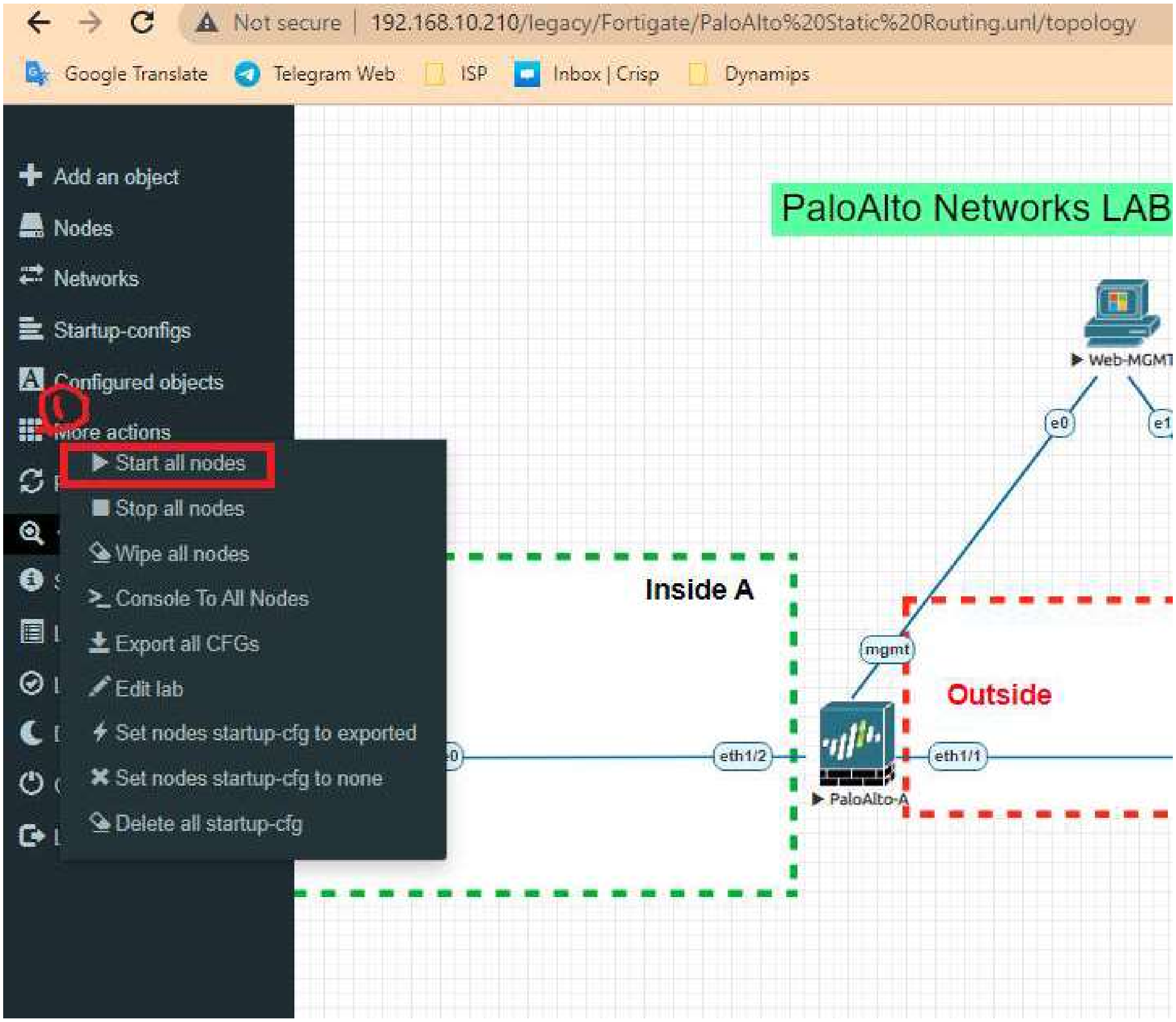
Detail information

List Device	***Interface***	***IP***
Desktop-01	Ethernet 1	IP: 10.1.1.2/24 GW: 10.1.1.1
Server	Ethernet 1	IP: 172.16.1.2/24 GW: 172.16.1.1
Firewall PaloAlto	MGMT	192.168.1.1/24
	Ethernet 1/1 ZONE: Clients	10.1.1.1/24
	Ethernet ½ ZONE: Servers	172.16.1.1/24
Web_MGMT	Ethernet 1	IP: 192.168.1.2/24 GW: 192.168.1.1

Guild Step-by-Step:

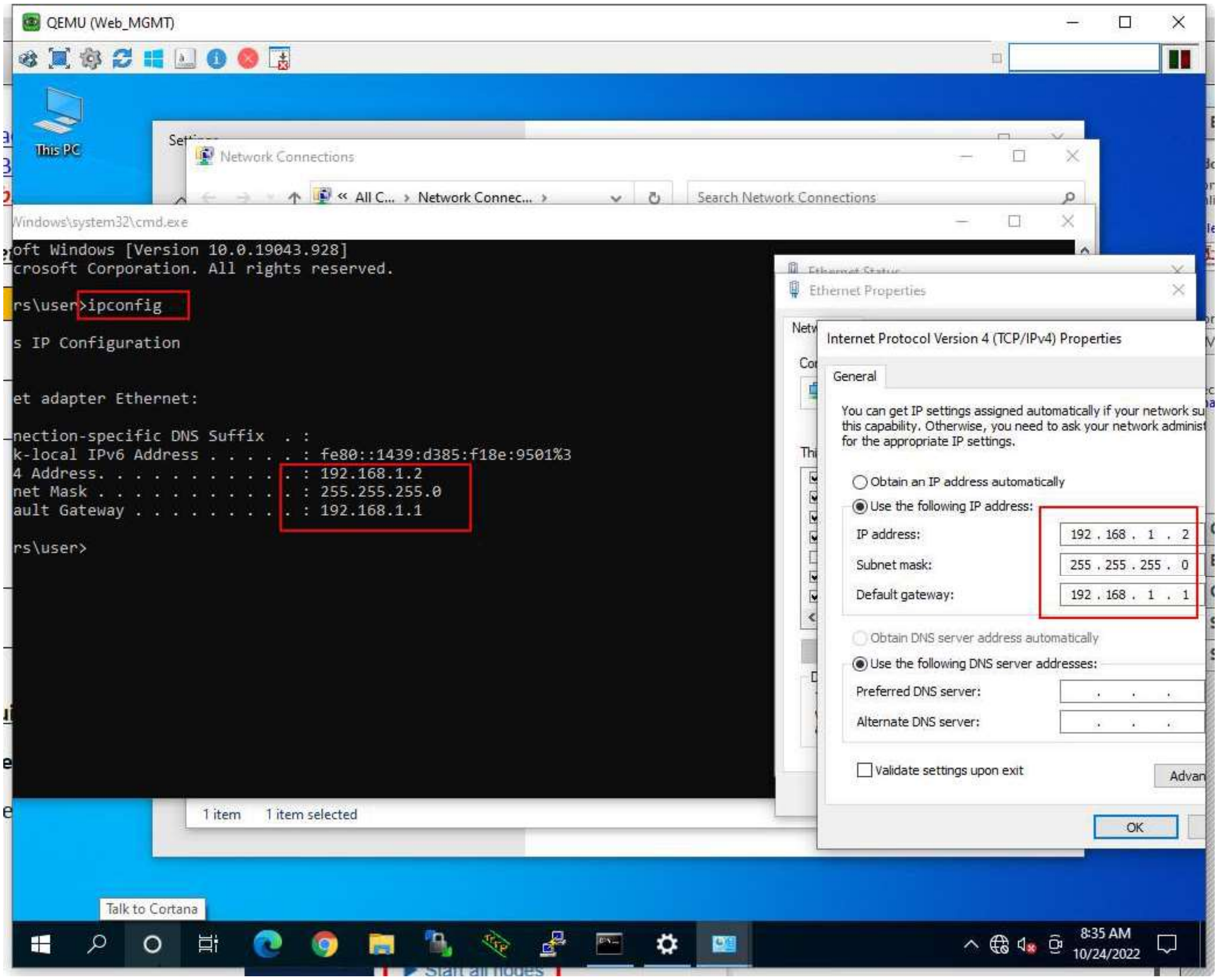
Step 1: Turn on Lab Device

Menu > Setup Nodes > Start all nodes


Not secure | 192.168.10.210/legacy/Fortigate/PaloAlto%20Static%20Routing.unl/topology
Google Translate
Telegram Web
ISP
Inbox | Crisp
Dynamips
Add an object
Nodes
Networks
Startup-configs
Configured objects
More actions
Start all nodes
Stop all nodes
Wipe all nodes
Console To All Nodes
Export all CFGs
Edit lab
Set nodes startup-cfg to exported
Set nodes startup-cfg to none
Delete all startup-cfg
PaloAlto Networks LAB
Web-MGMT
e0
e1
Inside A
mgmt
Outside
eth1/2
eth1/1
PaloAlto-A

Step 2: Verify status of devices, Device need have "Blue" color as picture

- Double click into "Desktop-01" and add the desired ip (table ip)



```
oft Windows [Version 10.0.19043.928]
crosoft Corporation. All rights reserved.

rs\user>ipconfig

s IP Configuration

et adapter Ethernet:

nection-specific DNS Suffix  . :
k-local IPv6 Address . . . . . : fe80::1439:d385:f18e:9501%3
4 Address. . . . . . . . . . . : 192.168.1.2
net Mask . . . . . . . . . . . : 255.255.255.0
ault Gateway . . . . . . . . . : 192.168.1.1

rs\user>
```

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network su
this capability. Otherwise, you need to ask your network adminis
for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

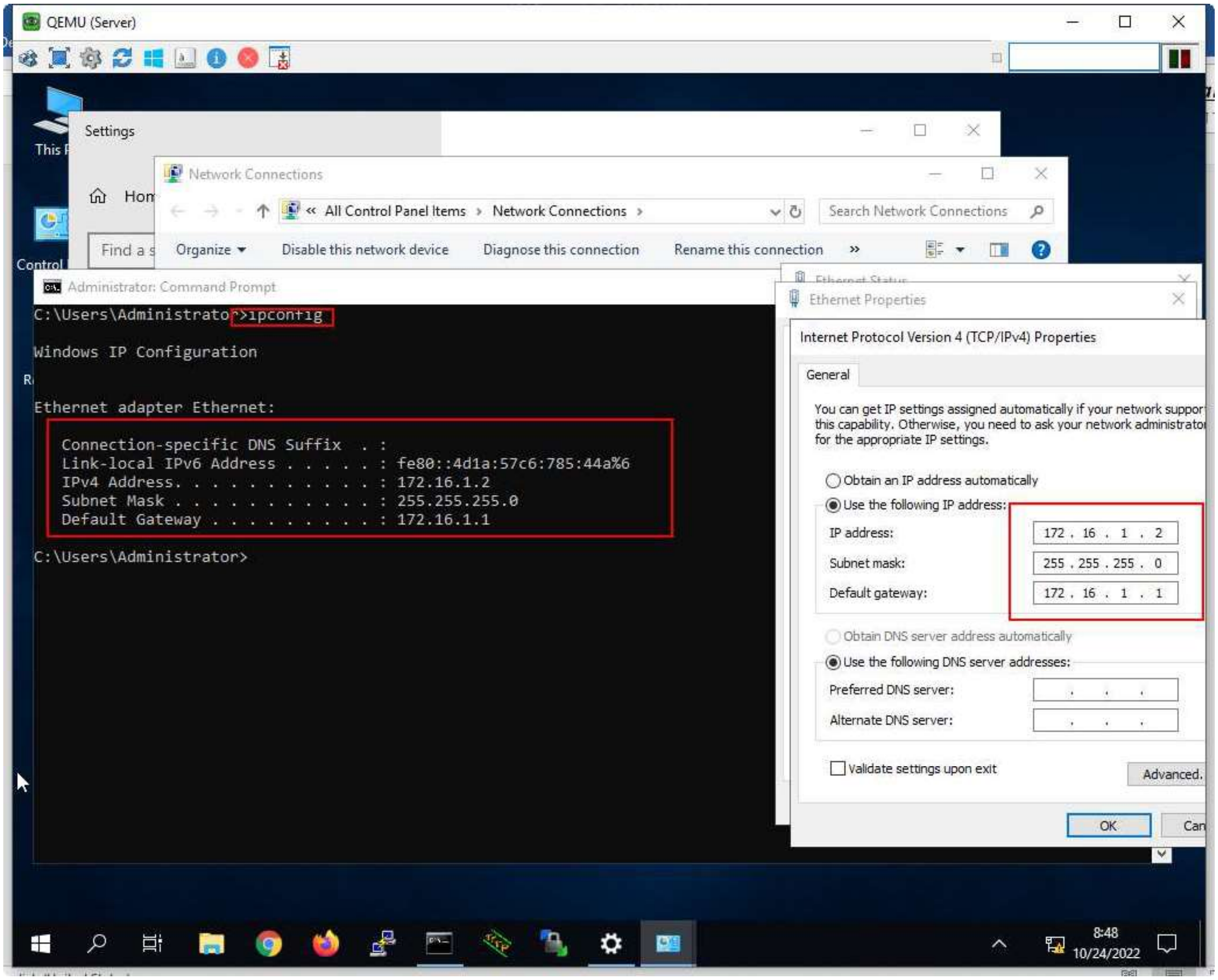
Advan

OK

➔ So, you can see Desktop have IP as requirement

step 4: verify configuration of "Server"

Login information Username: administrator / Password: Test123



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4d1a:57c6:785:44a%6
   IPv4 Address. . . . . . . . . . . : 172.16.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.1.1

C:\Users\Administrator>
```

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network suppor this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 172 . 16 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 16 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

Advanced.

OK Can

Type command: "ipconfig"

➔ So, you can see Server have IP as requirement

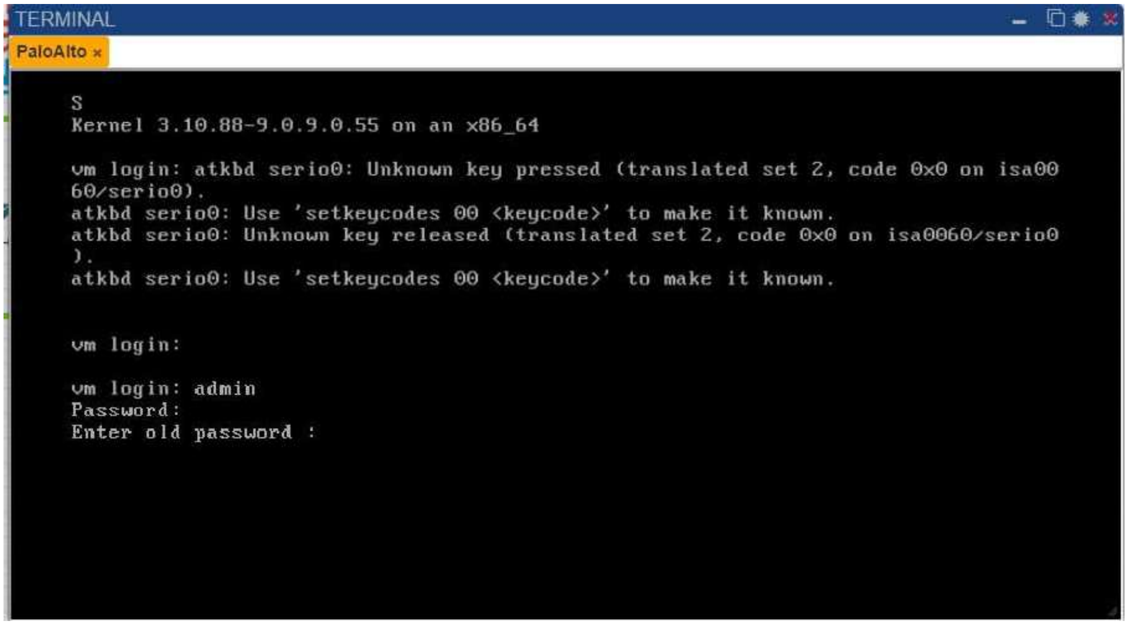
>>>>> Configuration PaloAlto via CLI <<<<<

Step 4: access into Paloalto's CLI

Username: admin

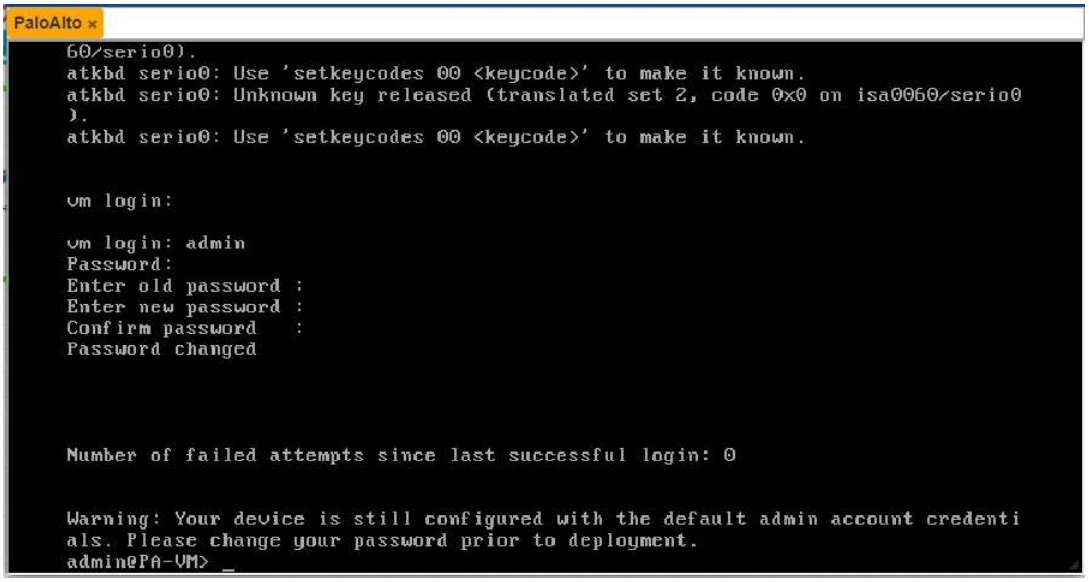
Password: admin

When you login success into firewall Paloalto via CLI, Device request you must be change admin password as following.



```
S
Kernel 3.10.88-9.0.9.0.55 on an x86_64

vm login: atkbd serio0: Unknown key pressed (translated set 2, code 0x0 on isa00
60/serio0).
atkbd serio0: Use 'setkeycodes 00 <keycode>' to make it known.
atkbd serio0: Unknown key released (translated set 2, code 0x0 on isa0060/serio0
).
atkbd serio0: Use 'setkeycodes 00 <keycode>' to make it known.


vm login:

vm login: admin
Password:
Enter old password :
```

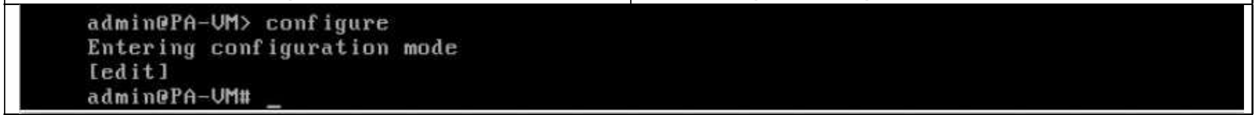
You should be take note <<password>>. You need it for login with Firewalls PaloAlto via GUI.



```
60/serio0).
atkbd serio0: Use 'setkeycodes 00 <keycode>' to make it known.
atkbd serio0: Unknown key released (translated set 2, code 0x0 on isa0060/serio0
).
atkbd serio0: Use 'setkeycodes 00 <keycode>' to make it known.


vm login:

vm login: admin
Password:
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 credenti
als. Please change your password prior to deployment.
admin@PA-VM> _
```

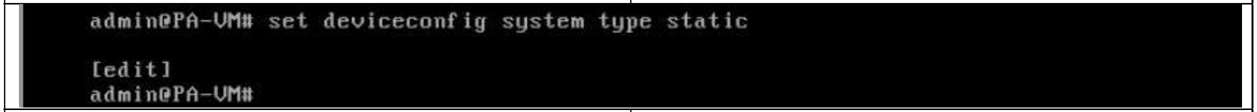
Bước 5: set IP MGMT PaloAlto Firewall

Command	***Detail***
admin@PA-VM>	// User mode
admin@PA-VM> configure	// moving to configuration mode



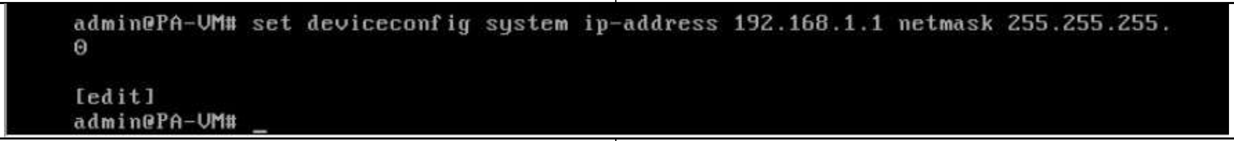
```
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# _
```

admin@PA-VM# set deviceconfig system type static	// change mode from DHCP Client to Static



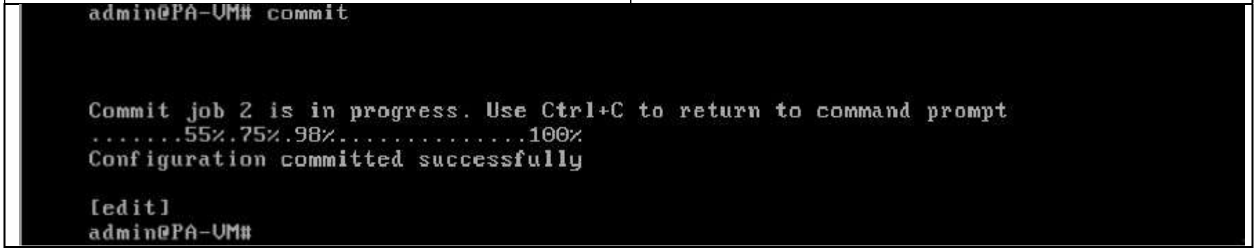
```
admin@PA-VM# set deviceconfig system type static

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

admin@PA-VM# set device config system ip-address 192.168.1.1 netmask 255.255.255.0	// Set IP Address for Interface MGMT



```
admin@PA-VM# set deviceconfig system ip-address 192.168.1.1 netmask 255.255.255.
0

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

admin@PA-VM# commit	// apply configuration to running-config.xml

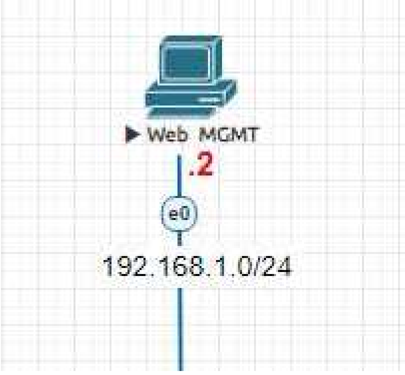


```
admin@PA-VM# commit



Commit job 2 is in progress. Use Ctrl+C to return to command prompt
.......55%.75%.98%.............100%
Configuration committed successfully

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

>>>>> Configuration PaloAlto firewall via GUI <<<<<

Bước 6:

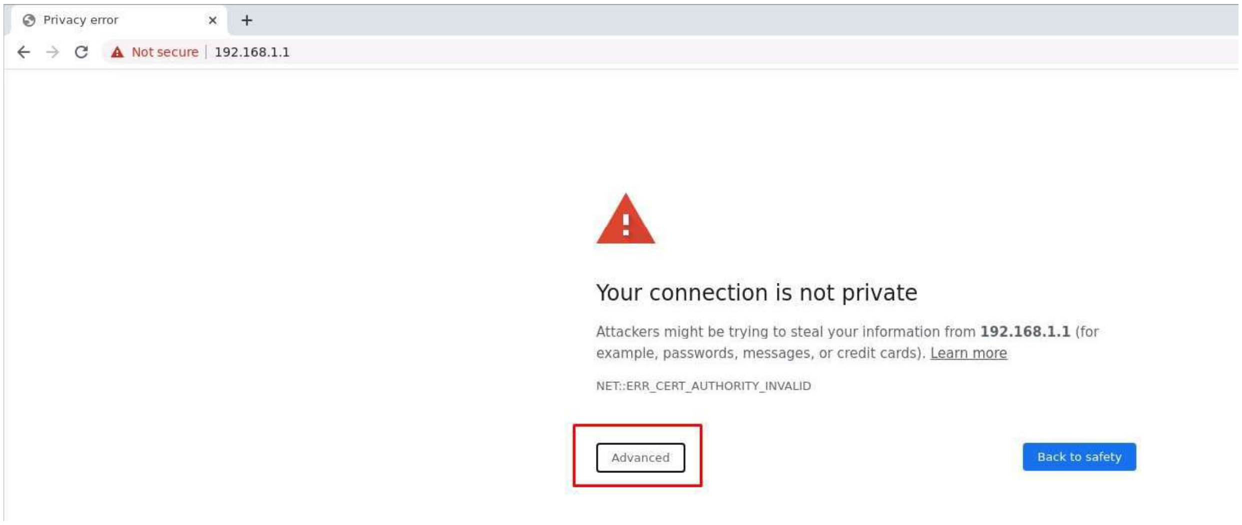
- Double-click “Web_MGMT”



- Login into Firewall GUI via Web browser with address as following:

https://192.168.1.1

- When you access by https into device have a issue with certification, we need bypass it. Select “Advanced

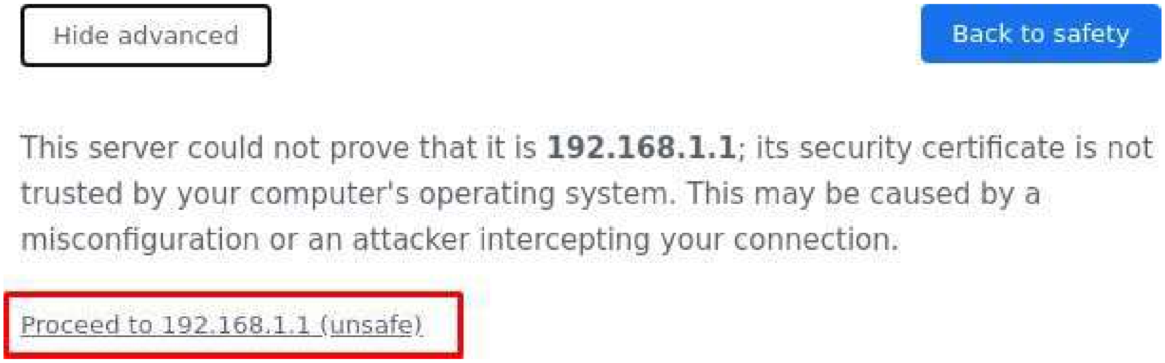


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

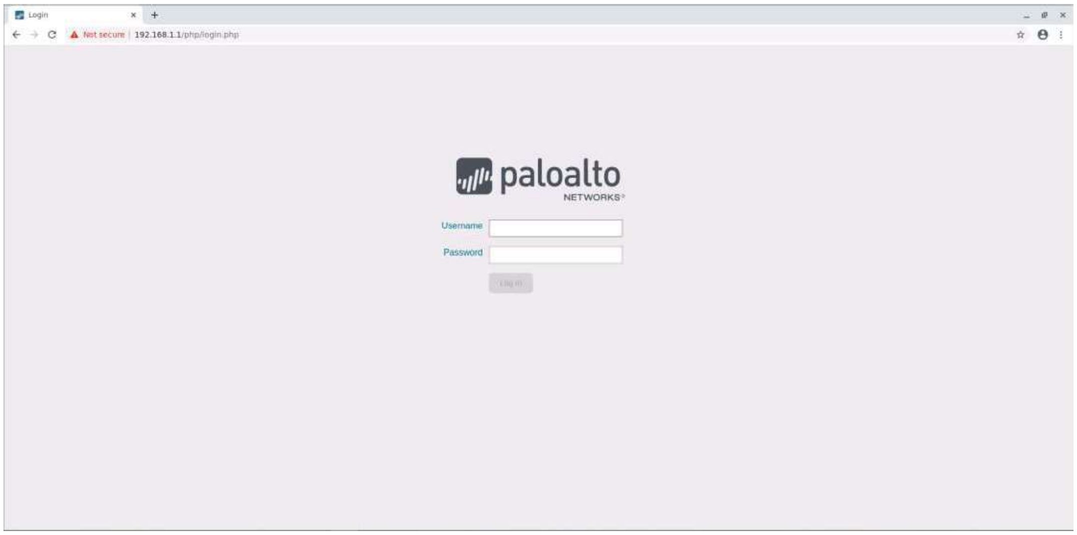
- click *“proceed to 192.168.1.1 (unsafe)”*



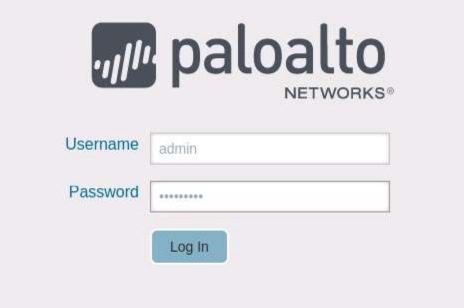
This server could not prove that it is **192.168.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.1 (unsafe)

- This is login page into PaloAlto Firewalls via GUI



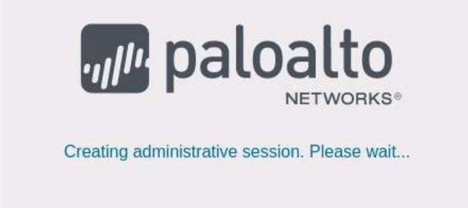
Step 7: Login into firewall with **<<password>>** you have changed at “step4”



Username admin

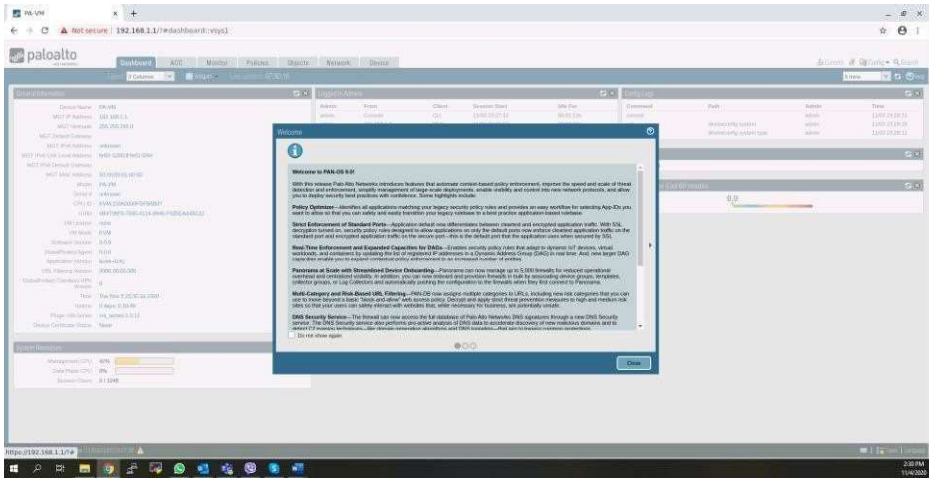
Password •••••••••

- click “login”, and waiting here



Creating administrative session. Please wait...

- and you can see Web Interface of Paloalto as picture



Welcome

Welcome to PAN-OS 9.0!

With this release Palo Alto Networks introduces features that automate content-based policy enforcement, improve the speed and scale of threat detection and enforcement, simplify management of large-scale deployments, enable visibility and control into new network protocols, and allow you to deploy security best practices with confidence. Some highlights include:

Policy Optimizer—Identifies all applications matching your legacy security policy rules and provides an easy workflow for selecting App-IDs you want to allow so that you can safely and easily transition your legacy rulebase to a best practice application-based rulebase.

Strict Enforcement of Standard Ports—Application default now differentiates between cleartext and encrypted application traffic. With SSL decryption turned on, security policy rules designed to allow applications on only the default ports now enforce cleartext application traffic on the standard port and encrypted application traffic on the secure port—this is the default port that the application uses when secured by SSL.

Real-Time Enforcement and Expanded Capacities for DAGs—Enables security policy rules that adapt to dynamic IoT devices, virtual workloads, and containers by updating the list of registered IP addresses in a Dynamic Address Group (DAG) in real time. And, new larger DAG capacities enable you to expand contextual policy enforcement to an increased number of entities.

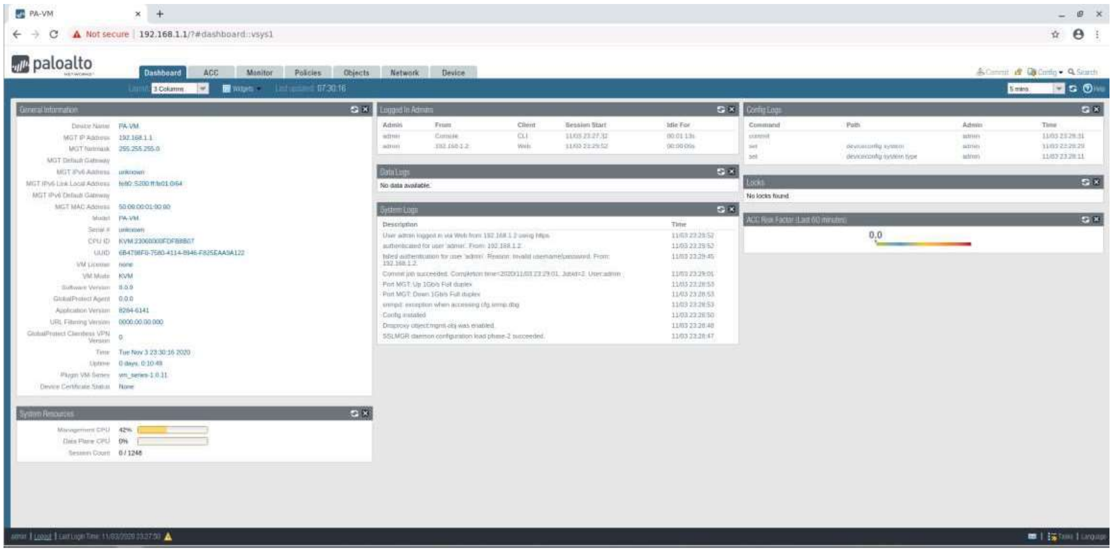
Panorama at Scale with Streamlined Device Onboarding—Panorama can now manage up to 5,000 firewalls for reduced operational overhead and centralized visibility. In addition, you can now onboard and provision firewalls in bulk by associating device groups, templates, collector groups, or Log Collectors and automatically pushing the configuration to the firewalls when they first connect to Panorama.

Multi-Category and Risk-Based URL Filtering—PAN-OS now assigns multiple categories to URLs, including new risk categories that you can use to move beyond a basic "block-and-allow" web access policy. Decrypt and apply strict threat prevention measures to high-and medium-risk sites so that your users can safely interact with websites that, while necessary for business, are potentially unsafe.

DNS Security Service—The firewall can now access the full database of Palo Alto Networks DNS signatures through a new DNS Security service. The DNS Security service also performs pro-active analysis of DNS data to accelerate discovery of new malicious domains and to [illegible]

□ Do not show again

- check "Do not show again" > click "Close"



General Information

Device Name	PA-VM
MGT IP Address	192.168.1.1
MGT Netmask	255.255.255.0
MGT Default Gateway	
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::5200:ff:fe01:0/64
MGT IPv6 Default Gateway	
MGT MAC Address	50:00:00:01:00:00
Model	PA-VM
Serial #	unknown
CPU ID	KVM:23068000FDFBBB07
UUID	6B4798F8-7580-4114-8946-F825EAA9A122
VM License	none
VM Mode	KVM
Software Version	9.0.9
GlobalProtect Agent	0.0.0
Application Version	8284-6141
URL Filtering Version	0000.00.00.000
GlobalProtect Clientless VPN Version	0
Time	Tue Nov 3 23:30:16 2020
Uptime	0 days, 0:10:49
Plugin VM-Series	vm_series-1.0.11
Device Certificate Status	None

System Resources

Management CPU	42%
Data Plane CPU	0%
Session Count	0 / 1248

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	Console	CLI	11/03 23:27:32	00:01:13s
admin	192.168.1.2	Web	11/03 23:29:52	00:00:00s

Data Logs

No data available.

System Logs

Description	Time
User admin logged in via Web from 192.168.1.2 using https	11/03 23:29:52
authenticated for user 'admin'. From: 192.168.1.2	11/03 23:29:52
failed authentication for user 'admin'. Reason: Invalid username/password. From: 192.168.1.2.	11/03 23:29:45
Commit job succeeded. Completion time=2020/11/03 23:29:01. JobId=2. User:admin	11/03 23:29:01
Port MGT: Up 1Gb/s Full duplex	11/03 23:28:53
Port MGT: Down 1Gb/s Full duplex	11/03 23:28:53
snmpd: exception when accessing cfg.snmp.dbg	11/03 23:28:53
Config installed	11/03 23:28:50
Dnsproxy object:mgmt-obj was enabled.	11/03 23:28:48
SSLMGR daemon configuration load phase-2 succeeded.	11/03 23:28:47

Config Logs

Command	Path	Admin	Time
commit		admin	11/03 23:28:31
set	deviceconfig system	admin	11/03 23:28:29
set	deviceconfig system type	admin	11/03 23:28:11

Locks

No locks found.

ACC Risk Factor (Last 60 minutes)

0.0