

## Chapter 11 Pre-task 2, Palo Alto and Fortinet Firewall Installation on GNS3

<b>File name:</b>	Ch11_Pre-task2_PaloAlto_and_Fortinet_Firewall_Installation_on_GNS3.pdf
<b>Version:</b>	1.1
<b>Created on:</b>	26/June/2023
<b>Download URL:</b>	<a href="https://github.com/ansnetauto/apress_ansnetauto">https://github.com/ansnetauto/apress_ansnetauto</a>

### About this document:

Welcome to the software installation guide for the Apress book, "**Introduction to Ansible Network Automation: The Practical Primer**". This guide has been created by the authors as supplementary material to the book, but it is not part of the actual book itself. **The content has been borrowed from the prequel book, "Introduction to Python Network Automation: The First Journey" written by Brendan Choi in 2021.** Its purpose is to provide clear and concise instructions to assist readers in installing the necessary software required to follow the examples and exercises.

By following the steps outlined in this guide, you will be able to set up the required software for Ansible/Python network automation and begin exploring the concepts while engaging in the practical exercises covered in the book. Please note that this guide is not intended to serve as a comprehensive resource on network automation or Ansible, but rather as a focused guide designed to help you get started quickly and easily.

If you encounter any questions or issues during the installation process, please do not hesitate to reach out to the authors or refer to the resources listed in the guide. We hope this guide proves helpful in your journey toward mastering Ansible/Python network automation.

### Required files for installation:

Description	File name	File Size
<b>Palo Alto Firewall:</b>	Pan-vm-fw.gns3a	8KB
	PA-VM-KVM-10.1.0.qcow2	3.4GB
<b>Fortinet Firewall:</b>	Fortigate.gns3a	22KB
	empty30G.qcow2	192.5KB
	FGT_VM64_KVM-v7.2.4.F-build1396-FORTINET.out.kvm.qcow2	90.8MB
<b>Internet connection:</b>	Yes	n/a

**Warning!** The software used in this guide may include a combination of open-source and proprietary software. Readers can search for most of the open-source software on the internet. However, the authors are unable to legally provide the proprietary software. Please ensure that you acquire the proprietary software through authorized channels.

## Contents

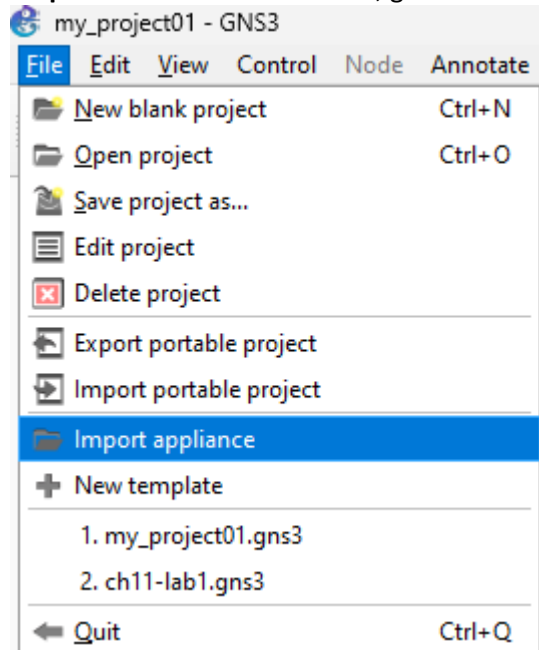
Chapter 11 Pre-task 2, Palo Alto and Fortinet Firewall Installation on GNS3.....	1
About this document: .....	1
Required files for installation:.....	1
Palo Alto PA-VM installation on GNS3 .....	3
Fortinet FortiGate installation on GNS3 .....	16
Palo GNS3 files download links:.....	21
FortiGate GNS3 files download links: .....	21

In this installation guide, you will install two types of virtual Firewalls, first, Palo Alto's PA-VM and second Fortinet's FortiGate. The installation of these devices on GNS3 is no different from installing Cisco or Juniper devices.

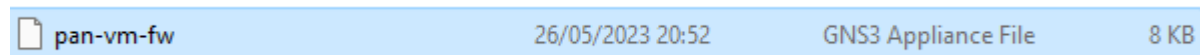
### Palo Alto PA-VM installation on GNS3

First, let's install Palo Alto's PA-VM with an IP address of 192.168.127.30/24. We will only do the installation here. Then, we will continue with the initial configuration and validation in the book.

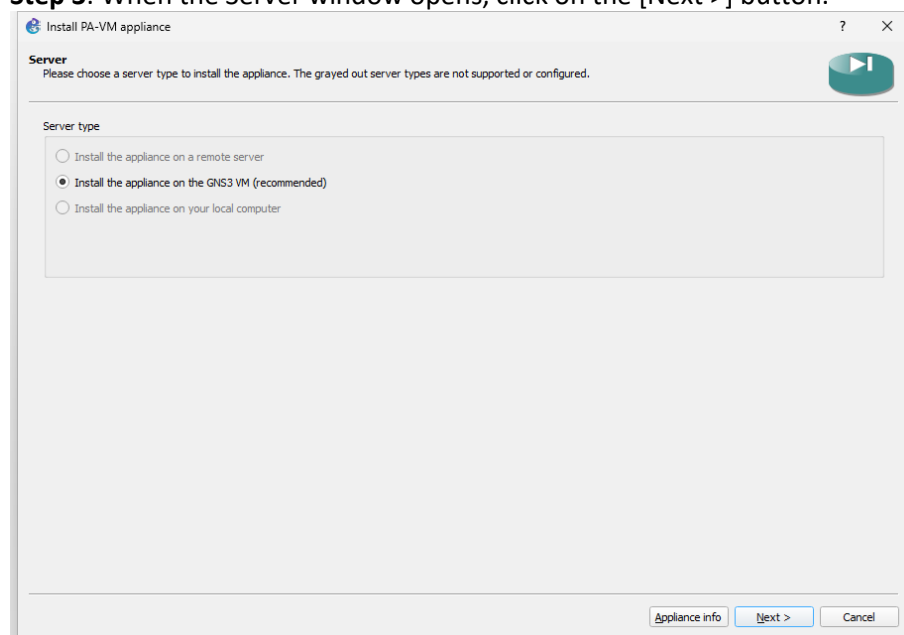
**Step 1:** On GNS3 main window, go to File > Import appliance.



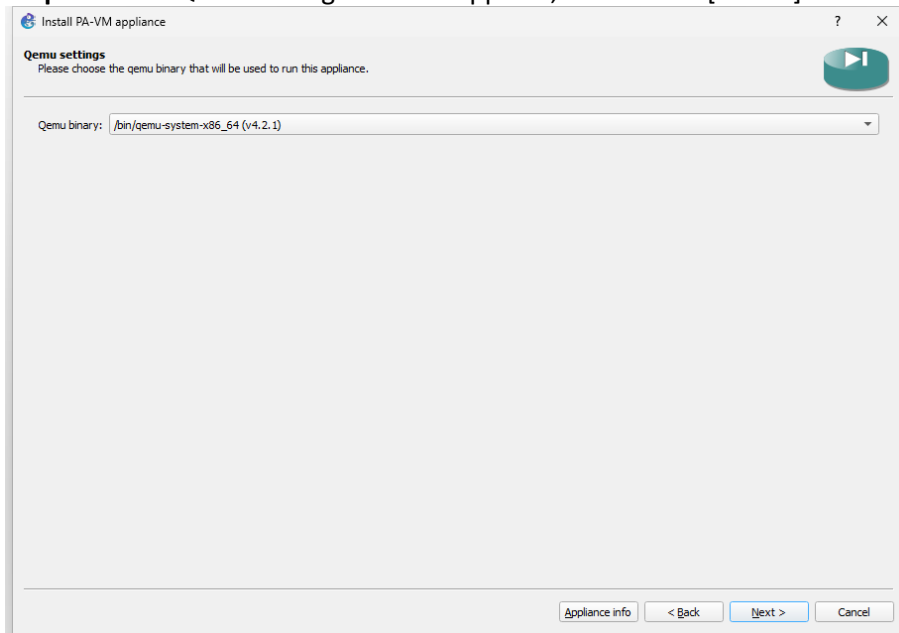
**Step 2:** Navigate to your Downloads folder and locate the file named 'pand-vm-fw.gns3a'. Select the file to open in the GNS3 Import appliance.



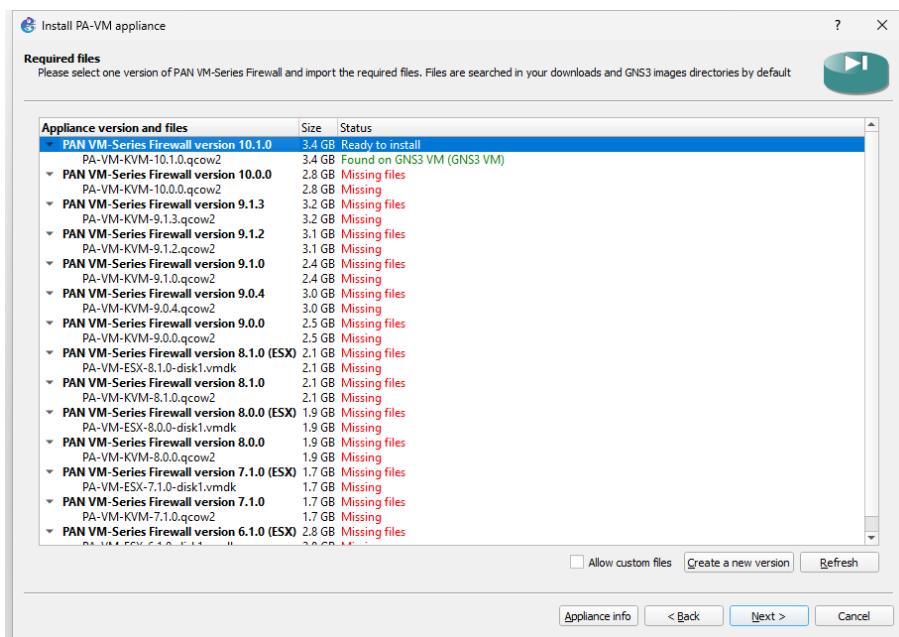
**Step 3:** When the Server window opens, click on the [Next >] button.



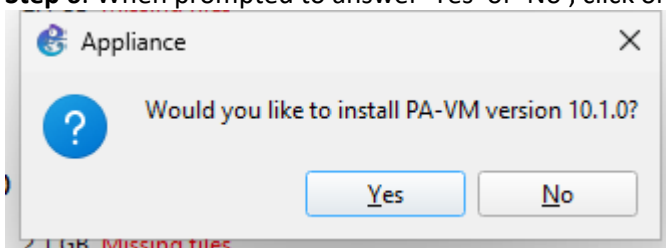
**Step 4:** When Qemu settings window appears, click on the [Next >] button again.



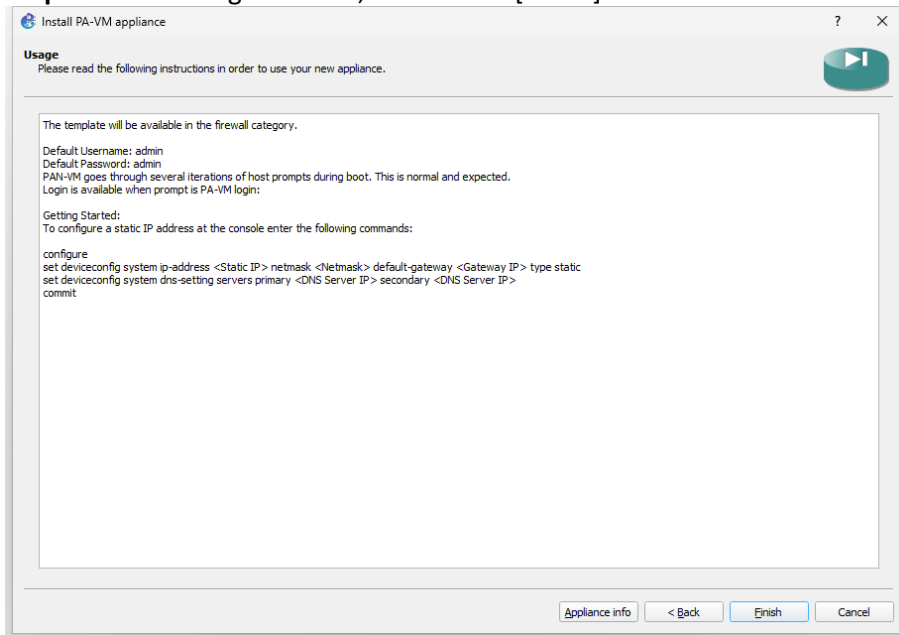
**Step 5:** If you have placed the correct PA-VM image under the Downloads folder, it will automatically detect your PA-VM image. The PA-VM image used in this example is PA-VM-KVM-10.1.0.qcow2. Highlight the populated version of PA-VM and click on the [Next >] button.



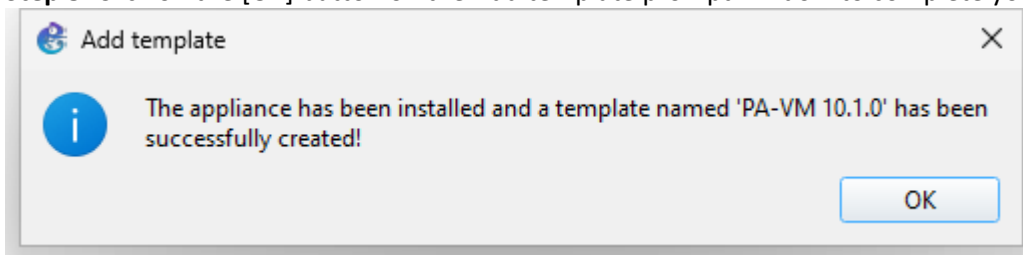
**Step 6:** When prompted to answer 'Yes' or 'No', click on the [Yes] button.



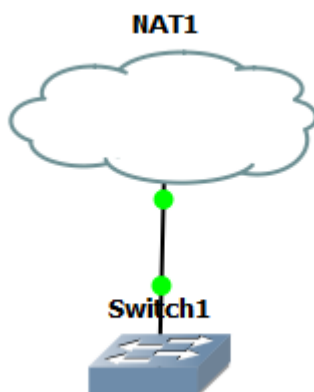
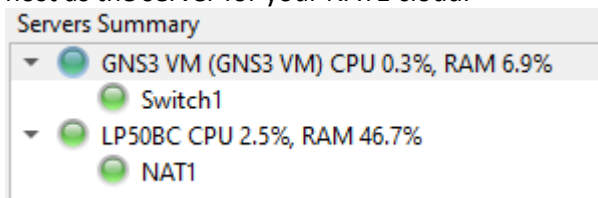
**Step 7:** On the Usage window, click on the [Finish] button.



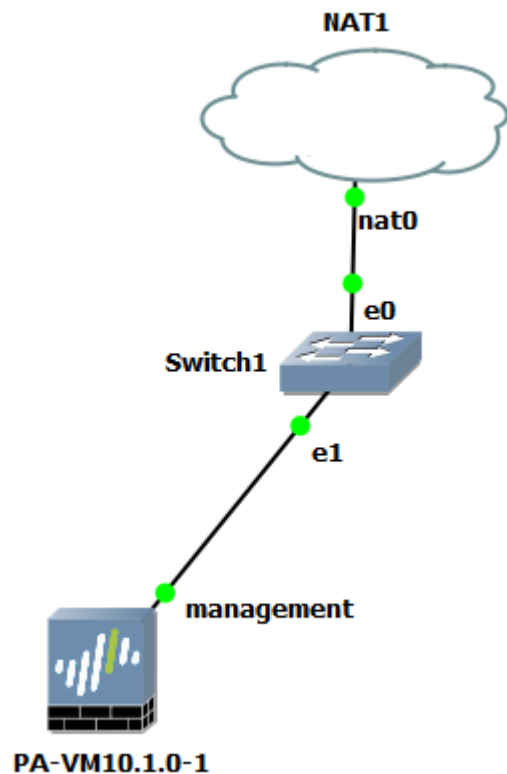
**Step 8:** Click on the [OK] button on the Add template prompt window to complete your installation.



**Step 9:** Drag and drop a NAT cloud and a GNS3's dummy Switch to the Topology Canvas. When you drop these items, make sure you select the GNS3 VM as the server for your Switch1 and your PC host as the server for your NAT1 cloud.



**Step 10:** Now go to All Devices and locate the PA-VM 10.1.0 icon and drag-n-drop to the canvas and connect the PA-VM's management interface to the Switch 1's Ethernet 1. Place the mouse cursor on the PA-VM, use the right-click, and then select the power on button.



**Step 11:** Double-click on the PA-VM icon to open the console, so you know it is booting up properly.

```

PA-VM10.1.0-1 - PuTTY
[ 3.398135] random: fast init done
[ 3.667400] EXT4-fs (vda2): recovery complete
[ 3.677265] EXT4-fs (vda2): mounted filesystem with ordered data mode. Opts:
(null)
[ 3.690532] VFS: Mounted root (ext3 filesystem) readonly on device 253:2.
[ 3.708489] devtmpfs: mounted
[ 3.721627] Freeing unused kernel memory: 2408K
[ 3.731812] Write protecting the kernel read-only data: 22528k
[ 3.750801] Freeing unused kernel memory: 2012K
[ 3.761804] Freeing unused kernel memory: 1496K
[ 3.932220] EXT4-fs (vda2): re-mounted. Opts: (null)
[ 3.983662] EXT4-fs (vda2): re-mounted. Opts: (null)
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.127.138 netmask 255.255.255.0 broadcast 192.168.127.255
    inet6 fe80::ec7:f7ff:fe23:0 prefixlen 64 scopeid 0x20<link>
    ether 0c:c7:f7:23:00:00 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 342 (342.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7 bytes 782 (782.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Masterd started successfully

PA-VM login: █
    
```

**Step 12:** Starting with PAN-OS 9.0.4, administrators must change **the default administrator password (admin/admin)** on the first admin account login on your device. Please go ahead and change this password and make sure you save the password for future reference and use. You have to get to the “PA-VM login:” prompt to log in and change the password.

[...omitted for brevity]

Masterd started successfully

vm login: **admin**

'cfg.general.need-acknowledgement-to-login': NO\_MATCHES

Password: **admin**

Login incorrect

PA-HDF login: **admin**

Password: **admin**

Login incorrect

PA-VM login: **admin**

Password: **admin**

Last login: Wed May 31 01:53:18 on ttyS0

Enter old password : **admin**

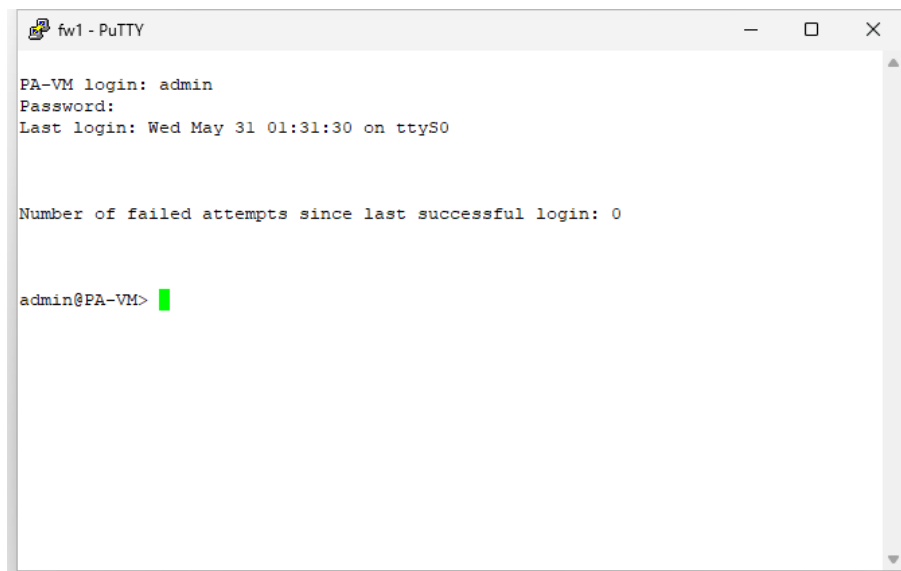
Enter new password : \*\*\*\*\*

Confirm password : \*\*\*\*\*

Password changed

Refer to this link for a password update on the first login:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=ka10g000000CloQCAS>



```
fw1 - PuTTY
PA-VM login: admin
Password:
Last login: Wed May 31 01:31:30 on ttyS0

Number of failed attempts since last successful login: 0

admin@PA-VM>
```

**Step 13:** We can now configure the management interface on our Palo Alto Network Firewalls. It is set to DHCP by default. Once we have configured the management IP, we should be able to log in via ssh and web GUI.

```
admin@PA-VM > configure
Entering configuration mode
[edit]
admin@ PA-VM # set deviceconfig system type static

[edit]
admin@ PA-VM # set deviceconfig system ip-address 192.168.127.31 netmask 255.255.255.0
default-gateway 192.168.127.2 dns-setting servers primary 192.168.127.2 secondary 8.8.8.8

[edit]
admin@ PA-VM # commit

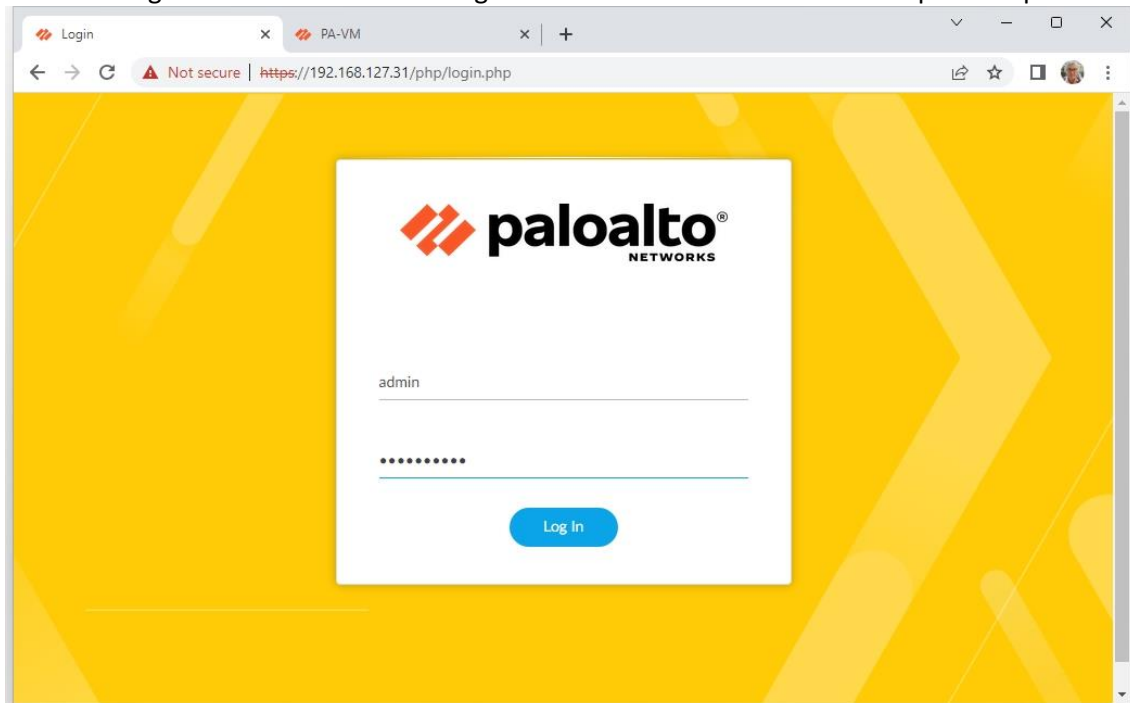
Commit job 3 is in progress. Use Ctrl+C to return to command prompt
.....55%70%98%.....100%
Configuration committed successfully
```

**Refer to this link for configuring the management interface IP of the firewall:**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK>

**NOTE:** The succeeding steps will include configurations only related to our example in chapter 19 to build and establish a site-to-site VPN IPSec tunnel between two Palo Alto Networks Firewall. You can optionally complete these steps once you reach the chapter.

Let's now login to the Web GUI to configure our Palo Alto Networks Lab setup for chapter 19.



**Step14:** Configure the Layer 3 Zones with names “Internet” and “DMZ”. Go to **Network > Zones > Add**. Add the name and the type. We will attach these zones to their respective interfaces.



### Internet Zone:

The screenshot shows the configuration page for the 'Internet' zone. The 'Name' field is set to 'Internet', 'Log Setting' is 'None', and 'Type' is 'Layer3'. On the left, there is a section for 'INTERFACES' with an 'Add' button. The main area is divided into two columns: 'User Identification ACL' and 'Device-ID ACL'. Each column has an 'INCLUDE LIST' section with a text input field and an 'Add' button, and an 'EXCLUDE LIST' section with a text input field. Below each list is a note: 'Users from these addresses/subnets will be identified.' and 'Devices from these addresses/subnets will be identified.' respectively.

### DMZ Zone:

The screenshot shows the configuration page for the 'DMZ' zone. The 'Name' field is set to 'DMZ', 'Log Setting' is 'None', and 'Type' is 'Layer3'. On the left, there is a section for 'INTERFACES' with an 'Add' button. The main area is divided into two columns: 'User Identification ACL' and 'Device-ID ACL'. Each column has an 'INCLUDE LIST' section with a text input field and an 'Add' button, and an 'EXCLUDE LIST' section with a text input field. Below each list is a note: 'Users from these addresses/subnets will be identified.' and 'Devices from these addresses/subnets will be identified.' respectively.

**Step15:** Configure the Interface Management Profile. Go to Network > Network Profiles > Interface Mgmt. We will only enable ping and we will attach it to the interfaces where we will test reachability to.

Interface Management Profile

Name

**Administrative Management Services**

- ☐ HTTP
- ☐ HTTPS
- ☐ Telnet
- ☐ SSH

**Network Services**

- ☒ Ping
- ☐ HTTP OCSP
- ☐ SNMP
- ☐ Response Pages
- ☐ User-ID
- ☐ User-ID Syslog Listener-SSL
- ☐ User-ID Syslog Listener-UDP

**PERMITTED IP ADDRESSES**

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

**Step16:** Configure the “Internet” interface. Go to Network > Interface > Ethernet > ethernet1/1. Set the interface type to Layer3, Virtual Router to default, Security Zone to Internet. Configure the IP as 1.1.1.1 which is for the first Palo Alto Firewall. Set the management profile to PING.

#### Internet Interface:

Ethernet Interface

Interface Name

Comment

Interface Type

Netflow Profile

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

**Assign Interface To**

Virtual Router

Security Zone

## Interface IP:

The screenshot shows the 'Ethernet Interface' configuration window with the 'IP4' tab selected. The 'Interface Name' is 'ethernet1/1', 'Interface Type' is 'Layer3', and 'Netflow Profile' is 'None'. Under 'Type', 'Static' is selected. A table lists IP addresses, with '1.1.1.1' selected. Below the table are controls for adding, deleting, and moving entries. The 'OK' button is highlighted.

IP
<input checked="" type="checkbox"/> 1.1.1.1

## Management Profile:

The screenshot shows the 'Ethernet Interface' configuration window with the 'Advanced' tab selected. 'Link Settings' show 'Link Speed' as 'auto', 'Link Duplex' as 'auto', and 'Link State' as 'up'. Under 'Other Info', 'Management Profile' is 'PING' and 'MTU' is '[576 - 1500]'. 'Adjust TCP MSS' is unchecked, with 'IPv4 MSS Adjustment' at 40 and 'IPv6 MSS Adjustment' at 60. 'Untagged Subinterface' is also unchecked. The 'OK' button is highlighted.

**Step16:** Configure the “DMZ” interface. Go to **Network > Interface > Loopback > Add**. Add Interface Name loopback.1 , set Virtual Router to default, Security Zone to DMZ. Configure the IP as 10.10.10.1/24 which is for the first Palo Alto Firewall. Set the management profile to PING.

### Internet Interface:

Loopback Interface

Interface Name

loopback

.

1

Comment

Netflow Profile

None

▼

Config

IPv4

IPv6

Advanced

Assign Interface To

Virtual Router

default

▼

Security Zone

DMZ

▼

OK

Cancel

### Interface IP:

Loopback Interface

Interface Name

loopback

.

1

Comment

Netflow Profile

None

▼

Config

IPv4

IPv6

Advanced

☐ IP

☒ 10.10.10.1/24

⊕ Add

⊖ Delete

↑ Move Up

↓ Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK

Cancel

### Management Profile:

Loopback Interface

Interface Name

loopback

.

1

Comment

Netflow Profile

None

Config

IPv4

IPv6

Advanced

Other Info

Management Profile

PING

MTU

[576 - 1500]

Network Packet Broker

☐ Adjust TCP MSS

IPv4 MSS Adjustment

40

IPv6 MSS Adjustment

60

OK

Cancel

**Step17:** Create a static default route pointing to the internet interface. Go to **Network > Virtual Routers > default > Static Routes > Add**.

Virtual Router - Static Route - IPv4

Name

default\_0.0.0.0

Destination

0.0.0.0/0

Interface

ethernet1/1

Next Hop

None

Admin Distance

10 - 240

Metric

10

Route Table

Unicast

BFD Profile

Disable BFD

☐ Path Monitoring

Failure Condition

☒ Any ☐ All

Preemptive Hold Time (min)

2

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
--------------------------	------	--------	-----------	----------------	--------------------	------------

+ Add

- Delete

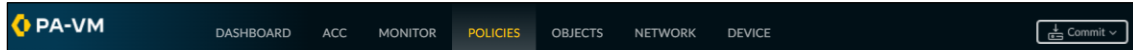
OK

Cancel

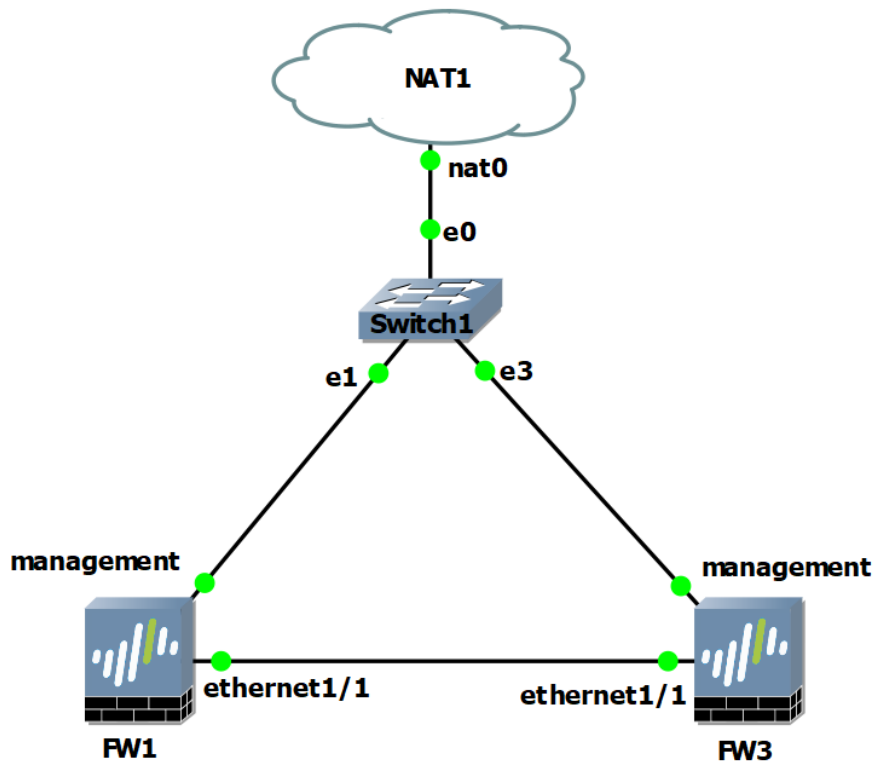
**Step 18:** Create a Security Policy to allow any traffic. Go to **Policies > Security > Add**. Add the name test, source and destination to any, application and service to any and action as allow.

NAME	Source		Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
	ZONE	ADDRESS	ZONE	ADDRESS					
test	any	any	any	any	any	any	✓ Allow	none	

**Step 19:** Commit the change.



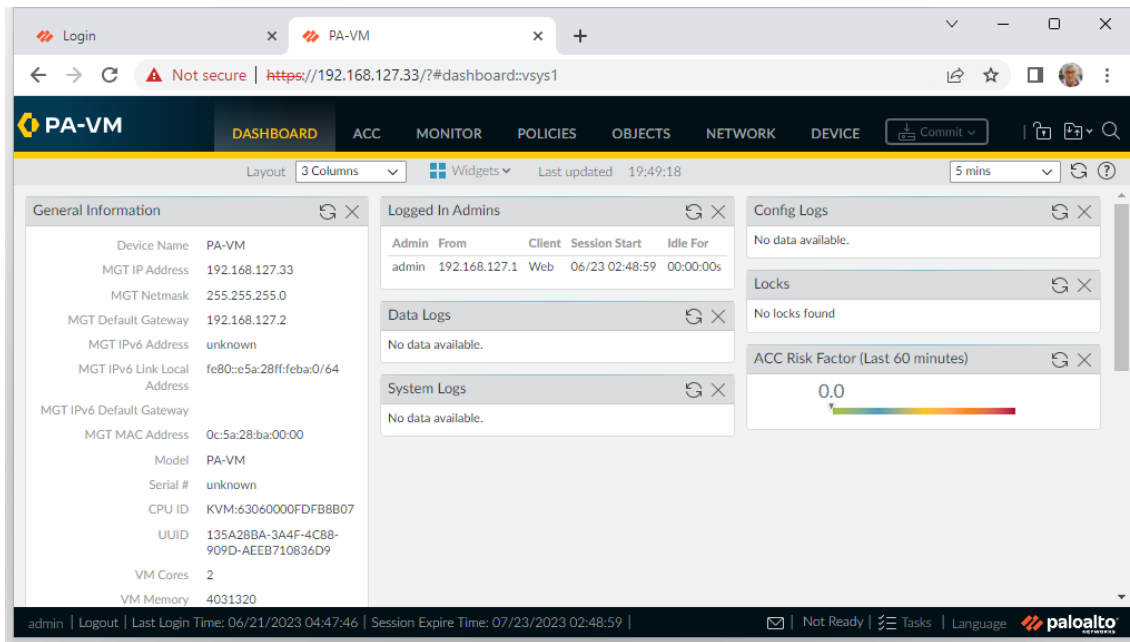
**Step 20:** Add a Second Palo Alto Firewall (FW3) and repeat steps 10 to 19 with the following values below. All the other values will remain similar.



Management IP Address: 192.168.127.33

Ethernet1/1 IP: 3.3.3.3

Loopback.1 IP: 10.10.30.1/24

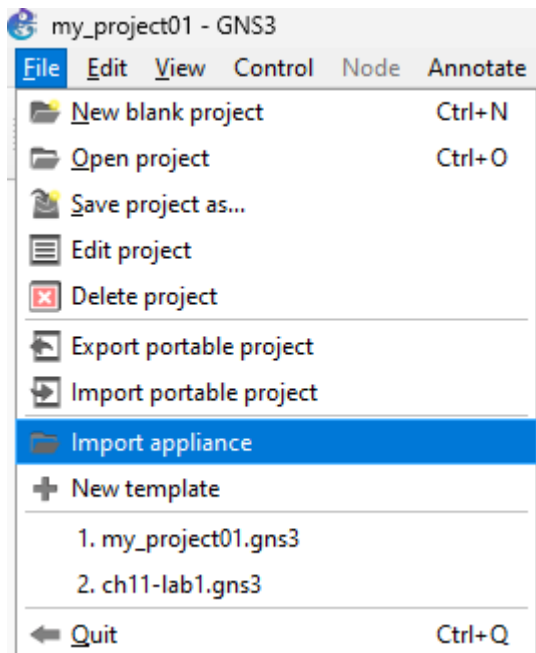


This completes Palo Alto Firewall configuration for Chapters 17-21. Let's configure Fortinet firewall for Chapters 17-18.

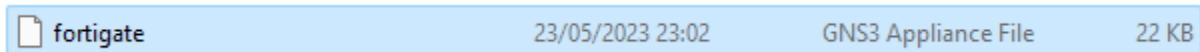
## Fortinet FortiGate installation on GNS3

Let's continue with the installation of Fortinet's FortiGate. Please follow along.

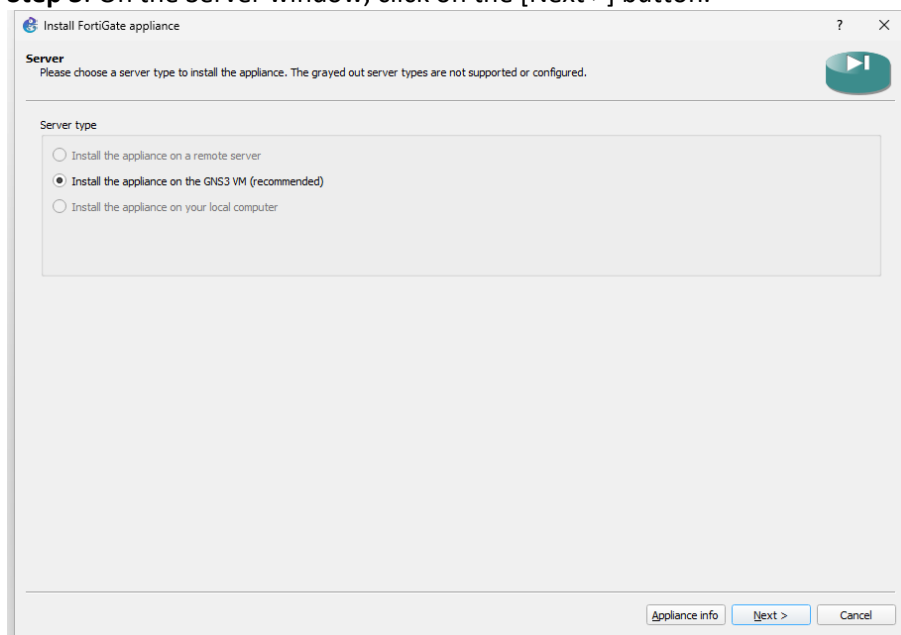
**Step 1:** On GNS3 main window, go to File > Import appliance.



**Step 2:** Navigate to your Downloads folder and locate the file named 'fortigate.gns3a'. Select the file to open in the GNS3 Import appliance.

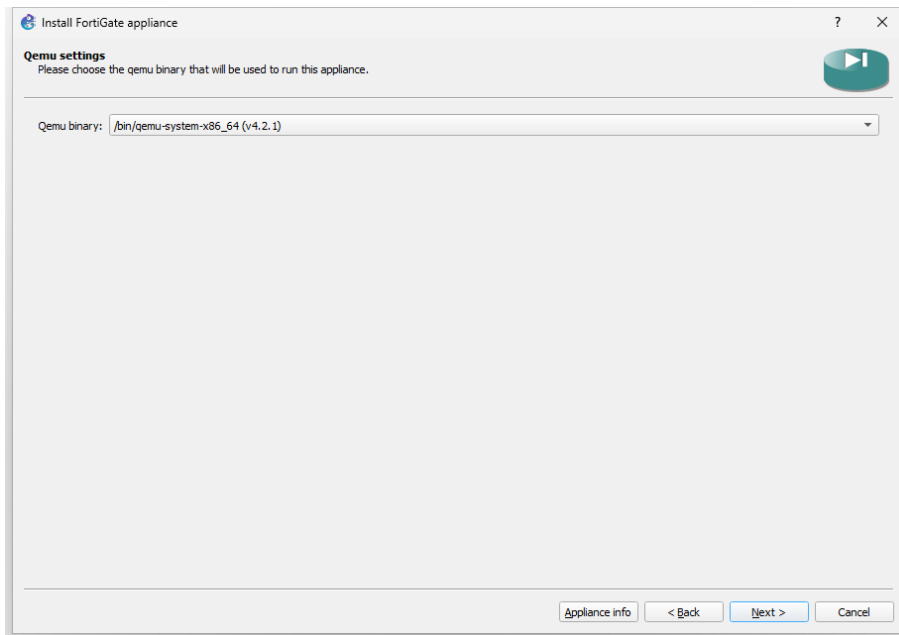


**Step 3:** On the Server window, click on the [Next >] button.

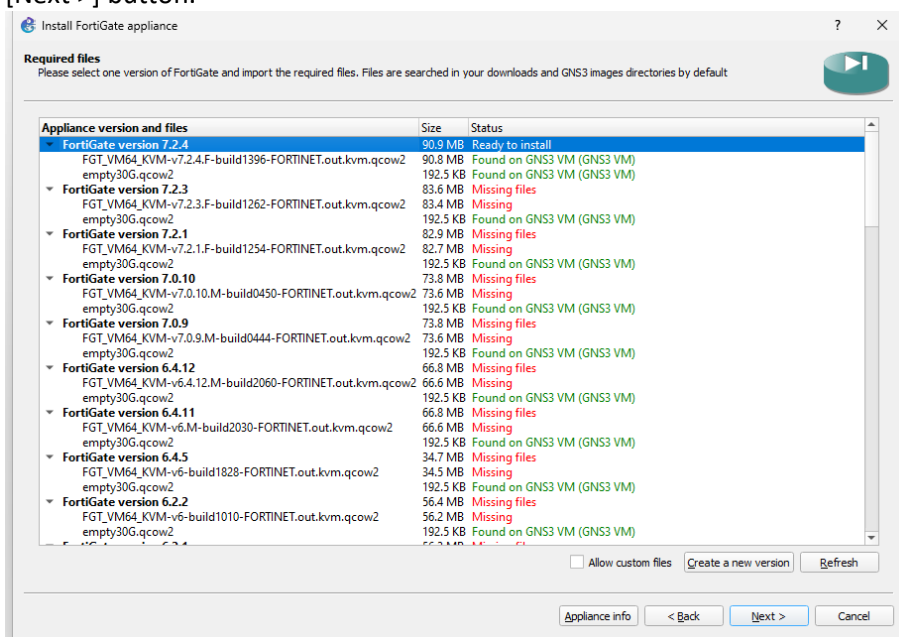


**Step 4:** On the Qemu settings window, click on the [Next >] button.

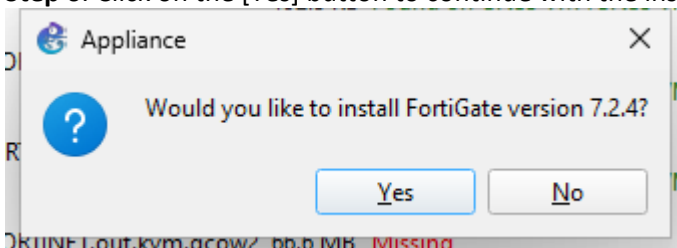




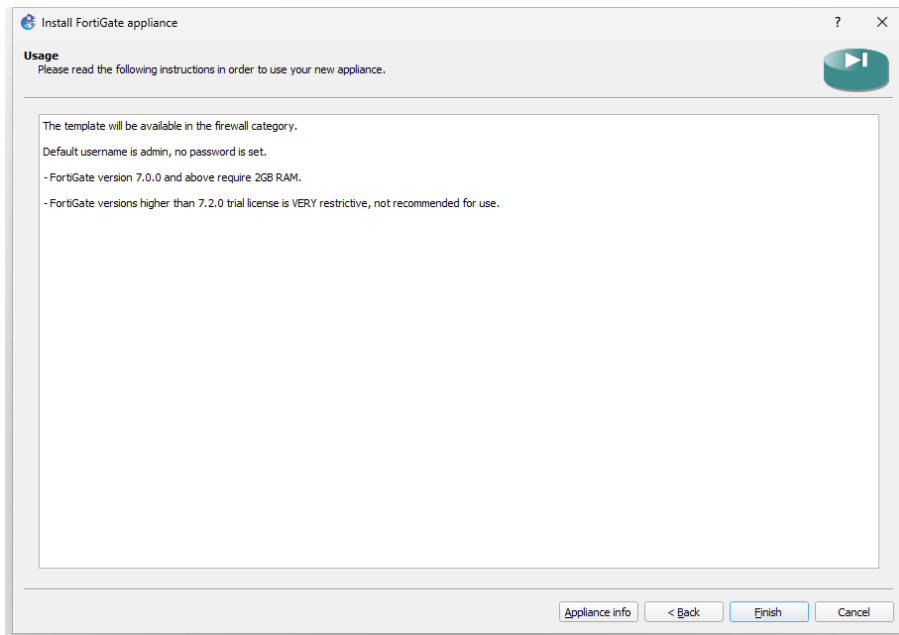
**Step 5:** If you have placed all the required files under the Downloads folder of your PC, you will see the FortiGate version populated in the Required Files window. Highlight your version and click on the [Next >] button.



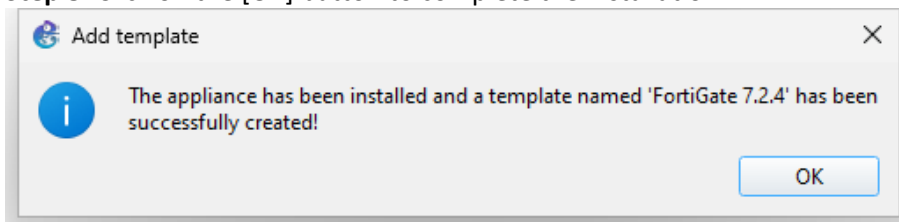
**Step 6:** Click on the [Yes] button to continue with the installation.



**Step 7:** Click on the [Finish] button to complete the installation.



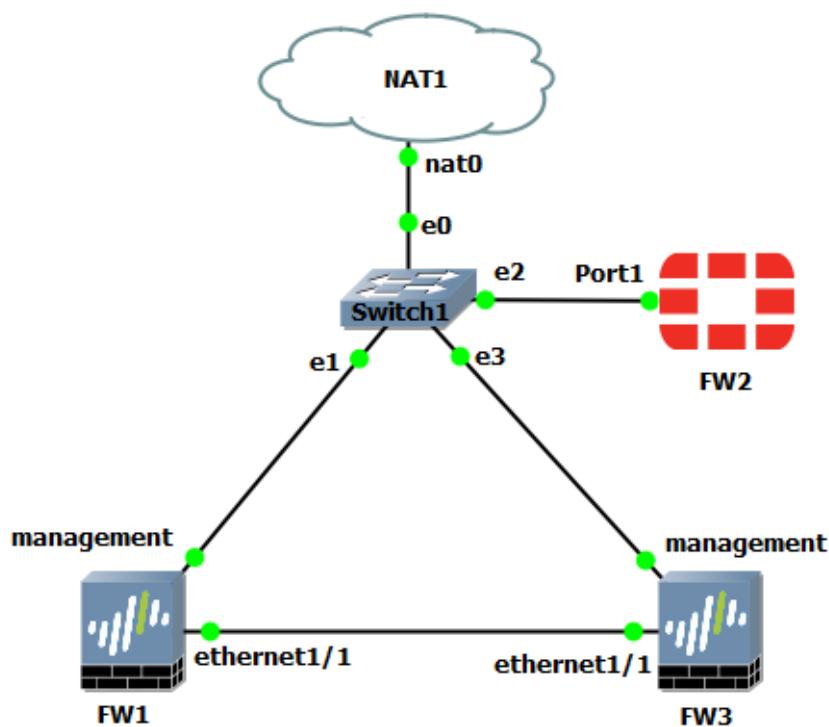
**Step 8:** Click on the [OK] button to complete the installation.



**Step 9:** Now, go to All devices in GNS3 and drag-n-drop FortiGate 7.2.4 onto the Topology canvas, then use Add a Link to connect Port1 of FortiGate to e2 of the GNS3's dummy switch. Finally, Power on the new Fortinet firewall.

Topology Summary	
Node	Console
FW1 ethernet1/1 <=> ethernet1/1 FW3 management <=> e1 Switch1	telnet 192.168.186.128:5002
FW2 Port1 <=> e2 Switch1	telnet 192.168.186.128:5016
FW3 ethernet1/1 <=> ethernet1/1 FW1 management <=> e3 Switch1	telnet 192.168.186.128:5006
NAT1 nat0 <=> e0 Switch1	none
Switch1 e0 <=> nat0 NAT1 e1 <=> management FW1 e2 <=> Port1 FW2 e3 <=> management FW3	none

Servers Summary	
▼	GNS3 VM (GNS3 VM) CPU 82.0%, RAM 96.9%
	FW1
	FW2
	FW3
	Switch1
▼	LP50BC CPU 13.7%, RAM 84.8%
	NAT1



**Step 10:** Double-click on the FortiGate icon and it will open the SSH session on the Putty. If your software loads up and you get the first login prompt, then you know that the installation has been completed successfully and you are ready to go.

```
FortiGate7.2.4-1 - PuTTY
Scanning /dev/vda1... (100%)
Scanning /dev/vda2... (100%)
Serial number is FGVMEVBYZ1-LJBC7

Disk usage changed, please wait for reboot...

Formatting the disk...
- unmounting /data2 : ok
Partitioning and formatting /dev/vdb label LOGUSEDXEB070131 ... done

The system is going down NOW !!

Please stand by while rebooting the system.
Restarting system

System is starting...
The config file may contain errors.
Please see details by the command 'diagnose debug config-error-log read'.
Serial number is FGVMEVBYZ1-LJBC7

FortiGate-VM64-KVM login: █
```

**Step 11:** On FortiGates, the default administrator username is admin with a blank password on the first boot. You must change the default administrator password (admin/blank) on the first admin account log in your device. Please go ahead and set the administrator password and keep the password handy.

FortiGate-VM64-KVM login: **admin**

Password: blank

You are forced to change your password. Please input a new password.

New Password:\*\*\*\*\*

Confirm Password: :\*\*\*\*\*

Welcome!

```
fw2 - PuTTY

System is starting...
Starting system maintenance...
Scanning /dev/vda1... (100%)
Scanning /dev/vda2... (100%)
Serial number is FGVMEVJAZDYLIA85

FortiGate-VM64-KVM login: admin
Password:
Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistency in the disk drive.
It is strongly recommended that you check the file system consistency before proceeding.
Please run 'execute disk list' and then 'execute disk scan <ref#>'.
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
FortiGate-VM64-KVM # █
```

**That's it!** Now you have completed the installation of two firewalls from two different vendors for your testing lab. Now continue your reading and study with the book.

Palo GNS3 files download links:

<https://www.gns3.com/marketplace/appliances/pa-vm>

**PA-VM 10.1.0** - – The .qcow2 file will require a valid account with access to the file on the Palo Alto site.

File	MD5	Size	
PA-VM-KVM-10.1.0.qcow2	8266fd412a22694749f2cd4afcd5fa33	3597 MB	<a href="#">Download</a>

**PA-VM 10.0.0**

File	MD5	Size	
PA-VM-KVM-10.0.0.qcow2	d73a41e4d8f6f5a5291fde08b79a071e	3059 MB	<a href="#">Download</a>

FortiGate GNS3 files download links: <https://www.gns3.com/marketplace/featured/fortigate>

**FortiGate 7.2.4** – The kvm.qcow2 file will require a valid account with access to the file on the Fortinet site.

File	MD5	Size	
FGT_VM64_KVM-v7.2.4.F-build1396-FORTINET.out.kvm.qcow2	e3bd5958ff3d4f9363152c340e9b9578	95 MB	<a href="#">Download</a>
empty30G.qcow2	3411a599e822f2ac6be560a26405821a	0 MB	<a href="#">Download</a>