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

File name:	Ch11_Pre-task2_PaloAlto_and_Fortinet_Firewall_Installation_on_GNS3.pdf
Version:	1.0
Created on:	25/June/2023
Download URL:	https://github.com/ansnetauto/appress_ansnetauto
Applicable to:	Chapters 17 - 21

About this document:

Welcome to the software installation guide for the Apress book, "***Introduction to Ansible Network Automation: A 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 in the book.

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

Warning! The software used in this guide may include a combination of free, open-source and proprietary software. Readers can search for most of the free and 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.

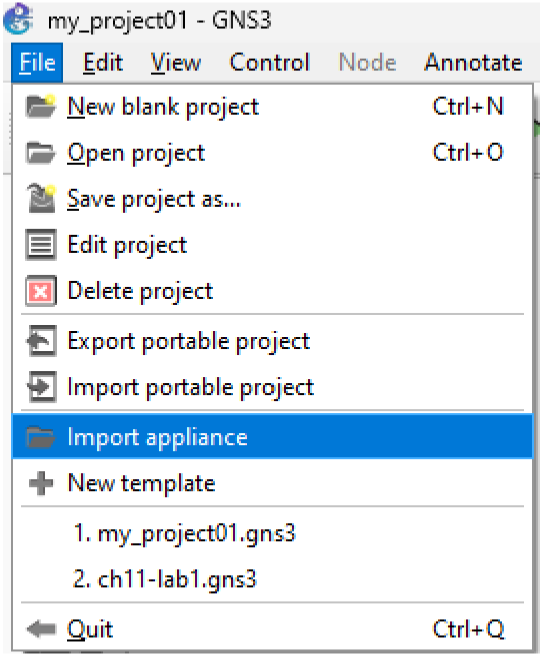
Contents

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.

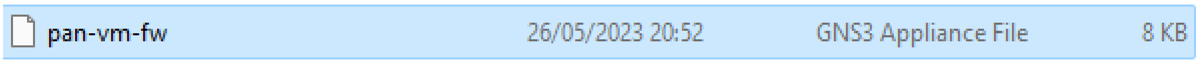
Palo Alto PA-VM installation on GNS3

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.

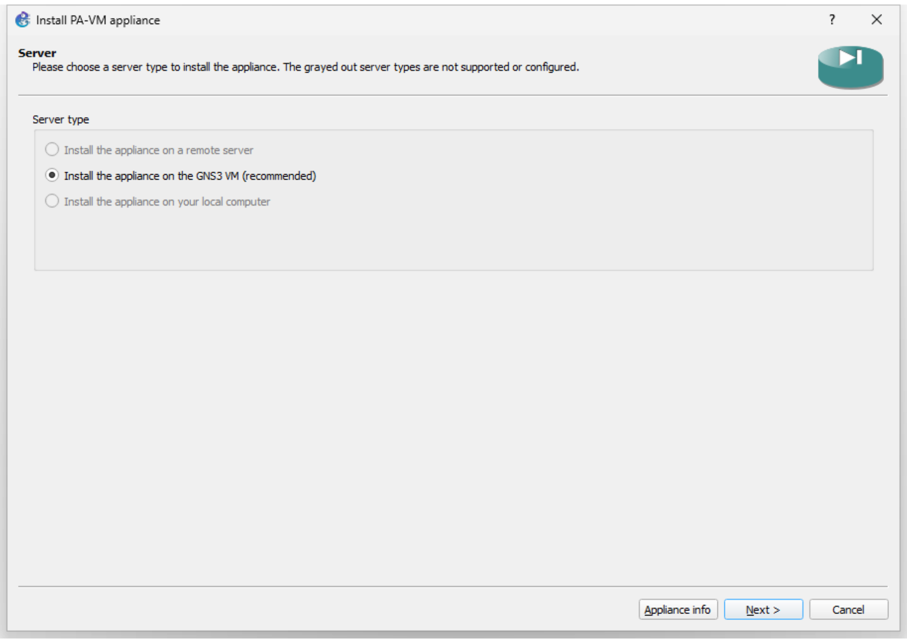
Step 1: On GNS3 main window, go to File > Import appliance.



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.


pan-vm-fw 26/05/2023 20:52 GNS3 Appliance File 8 KB

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



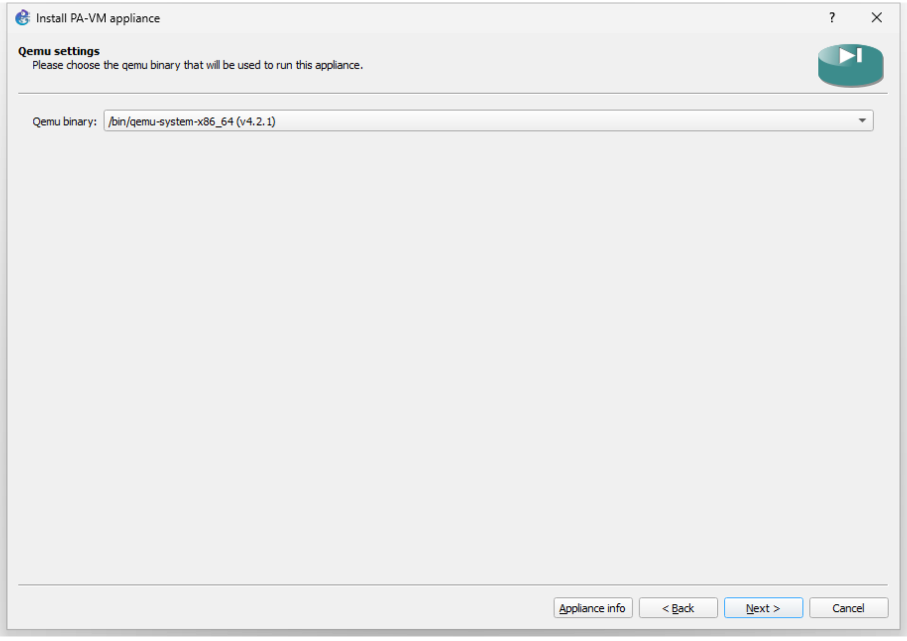
Install PA-VM appliance

Server
Please choose a server type to install the appliance. The grayed out server types are not supported or configured.

Server type

○ Install the appliance on a remote server
● Install the appliance on the GNS3 VM (recommended)
○ Install the appliance on your local computer

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

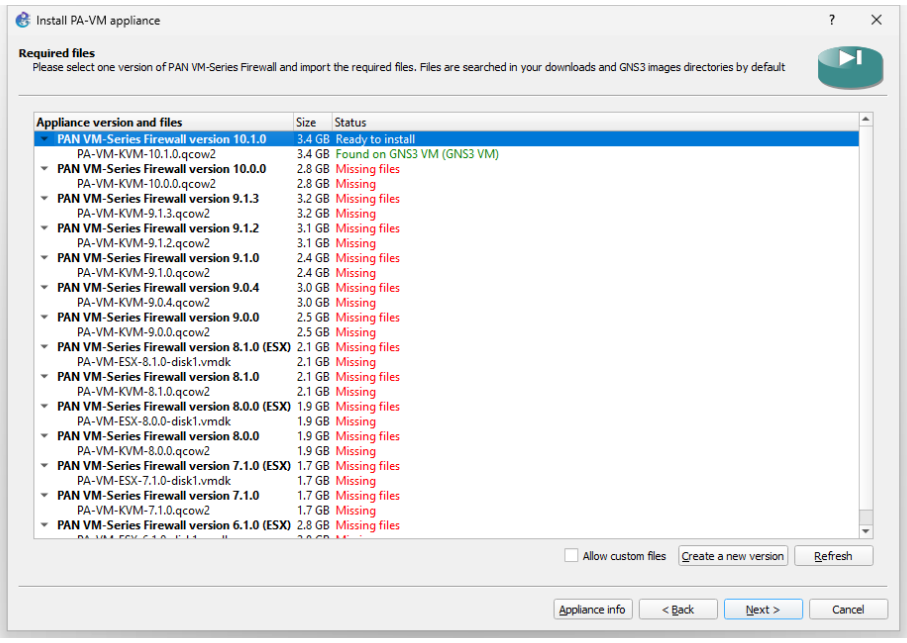


Install PA-VM appliance

Qemu settings
Please choose the qemu binary that will be used to run this appliance.

Qemu binary: /bin/qemu-system-x86_64 (v4.2.1)

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.

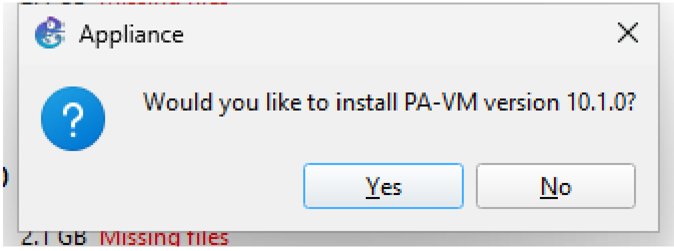


Install PA-VM appliance

Required files
Please select one version of PAN VM-Series Firewall and import the required files. Files are searched in your downloads and GNS3 images directories by default

Appliance version and files	Size	Status
PAN VM-Series Firewall version 10.1.0	3.4 GB	Ready to install
PA-VM-KVM-10.1.0.qcow2	3.4 GB	Found on GNS3 VM (GNS3 VM)
PAN VM-Series Firewall version 10.0.0	2.8 GB	Missing files
PA-VM-KVM-10.0.0.qcow2	2.8 GB	Missing
PAN VM-Series Firewall version 9.1.3	3.2 GB	Missing files
PA-VM-KVM-9.1.3.qcow2	3.2 GB	Missing
PAN VM-Series Firewall version 9.1.2	3.1 GB	Missing files
PA-VM-KVM-9.1.2.qcow2	3.1 GB	Missing
PAN VM-Series Firewall version 9.1.0	2.4 GB	Missing files
PA-VM-KVM-9.1.0.qcow2	2.4 GB	Missing
PAN VM-Series Firewall version 9.0.4	3.0 GB	Missing files
PA-VM-KVM-9.0.4.qcow2	3.0 GB	Missing
PAN VM-Series Firewall version 9.0.0	2.5 GB	Missing files
PA-VM-KVM-9.0.0.qcow2	2.5 GB	Missing
PAN VM-Series Firewall version 8.1.0 (ESX)	2.1 GB	Missing files
PA-VM-ESX-8.1.0-disk1.vmdk	2.1 GB	Missing
PAN VM-Series Firewall version 8.1.0	2.1 GB	Missing files
PA-VM-KVM-8.1.0.qcow2	2.1 GB	Missing
PAN VM-Series Firewall version 8.0.0 (ESX)	1.9 GB	Missing files
PA-VM-ESX-8.0.0-disk1.vmdk	1.9 GB	Missing
PAN VM-Series Firewall version 8.0.0	1.9 GB	Missing files
PA-VM-KVM-8.0.0.qcow2	1.9 GB	Missing
PAN VM-Series Firewall version 7.1.0 (ESX)	1.7 GB	Missing files
PA-VM-ESX-7.1.0-disk1.vmdk	1.7 GB	Missing
PAN VM-Series Firewall version 7.1.0	1.7 GB	Missing files
PA-VM-KVM-7.1.0.qcow2	1.7 GB	Missing
PAN VM-Series Firewall version 6.1.0 (ESX)	2.8 GB	Missing files

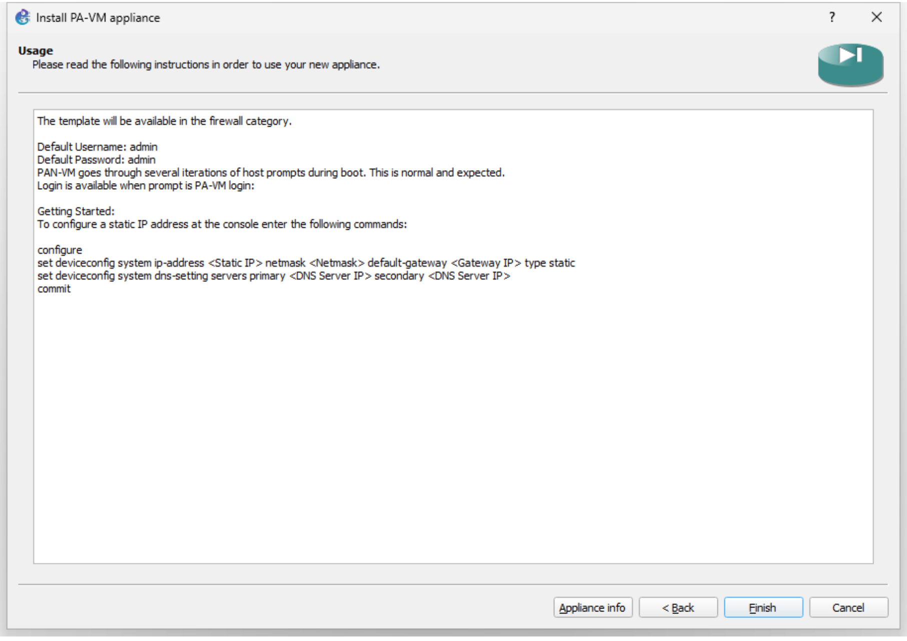
Step 6: When prompted to answer 'Yes' or 'No', click on the [Yes] button.



Appliance

Would you like to install PA-VM version 10.1.0?

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

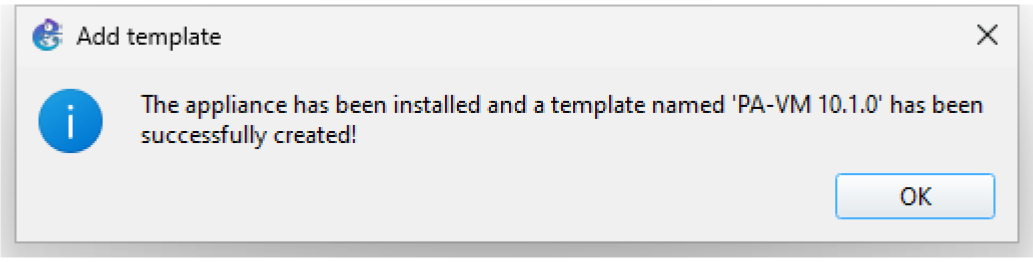


Install PA-VM appliance

Usage
Please read the following instructions in order to use your new appliance.

```
The template will be available in the firewall category.

Default Username: admin
Default Password: admin
PAN-VM goes through several iterations of host prompts during boot. This is normal and expected.
Login is available when prompt is PA-VM login:

Getting Started:
To configure a static IP address at the console enter the following commands:

configure
set deviceconfig system ip-address <Static IP> netmask <Netmask> default-gateway <Gateway IP> type static
set deviceconfig system dns-setting servers primary <DNS Server IP> secondary <DNS Server IP>
commit
```

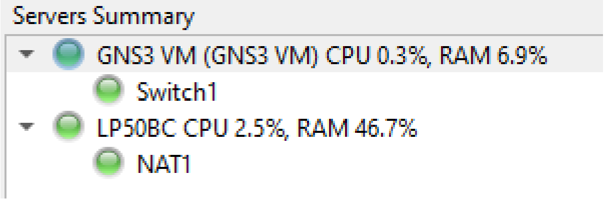
Step 8: Click on the [OK] button on the Add template prompt window to complete your installation.



Add template

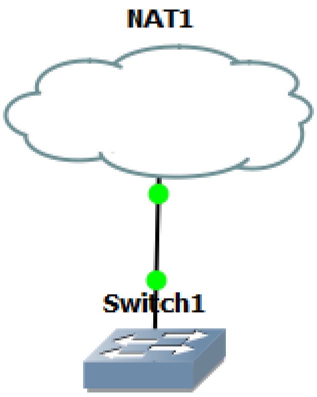
The appliance has been installed and a template named 'PA-VM 10.1.0' has been successfully created!

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.

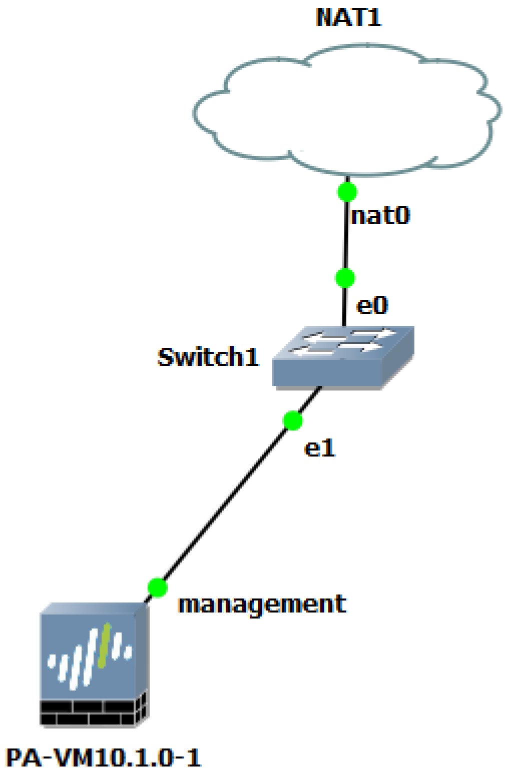


Servers Summary

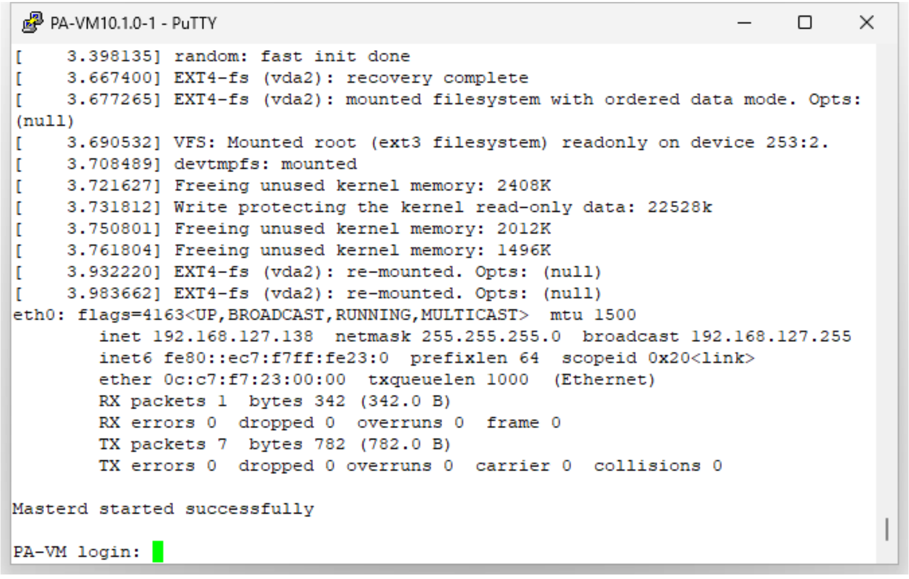
- GNS3 VM (GNS3 VM) CPU 0.3%, RAM 6.9%
  - Switch1
- LP50BC CPU 2.5%, RAM 46.7%
  - NAT1



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.

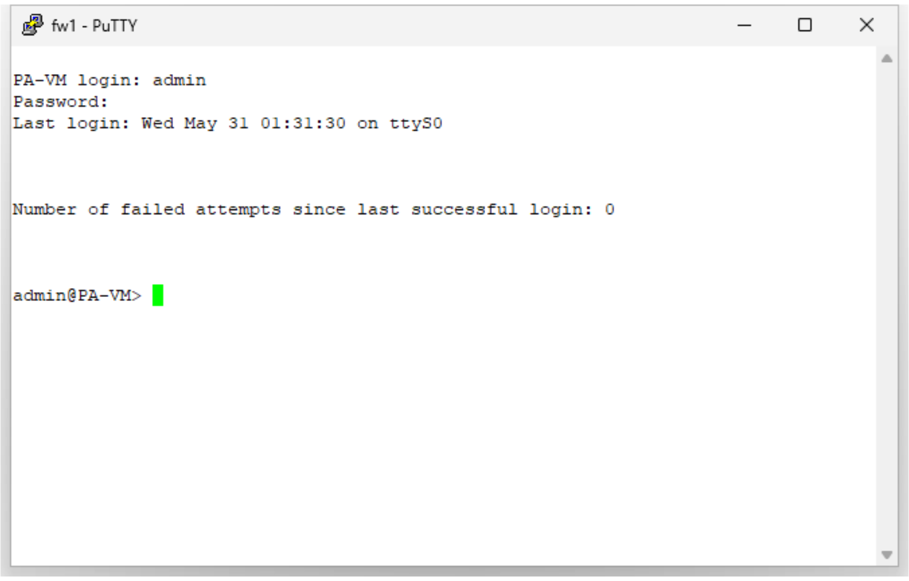


```
[    3.398135] random: fast init done
[    3.667400] EXT4-fs (vda2): recovery complete
[    3.677265] EXT4-fs (vda2): mounted filesystem with ordered data mode. Opts:
(null)
[    3.690532] VFS: Mounted root (ext3 filesystem) readonly on device 253:2.
[    3.708489] devtmpfs: mounted
[    3.721627] 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



```
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>
```

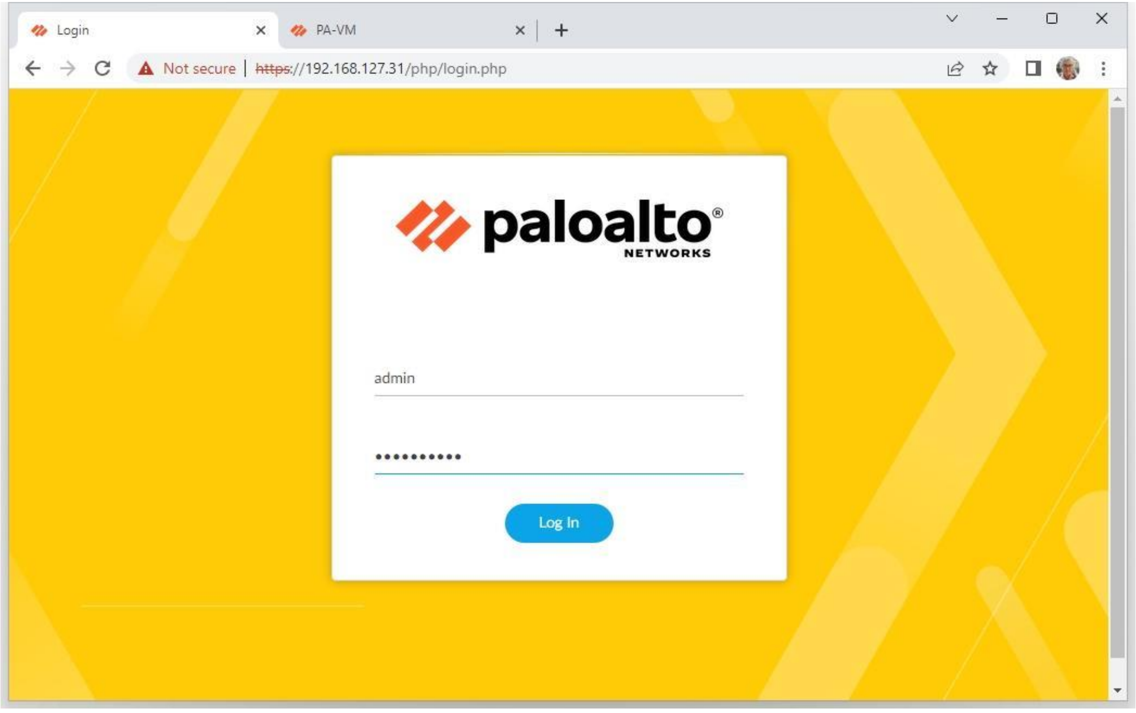
Step 13: We can now configure the management interface on our Palo Alto Network Firewalls. It is set to DHCP by default. Once we have configured the management IP, we should be able to log in via ssh and web GUI.

```
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=kA10g000000ClN7CAK

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 Firewalls. 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.



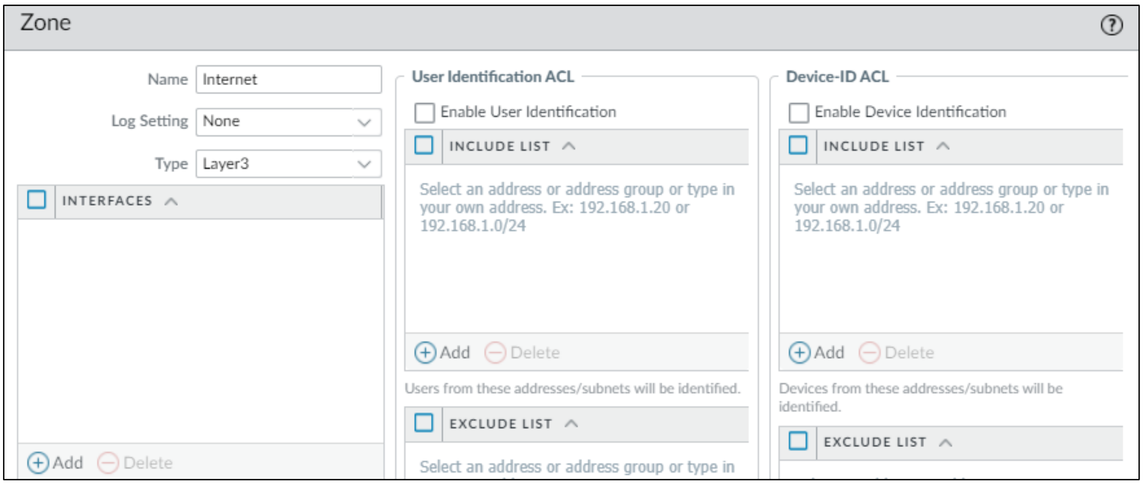
https://192.168.127.31/php/login.php

admin

••••••••••

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:



Zone

Name: Internet

Log Setting: None

Type: Layer3

User Identification ACL

□ Enable User Identification

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

Users from these addresses/subnets will be identified.

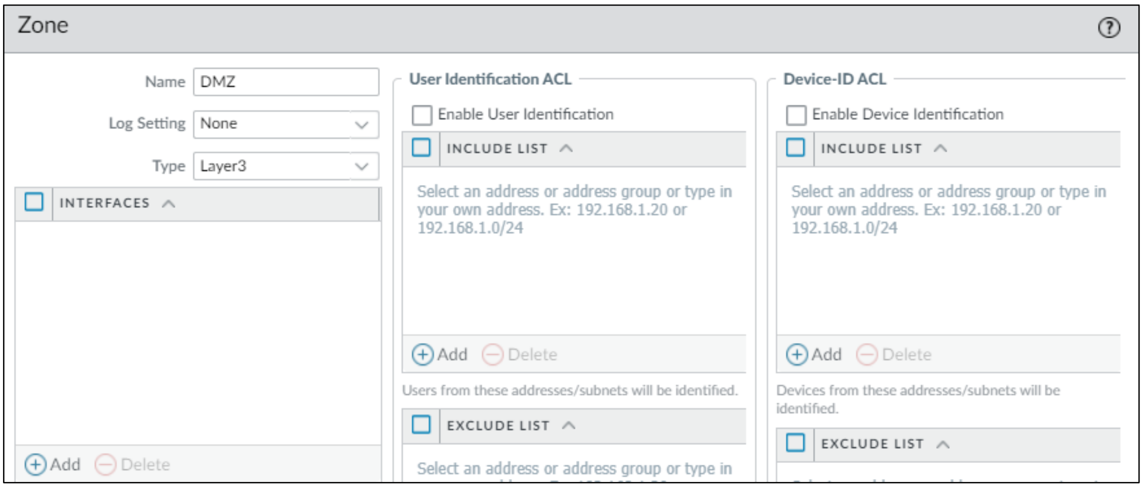
Device-ID ACL

□ Enable Device Identification

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

Devices from these addresses/subnets will be identified.

DMZ Zone:



Zone

Name: DMZ

Log Setting: None

Type: Layer3

User Identification ACL

□ Enable User Identification

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

Users from these addresses/subnets will be identified.

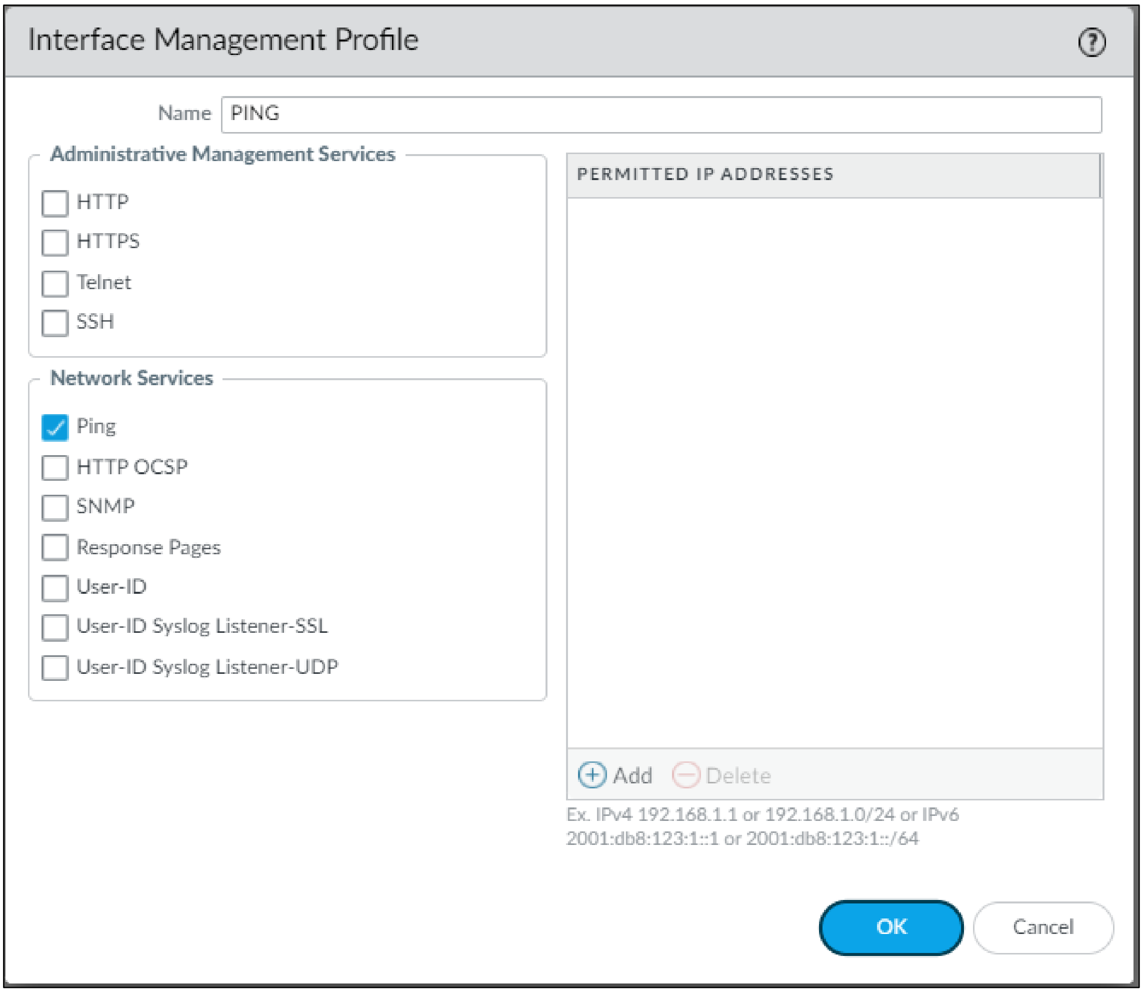
Device-ID ACL

□ Enable Device Identification

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

Devices from these addresses/subnets will be identified.

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: PING

Administrative Management Services

- □ HTTP
- □ HTTPS
- □ Telnet
- □ SSH

Network Services

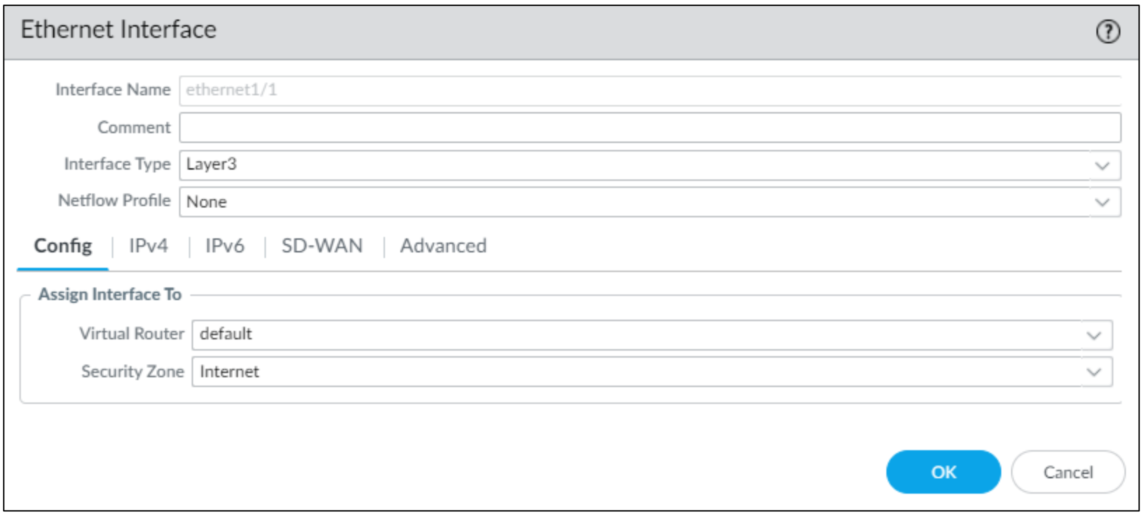
- ☑ Ping
- □ HTTP OCSP
- □ SNMP
- □ Response Pages
- □ User-ID
- □ User-ID Syslog Listener-SSL
- □ User-ID Syslog Listener-UDP

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: ethernet1/1

Comment:

Interface Type: Layer3

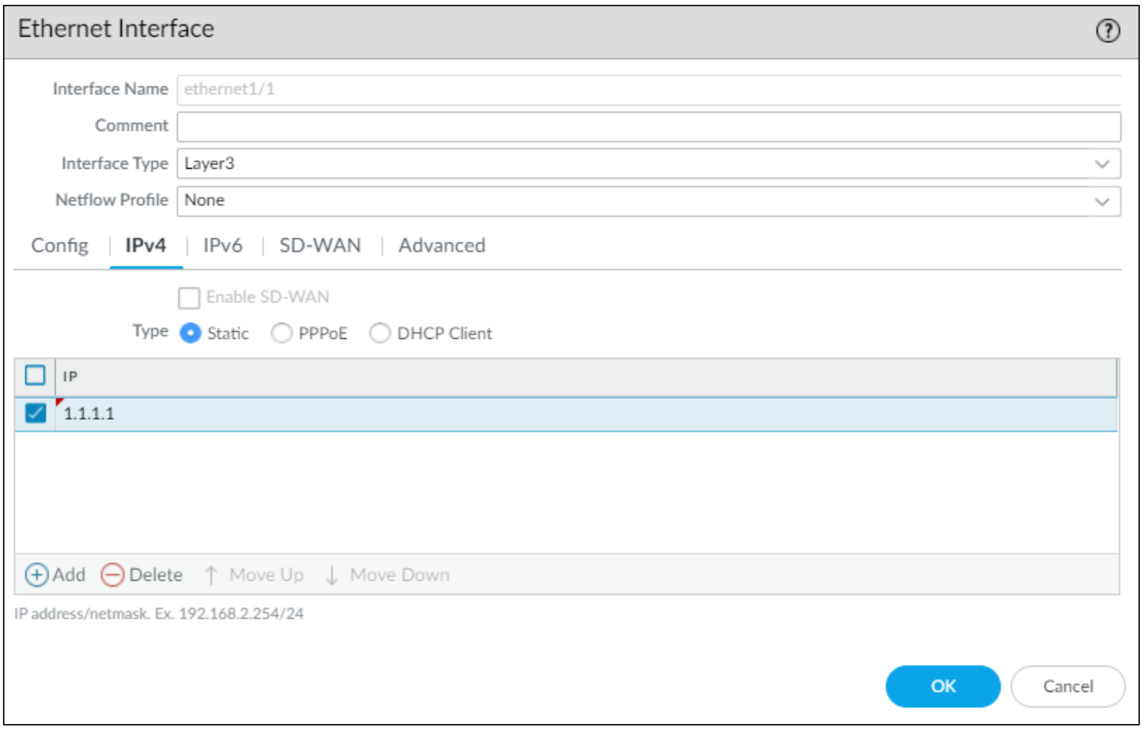
Netflow Profile: None

Assign Interface To

Virtual Router: default

Security Zone: Internet

Interface IP:



Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

□ Enable SD-WAN

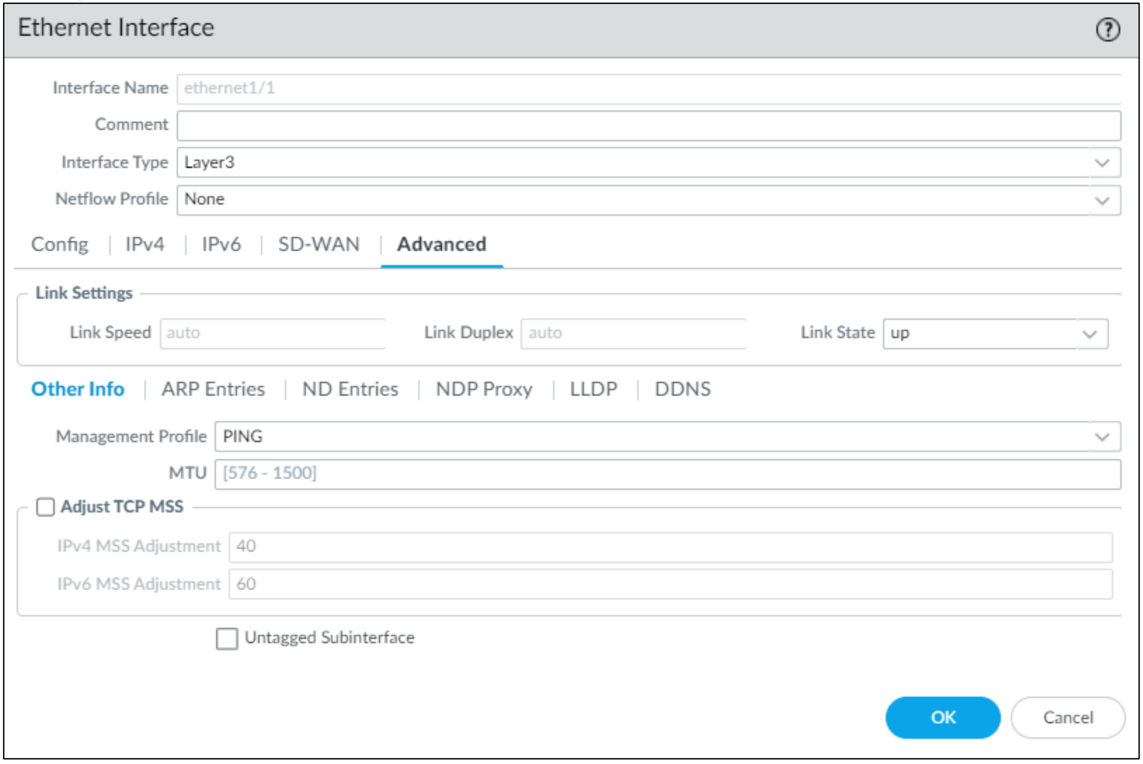
Type ● Static ○ PPPoE ○ DHCP Client

□	IP
☑	1.1.1.1

⊕ Add ⊖ Delete ↑ Move Up ↓ Move Down

IP address/netmask. Ex. 192.168.2.254/24

Management Profile:



Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Link Settings

Link Speed: auto Link Duplex: auto Link State: up

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP | DDNS

Management Profile: PING

MTU: [576 - 1500]

□ Adjust TCP MSS

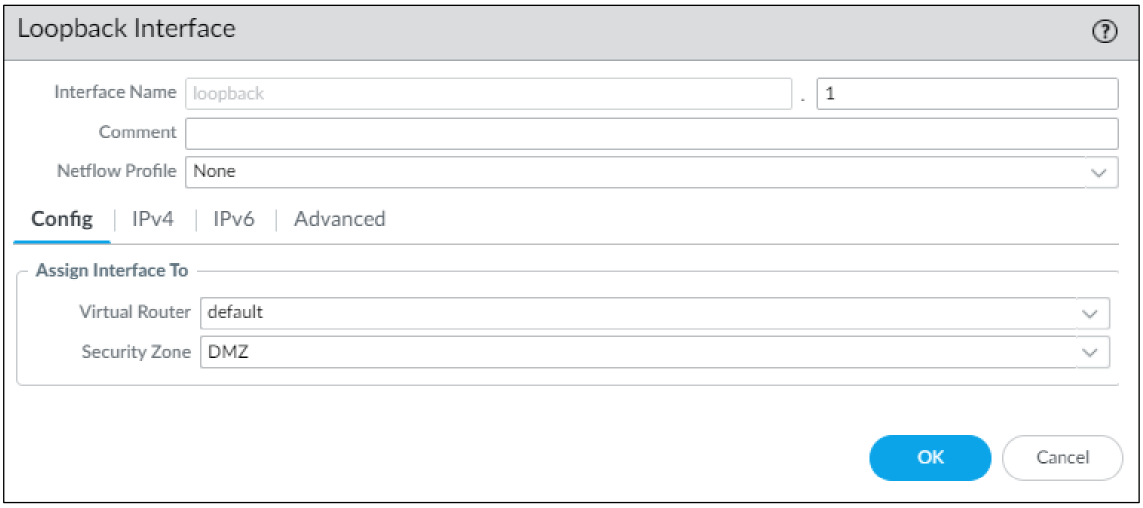
IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

□ Untagged Subinterface

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:

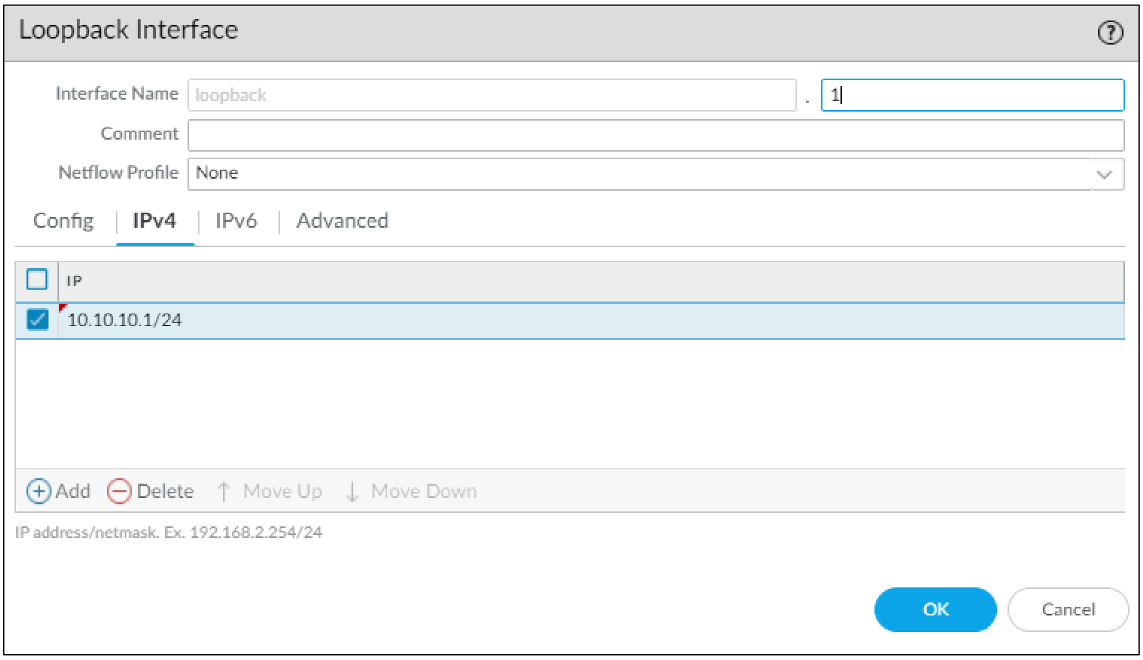
Netflow Profile: None

Assign Interface To

Virtual Router: default

Security Zone: DMZ

Interface IP:



Loopback Interface

Interface Name: loopback . 1

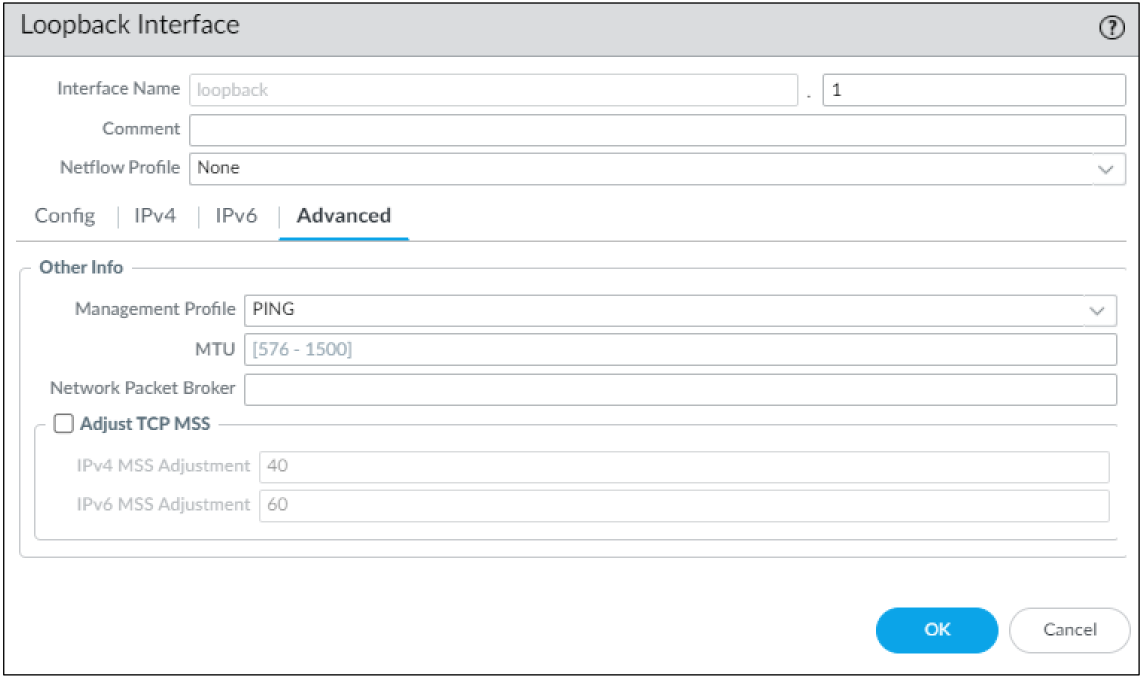
Comment:

Netflow Profile: None

□	IP
☑	10.10.10.1/24

IP address/netmask. Ex. 192.168.2.254/24

Management Profile:



Loopback Interface

Interface Name	loopback . 1
Comment	
Netflow Profile	None

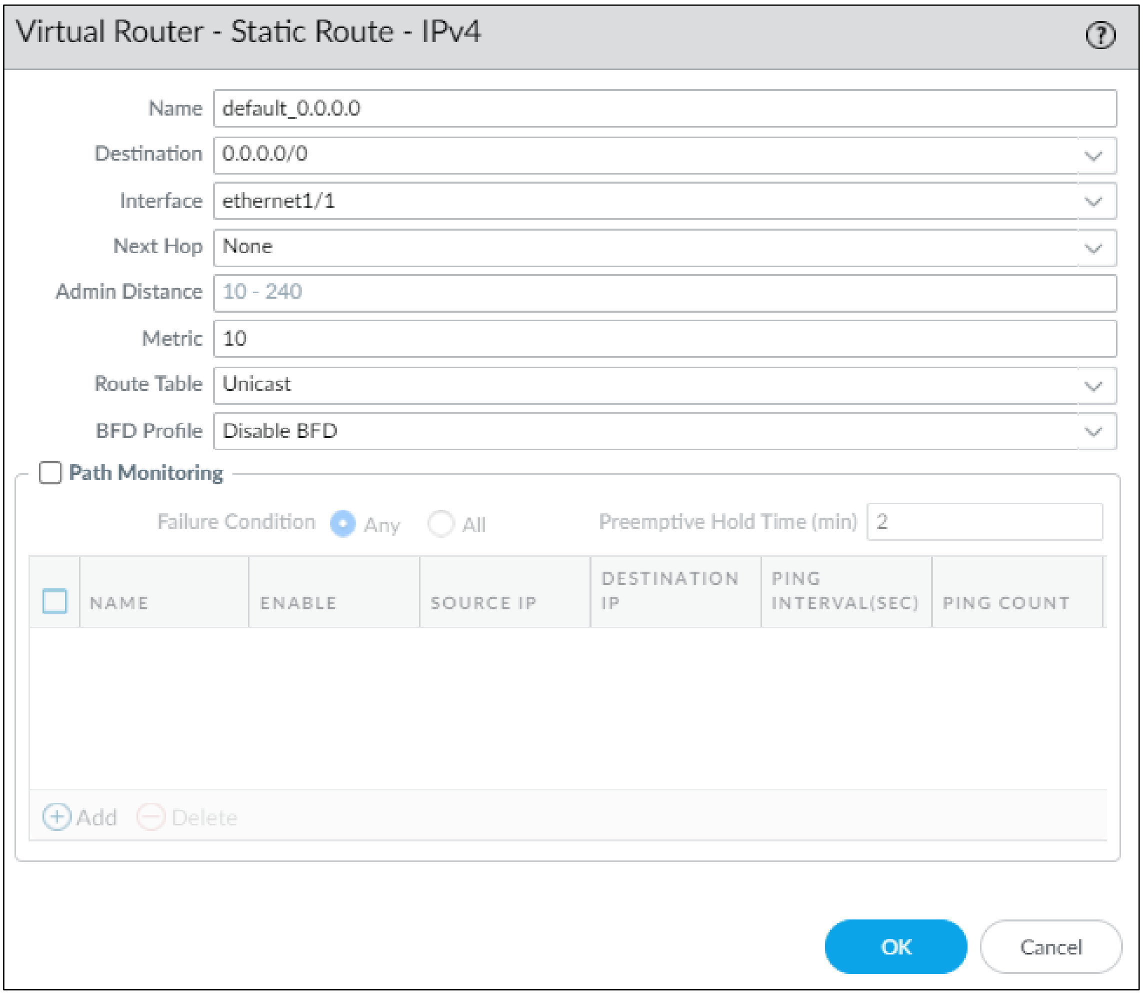
Other Info

Management Profile	PING
MTU	[576 - 1500]
Network Packet Broker	

□ Adjust TCP MSS

IPv4 MSS Adjustment	40
IPv6 MSS Adjustment	60

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

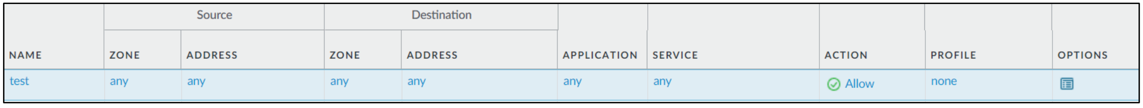
Name	default_0.0.0.0
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	None
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

□ Path Monitoring

Failure Condition ● Any ○ All   Preemptive Hold Time (min) 2

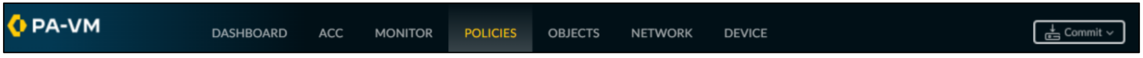
□	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

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.

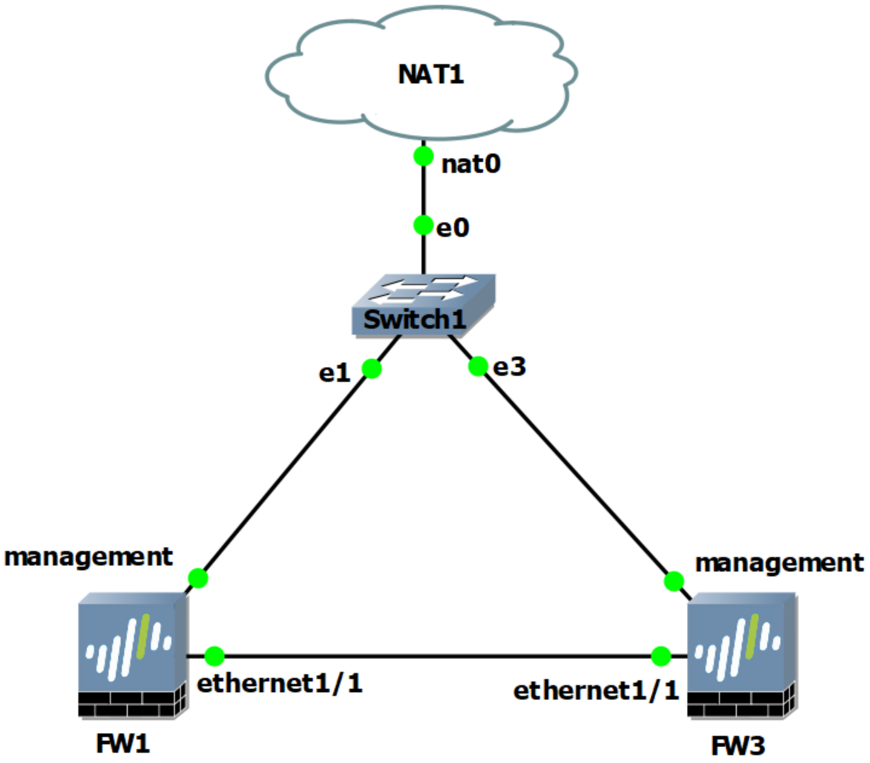


	Source		Destination						
NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
test	any	any	any	any	any	any	✓ Allow	none	▤

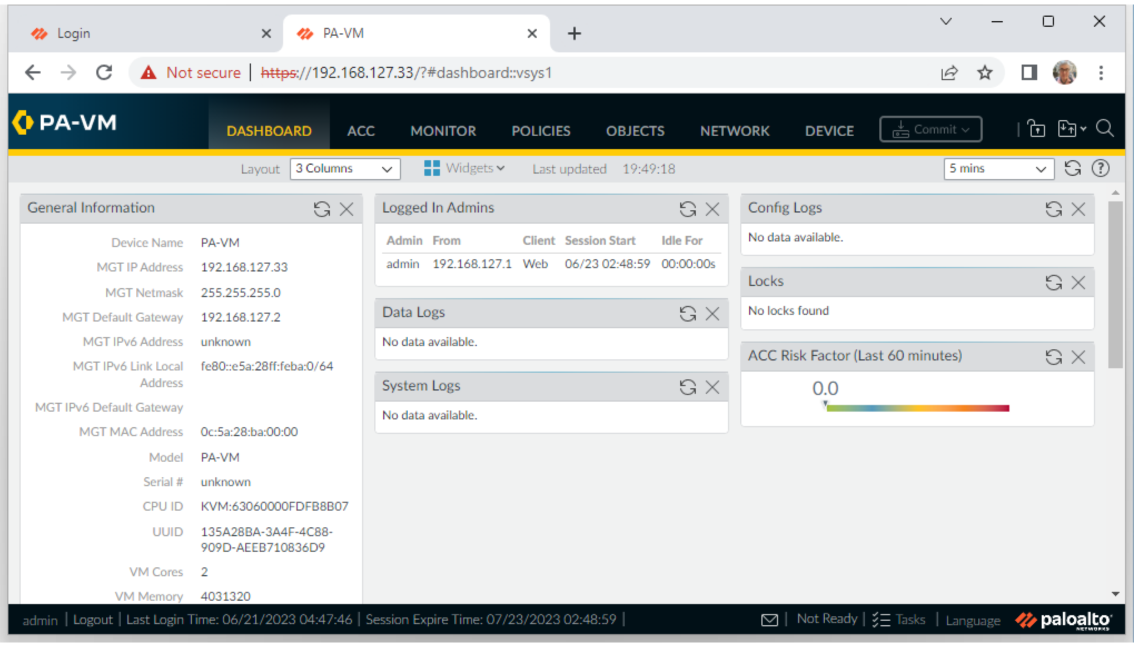
Step 19: Commit the change.



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 the same.



Management IP Address: 192.168.127.33
Ethernet1/1 IP: 3.3.3.3
Loopback.1 IP: 10.10.30.1/24



General Information

Device Name	PA-VM
MGT IP Address	192.168.127.33
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.127.2
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::e5a:28ff:feba:0/64
MGT IPv6 Default Gateway	
MGT MAC Address	0c:5a:28:ba:00:00
Model	PA-VM
Serial #	unknown
CPU ID	KVM:63060000FDFB8B07
UUID	135A28BA-3A4F-4C88-909D-AEEB710836D9
VM Cores	2
VM Memory	4031320

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	192.168.127.1	Web	06/23 02:48:59	00:00:00s

Data Logs

No data available.

System Logs

No data available.

Config Logs

No data available.

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

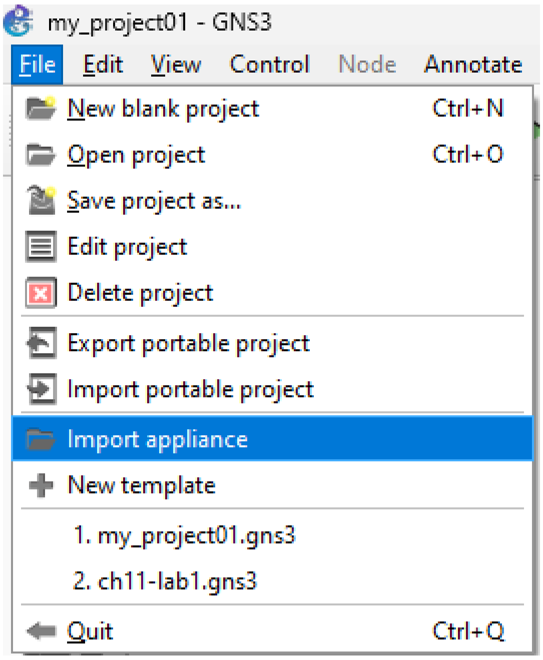
0.0

admin | Logout | Last Login Time: 06/21/2023 04:47:46 | Session Expire Time: 07/23/2023 02:48:59 | Not Ready | Tasks | Language

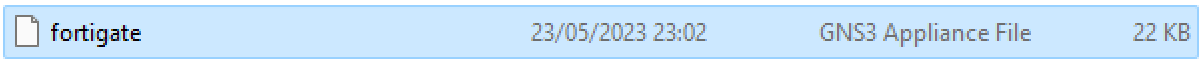
This completes Palo Alto Firewall configuration for Chapters 17-21. Let's configure the Fortinet firewall for Chapters 17-18.

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.

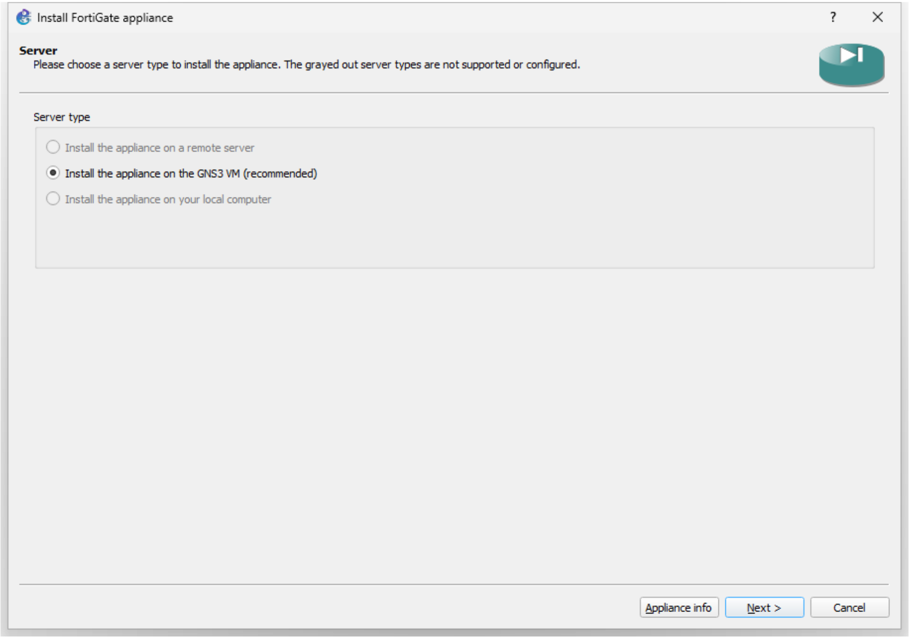


Step 2: Navigate to your Downloads folder and locate the file named 'fortigate.gns3a'. Select the file to open in the GNS3 Import appliance.



fortigate 23/05/2023 23:02 GNS3 Appliance File 22 KB

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

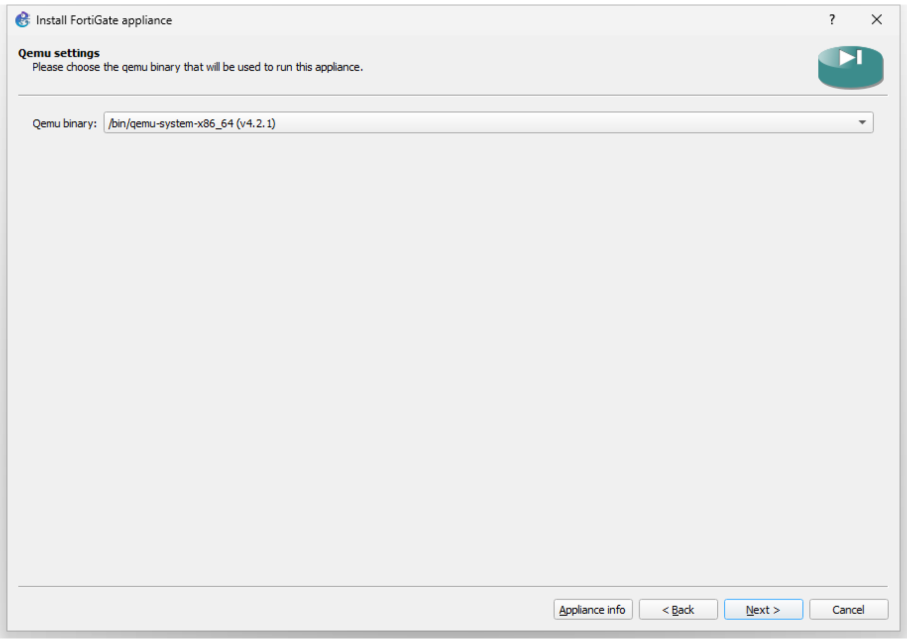


Install FortiGate appliance

Server
Please choose a server type to install the appliance. The grayed out server types are not supported or configured.

Server type
○ Install the appliance on a remote server
● Install the appliance on the GNS3 VM (recommended)
○ Install the appliance on your local computer

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

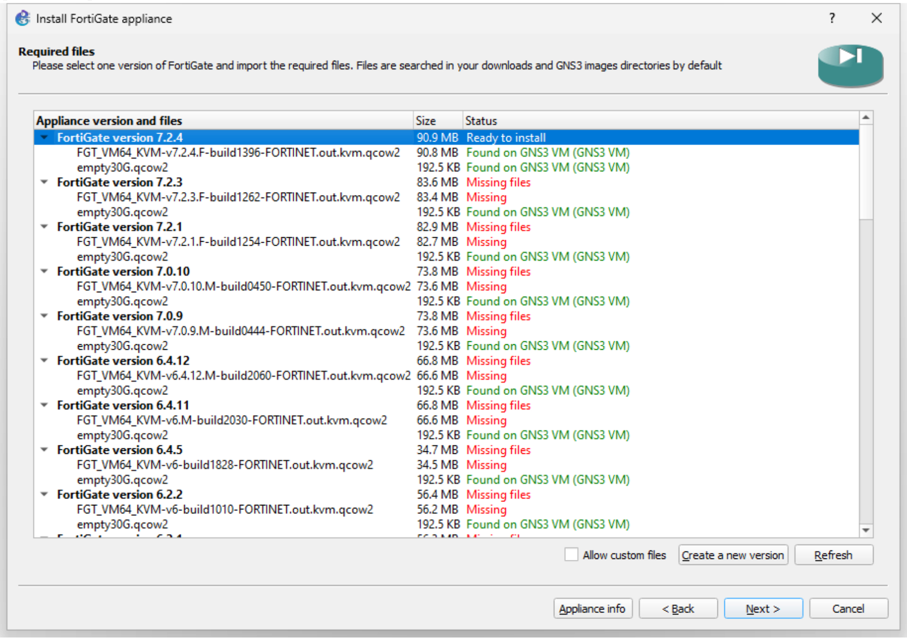


Install FortiGate appliance

Qemu settings
Please choose the qemu binary that will be used to run this appliance.

Qemu binary: /bin/qemu-system-x86_64 (v4.2.1)

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.



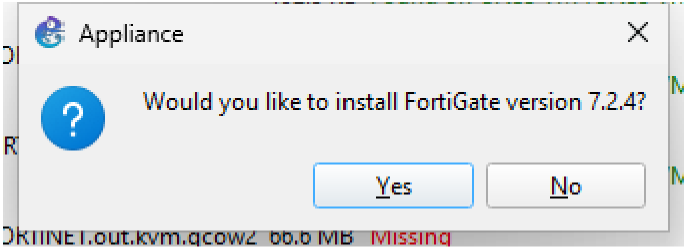
Install FortiGate appliance

Required files
Please select one version of FortiGate and import the required files. Files are searched in your downloads and GNS3 images directories by default

Appliance version and files	Size	Status
FortiGate version 7.2.4	90.9 MB	Ready to install
FGT_VM64_KVM-v7.2.4.F-build1396-FORTINET.out.kvm.qcow2	90.8 MB	Found on GNS3 VM (GNS3 VM)
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
FortiGate version 7.2.3	83.6 MB	Missing files
FGT_VM64_KVM-v7.2.3.F-build1262-FORTINET.out.kvm.qcow2	83.4 MB	Missing
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
FortiGate version 7.2.1	82.9 MB	Missing files
FGT_VM64_KVM-v7.2.1.F-build1254-FORTINET.out.kvm.qcow2	82.7 MB	Missing
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
FortiGate version 7.0.10	73.8 MB	Missing files
FGT_VM64_KVM-v7.0.10.M-build0450-FORTINET.out.kvm.qcow2	73.6 MB	Missing
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
FortiGate version 7.0.9	73.8 MB	Missing files
FGT_VM64_KVM-v7.0.9.M-build0444-FORTINET.out.kvm.qcow2	73.6 MB	Missing
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
FortiGate version 6.4.12	66.8 MB	Missing files
FGT_VM64_KVM-v6.4.12.M-build2060-FORTINET.out.kvm.qcow2	66.6 MB	Missing
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
FortiGate version 6.4.11	66.8 MB	Missing files
FGT_VM64_KVM-v6.M-build2030-FORTINET.out.kvm.qcow2	66.6 MB	Missing
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
FortiGate version 6.4.5	34.7 MB	Missing files
FGT_VM64_KVM-v6-build1828-FORTINET.out.kvm.qcow2	34.5 MB	Missing
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
FortiGate version 6.2.2	56.4 MB	Missing files
FGT_VM64_KVM-v6-build1010-FORTINET.out.kvm.qcow2	56.2 MB	Missing
empty30G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)

□ Allow custom files

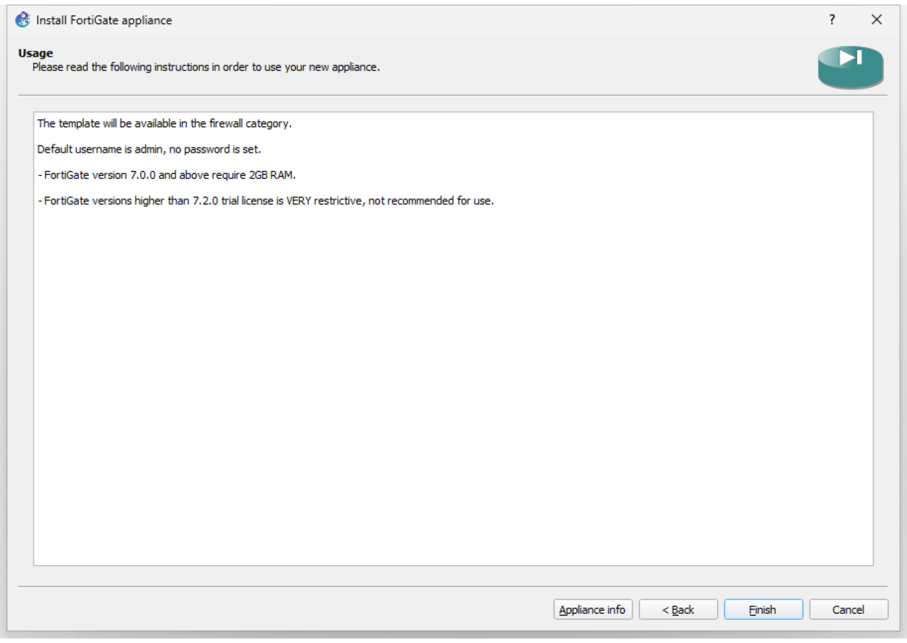
Step 6: Click on the [Yes] button to continue with the installation.



Appliance

Would you like to install FortiGate version 7.2.4?

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



Install FortiGate appliance

Usage
Please read the following instructions in order to use your new appliance.

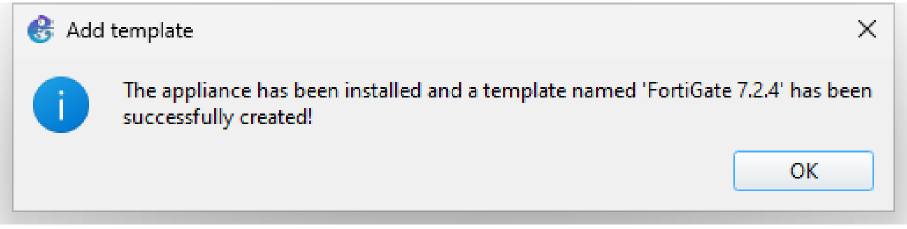
The template will be available in the firewall category.

Default username is admin, no password is set.

- FortiGate version 7.0.0 and above require 2GB RAM.

- FortiGate versions higher than 7.2.0 trial license is VERY restrictive, not recommended for use.

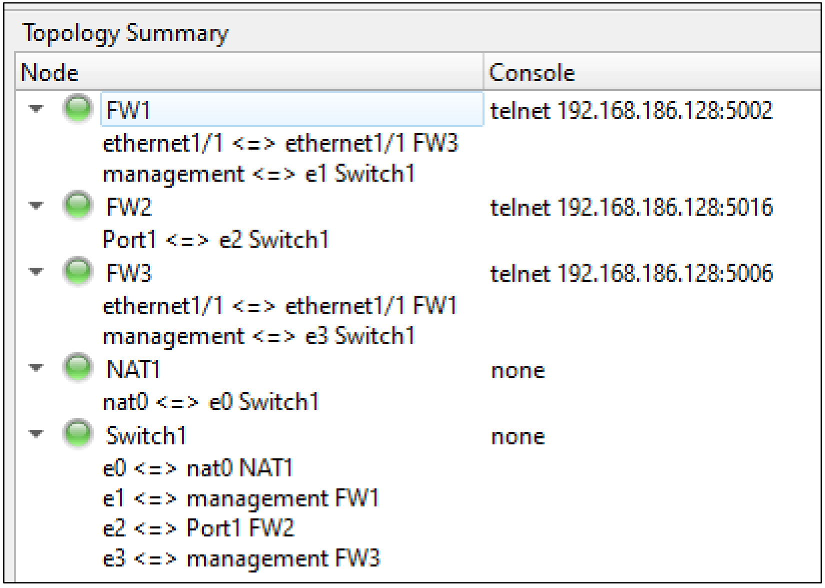
Step 8: Click on the [OK] button to complete the installation.



Add template

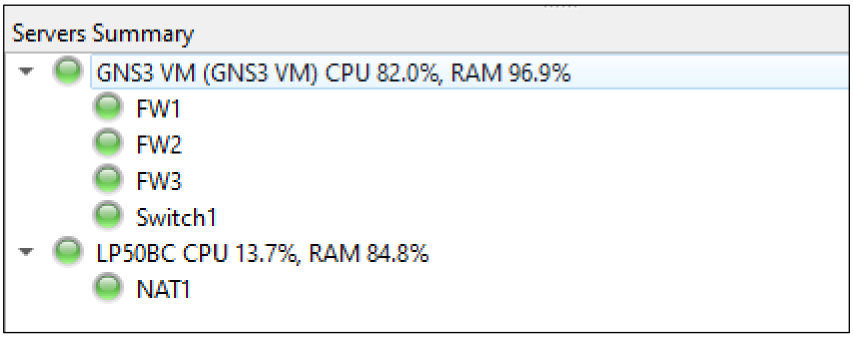
The appliance has been installed and a template named 'FortiGate 7.2.4' has been successfully created!

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. Use GNS3 hostname option to change the hostnames and enable display connections option to show the connecting interfaces. Finally, Power on the new Fortinet firewall.



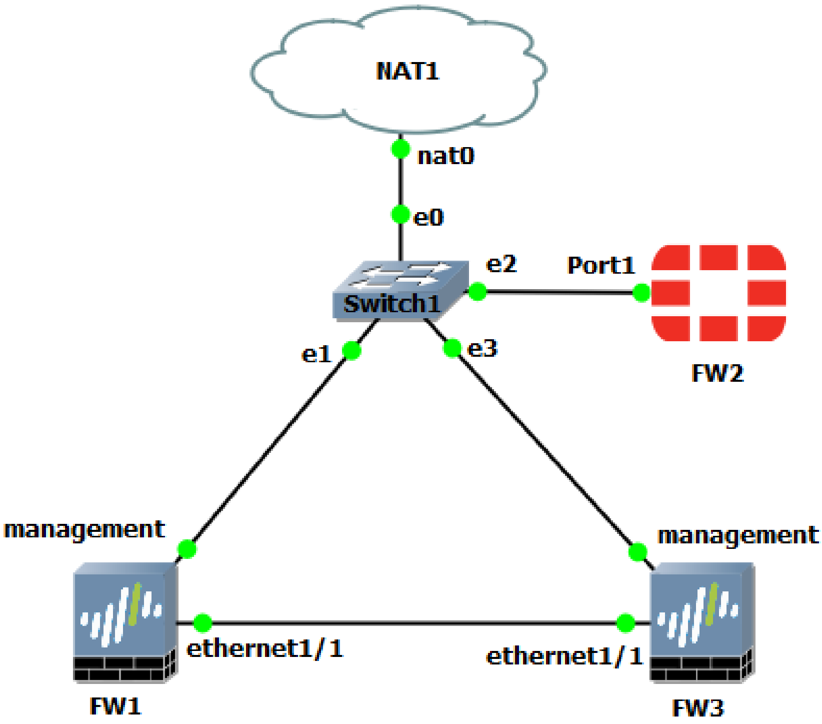
Topology Summary

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

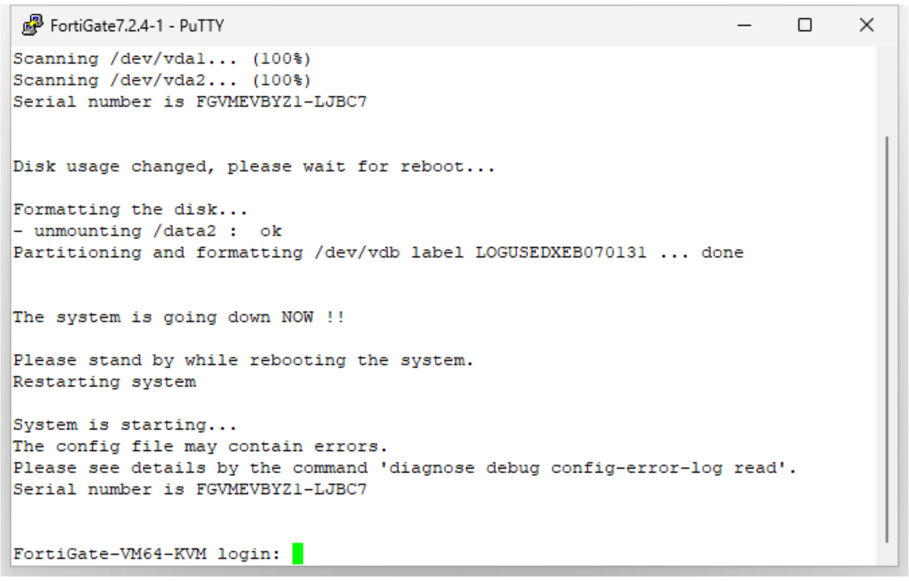


Servers Summary
- GNS3 VM (GNS3 VM) CPU 82.0%, RAM 96.9%
  - FW1
  - FW2
  - FW3
  - Switch1
- LP50BC CPU 13.7%, RAM 84.8%
  - NAT1

Please note, this lab topology will be used in the chapters 17-20, so keep this GNS3 project handy.



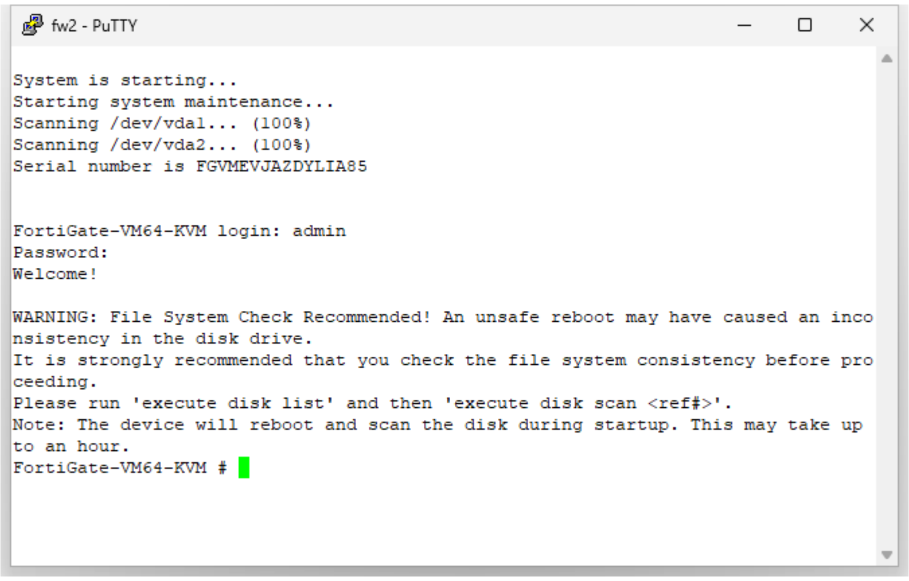
Step 10: Double-click on the FortiGate icon and it will open the SSH session on the Putty. If your software loads up and you get the first login prompt, then you know that the installation has been completed successfully and you are ready to go.



```
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!
```



```

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 inco
nsistency in the disk drive.
It is strongly recommended that you check the file system consistency before pro
ceeding.
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	Download

PA-VM 10.0.0

File	MD5	Size	
PA-VM-KVM-10.0.0.qcow2	d73a41e4d8f6f5a5291fde08b79a071e	3059 MB	Download

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	Download
empty30G.qcow2	3411a599e822f2ac6be560a26405821a	0 MB	Download