

Chapter 11 Pre-task 5, Installing the Microsoft Loopback Adapter to allow Host PC to communicate to GNS3 VMs, featuring Palo Alto PA-VM and Fortinet FortiGate (Optional)

| | |
|----------------------|---|
| File name: | Ch10_Pre-task5_Host_PC_Loopback_GNS3_Installation_Optional.pdf |
| Version: | 1.0 |
| Created on: | 29/May/2023 |
| Download URL: | https://github.com/ansnetauto/apress_ansnetauto |

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 & 2023.** 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 towards mastering Ansible/Python network automation.

What's required?

| | |
|-----------------------------|---------------------------|
| Host OS: | Windows 11 |
| Desktop Hypervisor: | VMware Workstation 17 Pro |
| File name: | N/A |
| Internet connection: | Yes |

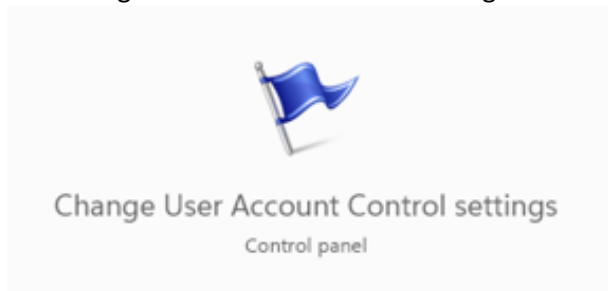
Warning! The software used in this guide may include a combination of open-source and proprietary software. Readers can search for most of the open-source software on the internet. However, the authors are unable to legally provide the proprietary software. Please ensure that you acquire the proprietary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

Welcome to this comprehensive guide, designed to offer readers an alternative method for managing devices running on GNS3 VM directly from their Host PC (your PC/Laptop). By utilizing Microsoft Loopback and a Cisco router, we present you with an additional option to streamline the process. Although it involves several steps, we will delve right into them, ensuring you have a clear understanding throughout. Also, please be reminded that this document is based on the content of "Introduction to Python Network Automation: The First Journey" written by Brendan Choi in 2021 & 2023.

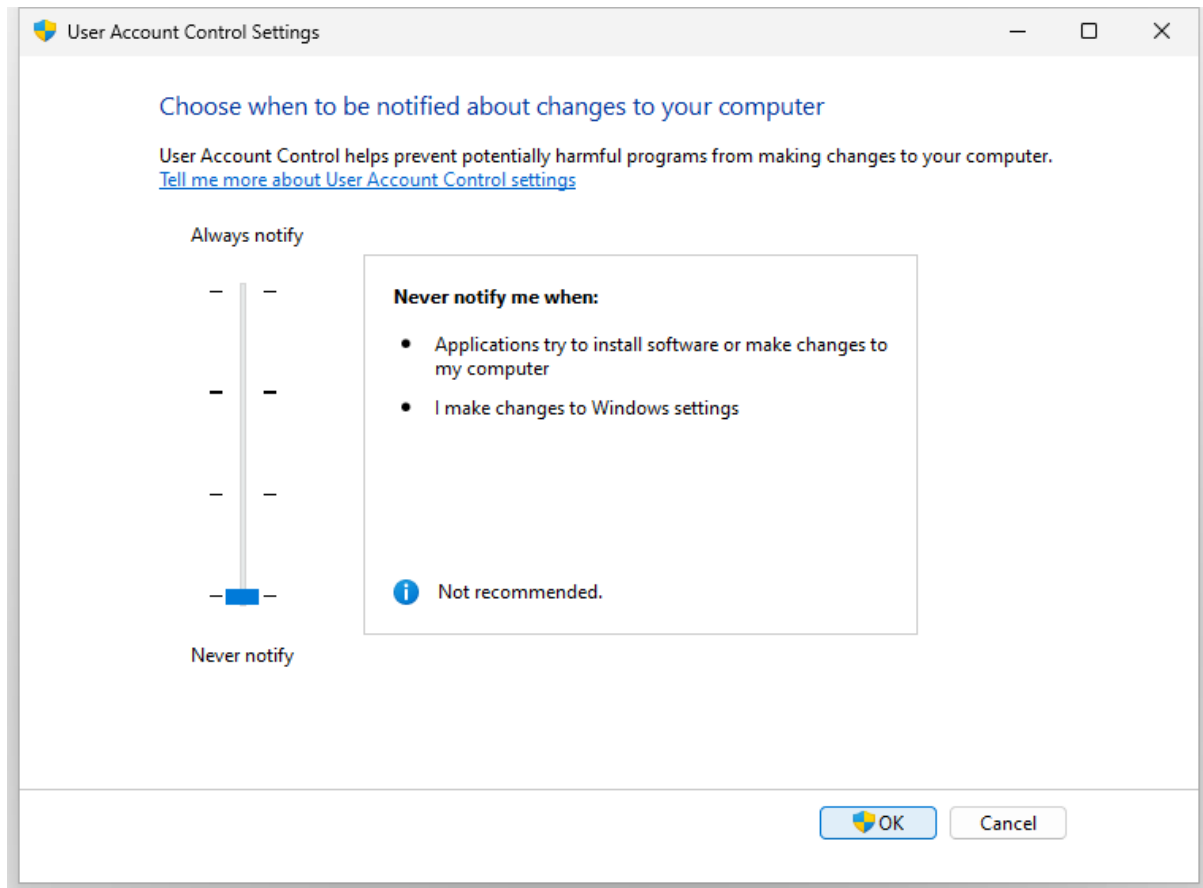
Installation Steps:

In this section, we will guide you through the installation process of the Microsoft Loopback Adapter. This adapter enables seamless communication between your Host PC and GNS3 VMs, including popular virtual appliances such as Palo Alto PA-VM and Fortinet FortiGate. Follow these steps to set it up successfully.

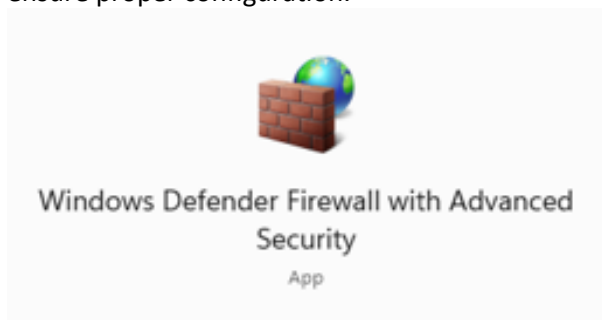
Step 1: To allow a smooth communication between the Host PC and the virtual devices running on GNS3 VM, we have to make some changes to your Windows 11 OS. First, let's make some changes on "Change User Account Control settings".



Move the scroll-bar down to Never notify and click on the [OK] key.

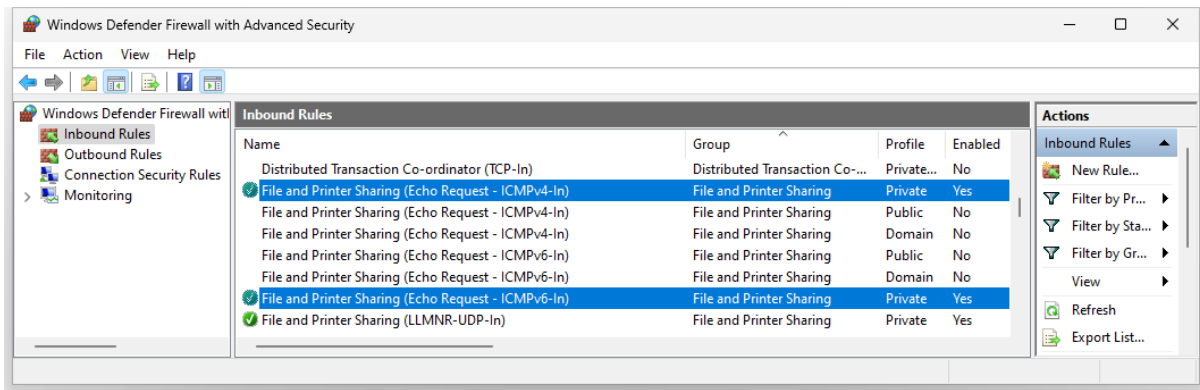


Step 2: Next, you need to check the Windows Defender Firewall with Advanced Security settings to ensure proper configuration.

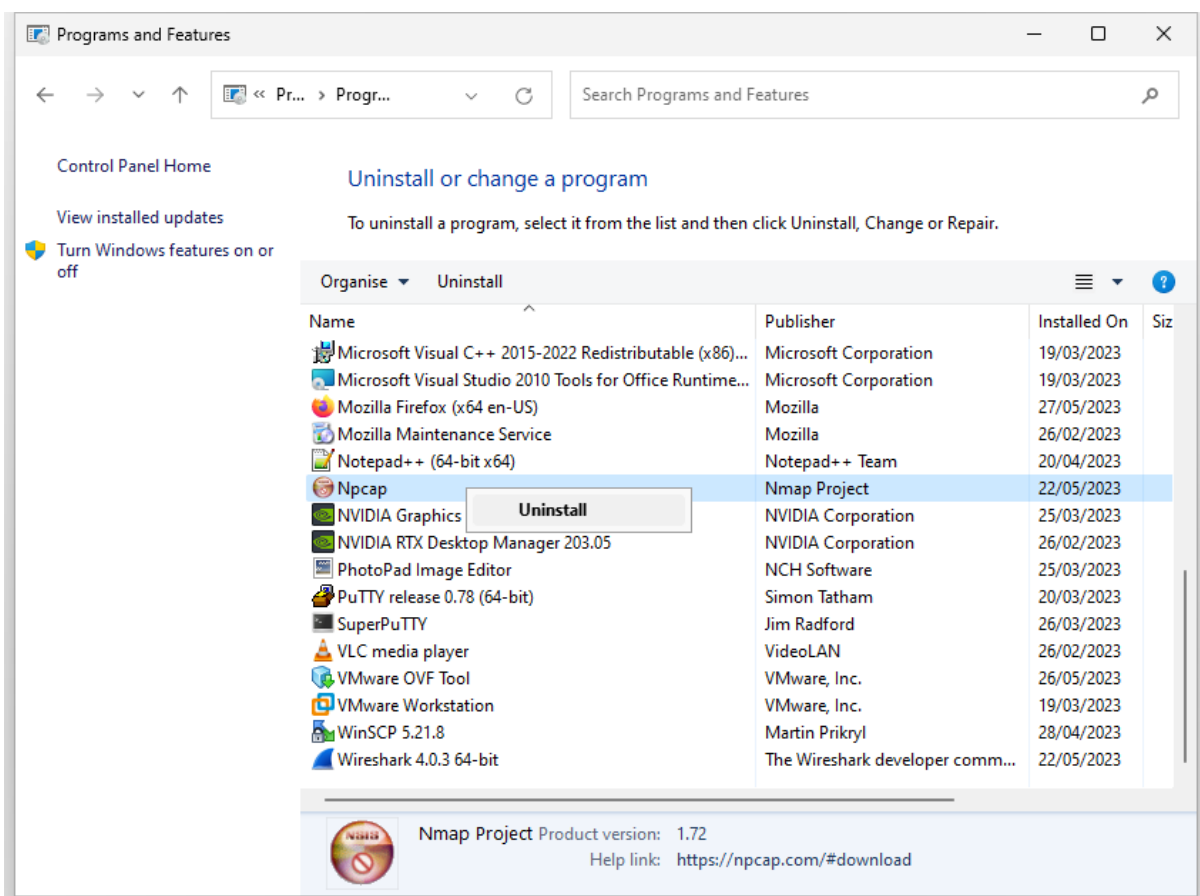


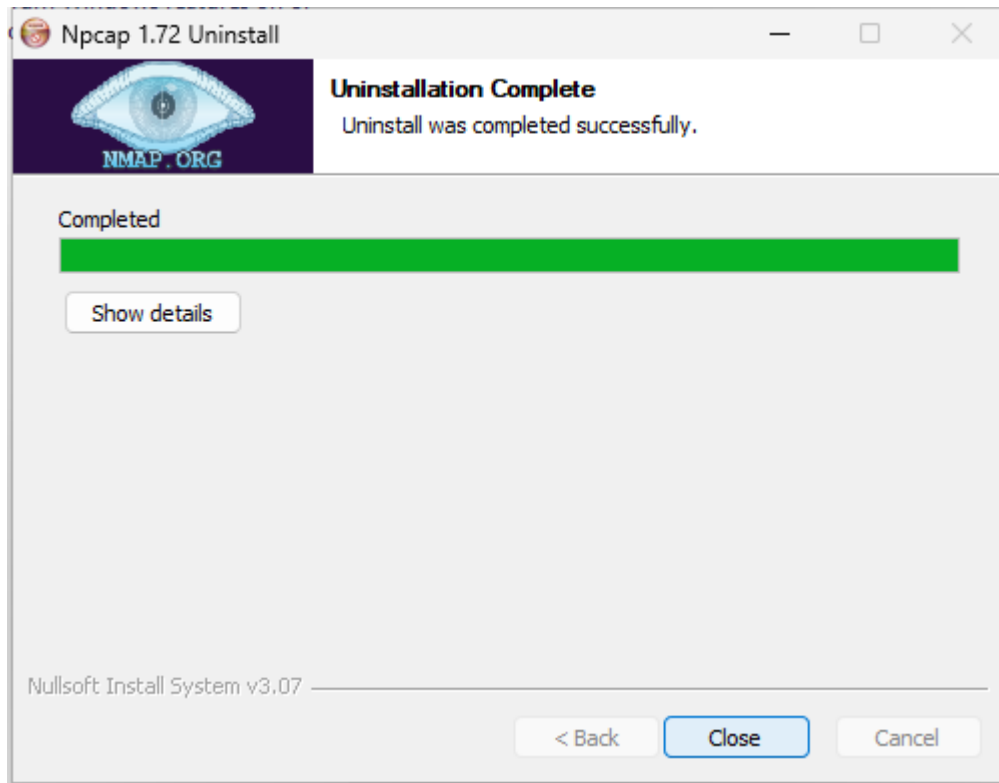
Ensure that the following two settings are enabled and active. While these settings are typically enabled by default, if they have been disabled for any reason, please proceed to re-enable them. This will allow ICMP and IP communication.

- File and Printer Sharing (Echo Request – CIMPv4-In) for Private Profile.
- File and Printer Sharing (Echo Request – CIMPv6-In) for Private Profile.



Step 3: When you install GNS3, the later version of the software installs Npcap instead of WinPcap. This can also cause malfunctions in ICMP and IP communication. To resolve this issue, open the "Uninstall or change a program" option from the control panel and uninstall Npcap.

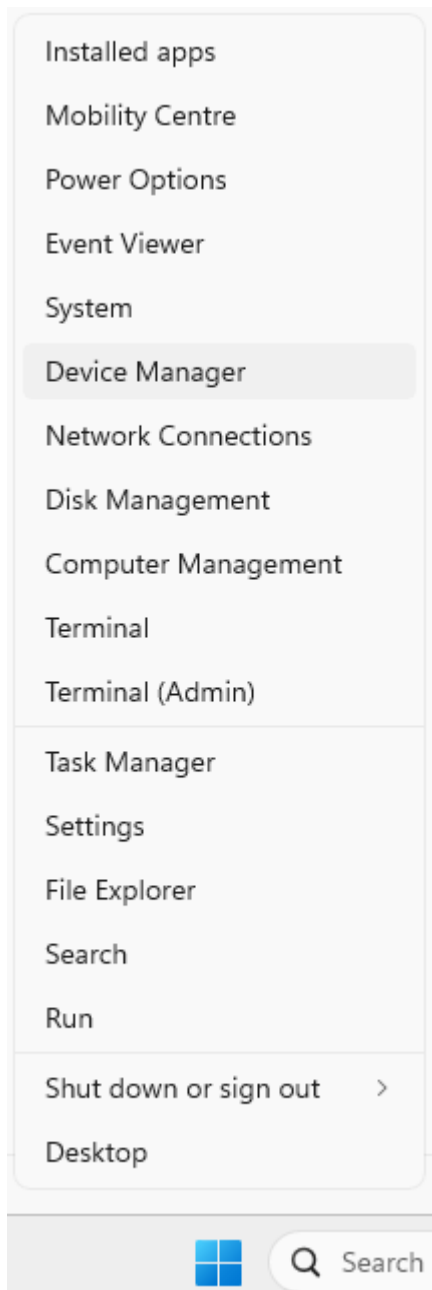




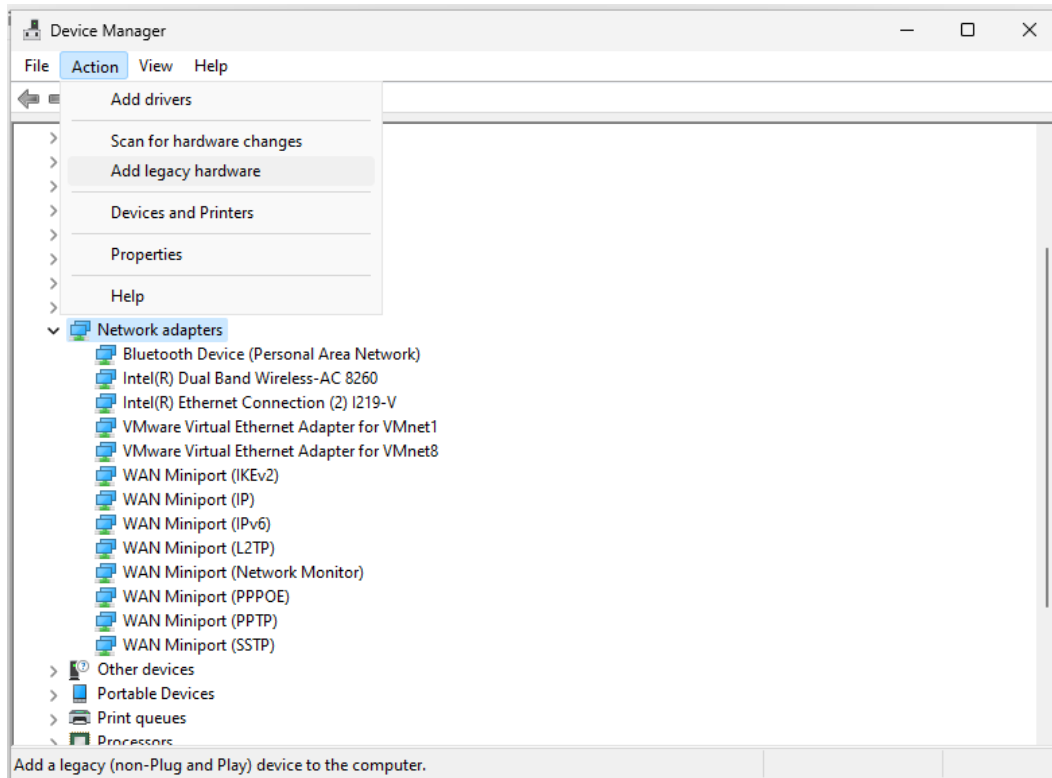
Step 4: Go to the internet and download WinPcap 4.1.3.exe from the official website (<https://www.winpcap.org/install/>), and install the downloaded software. Then restart your PC/Laptop.

| | | | |
|---------------|------------------|-------------|--------|
| WinPcap_4_1_3 | 29/05/2023 11:56 | Application | 894 KB |
|---------------|------------------|-------------|--------|

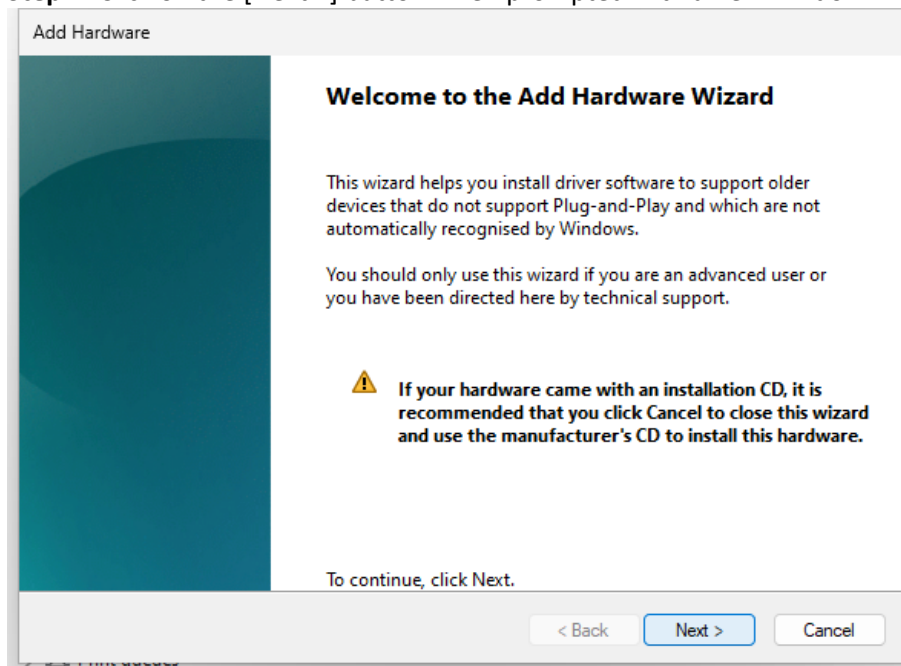
Step 5: Right-click the Microsoft icon in the taskbar menu and select Device Manager.



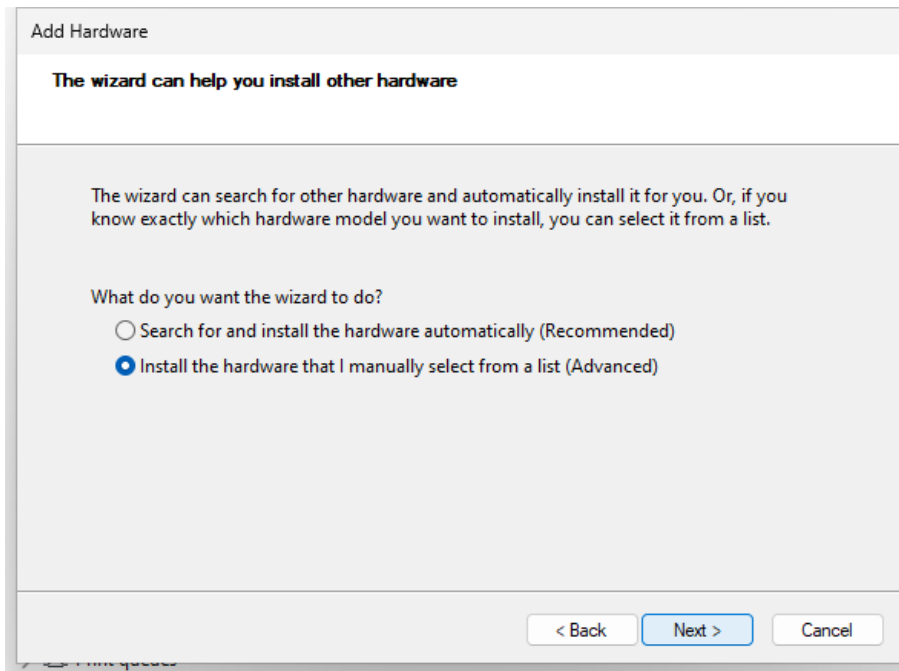
Step 6: Highlight the Network adapters, and then click on Action > Add legacy hardware.



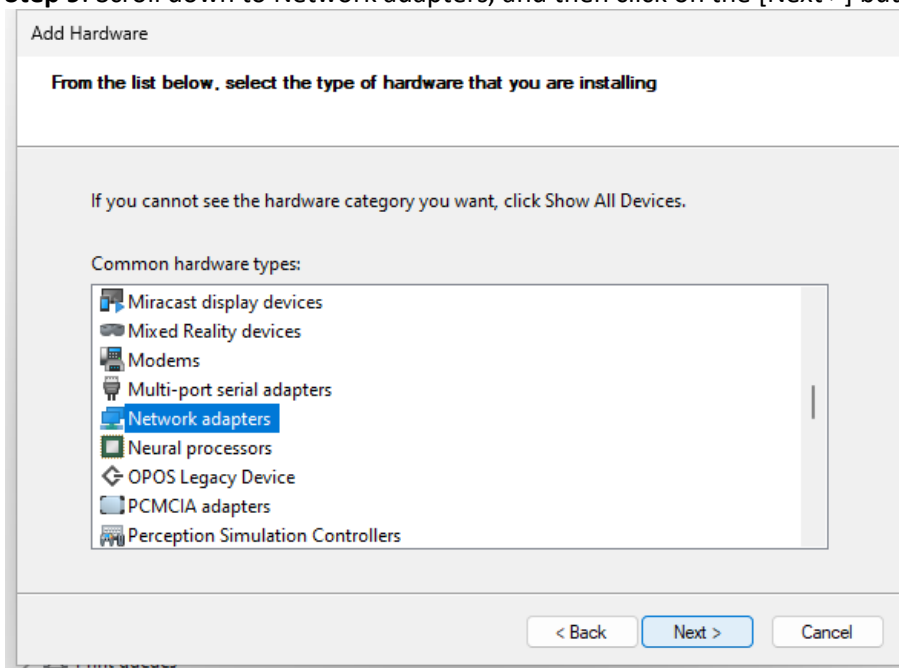
Step 7: Click on the [Next >] button when prompted with a new window.



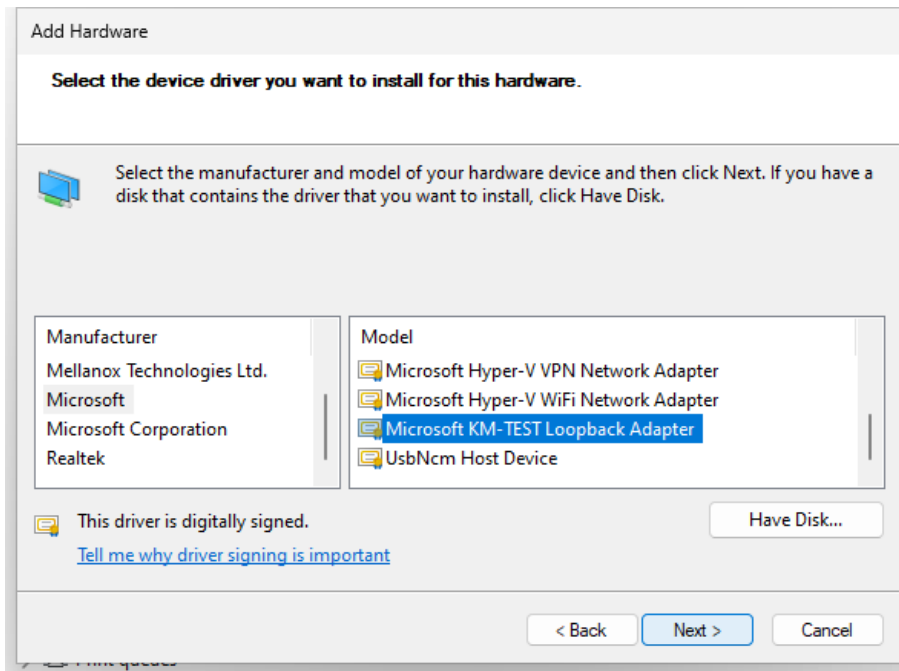
Step 8: On the next window, select "Install the hardware that I manually select from a list (Advanced)" and click on the [Next >] button.



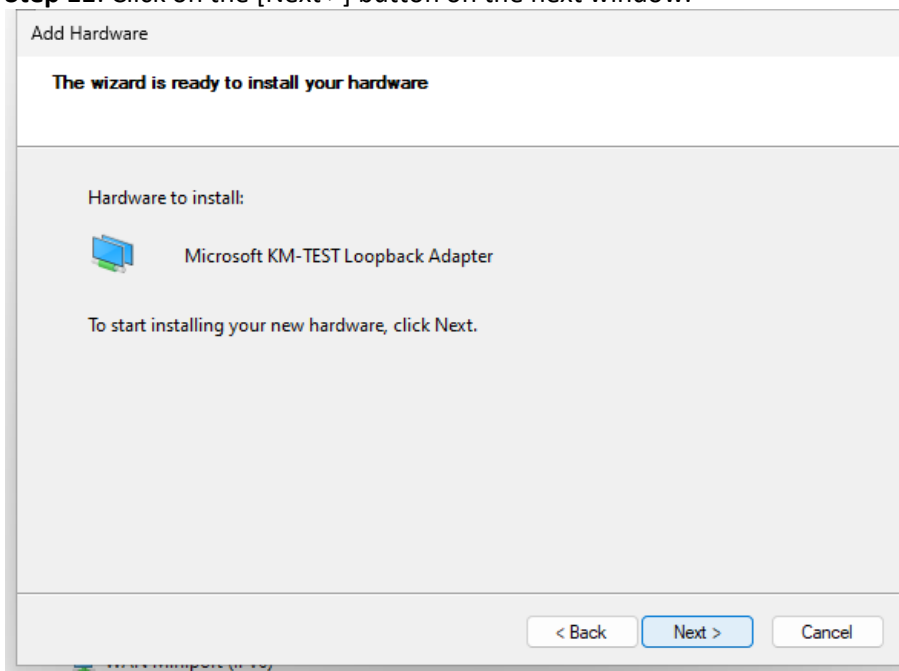
Step 9: Scroll down to Network adapters, and then click on the [Next >] button.



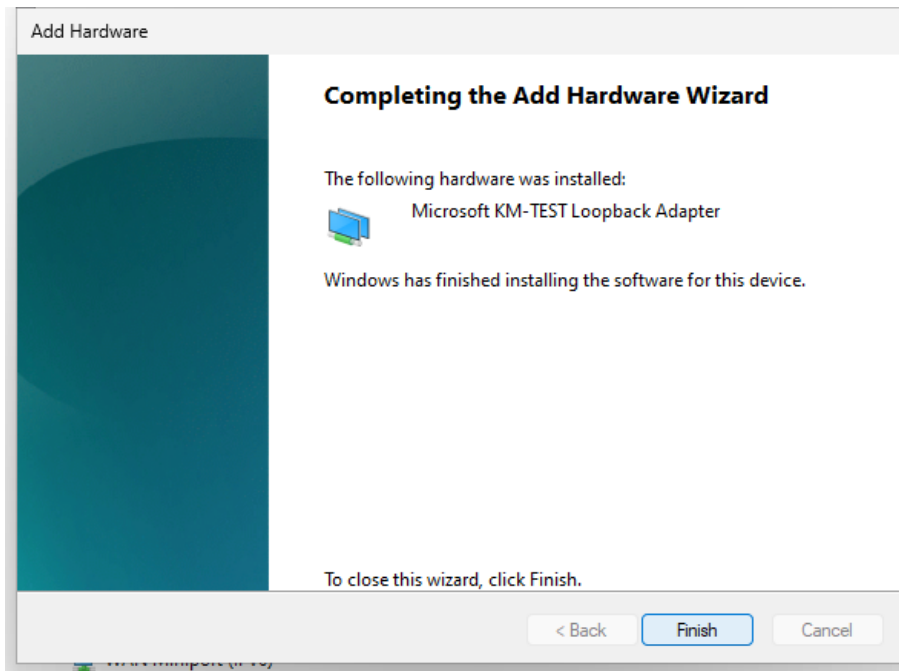
Step 10: Select Microsoft as the Manufacturer, then highlight the Microsoft KM-Test Loopback Adapter in the Model options, and click on the [Next >] button.



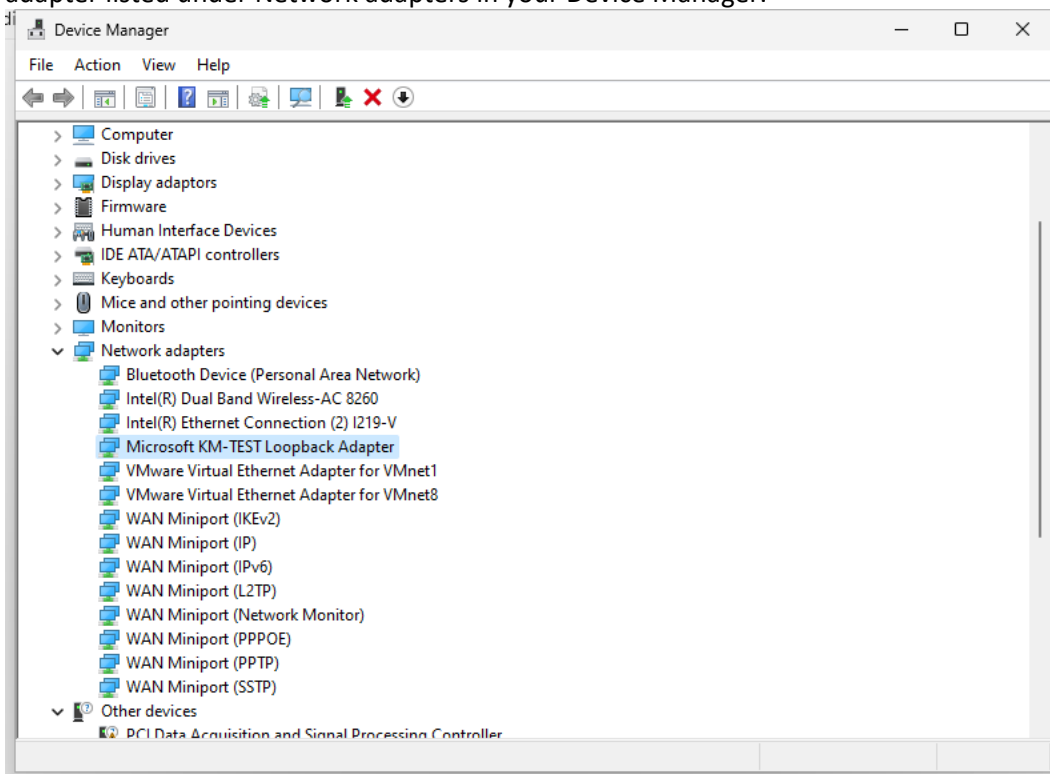
Step 11: Click on the [Next >] button on the next window.



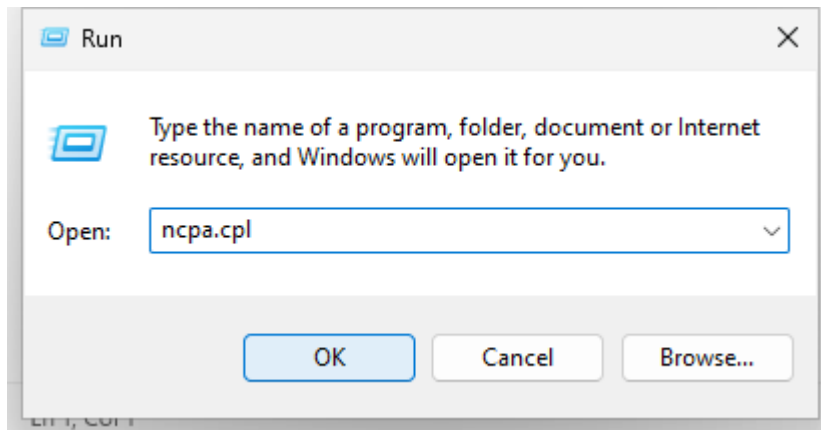
Step 12: Click on the [Finish] button to complete the MS Loopback Adapter.



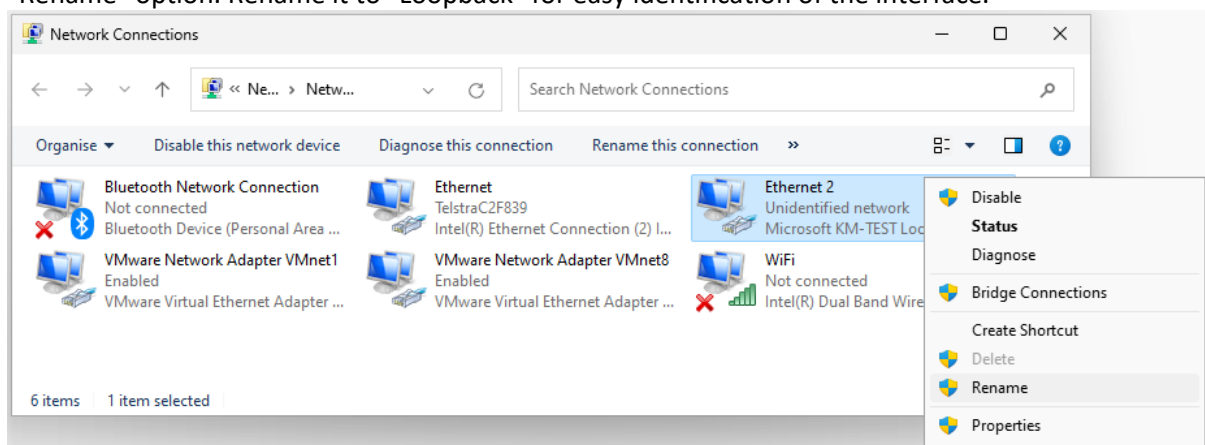
Step 13: If the Microsoft Loopback Adapter has been installed successfully, you should see the adapter listed under Network adapters in your Device Manager.



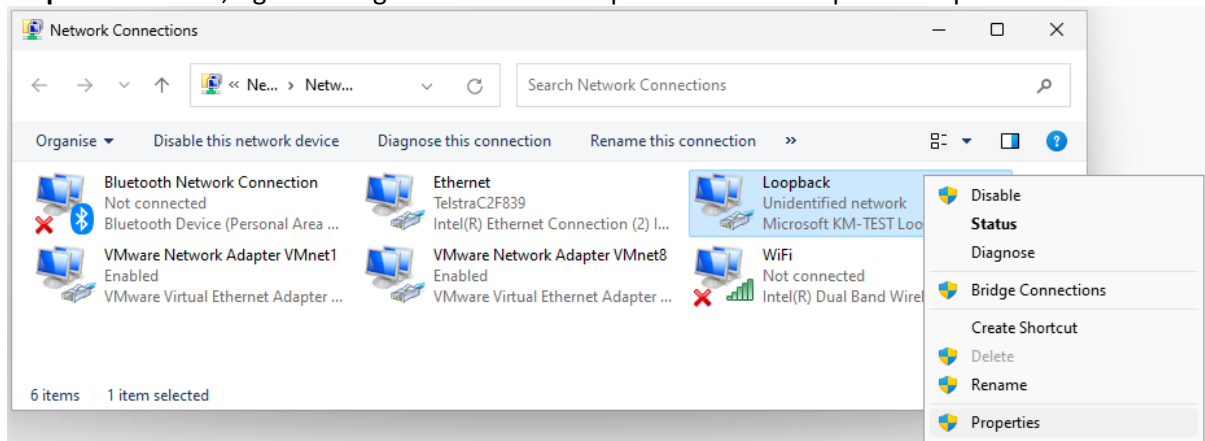
Step 14: Go to the Search bar and type "Run" to start the Windows Run. Then, type "ncpa.cpl" to launch the Network Connections window. Alternatively, you can also access it by navigating through the Control Panel menu.



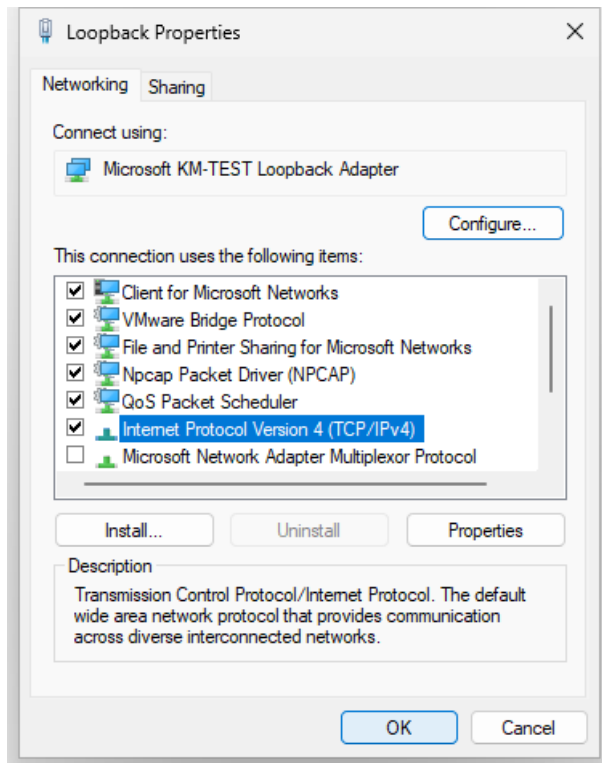
Step 15: Now, locate the newly added Microsoft Loopback adapter and right-click on it to select the "Rename" option. Rename it to "Loopback" for easy identification of the interface.



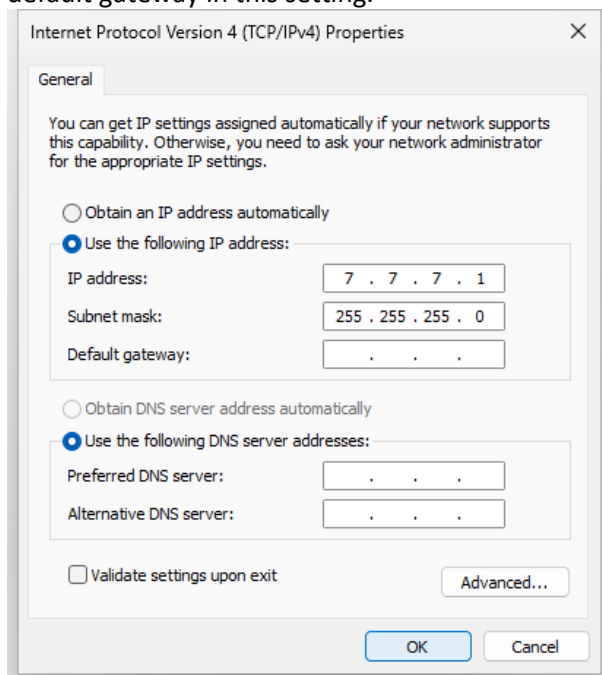
Step 16: This time, right-click again and select "Properties" of the Loopback adapter.



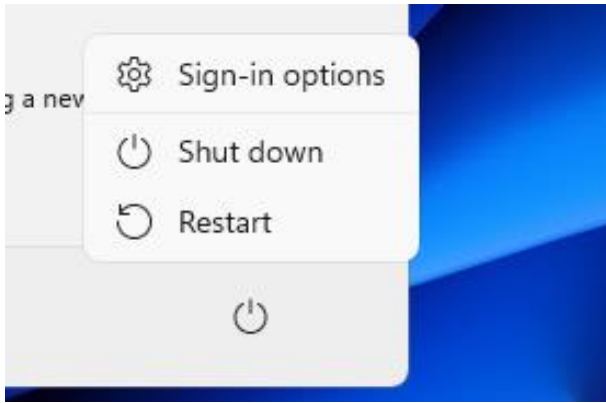
Step 17: Select "Internet Protocol Version (TCP/IPv4)" and then click on the "Properties" button to open the "Internet Protocol Version 4 (TCP/IPv4) Properties."



Step 18: Assign your IP address as 7.7.7.1 with a subnet of /24. There is no need to configure a default gateway in this setting.



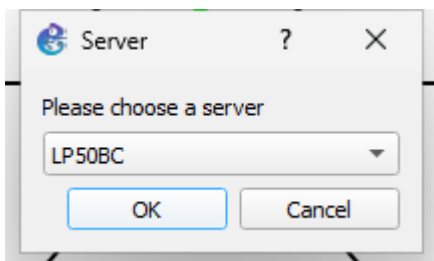
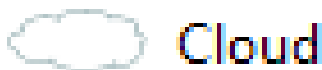
Step19 : Restart your PC to apply the new settings.



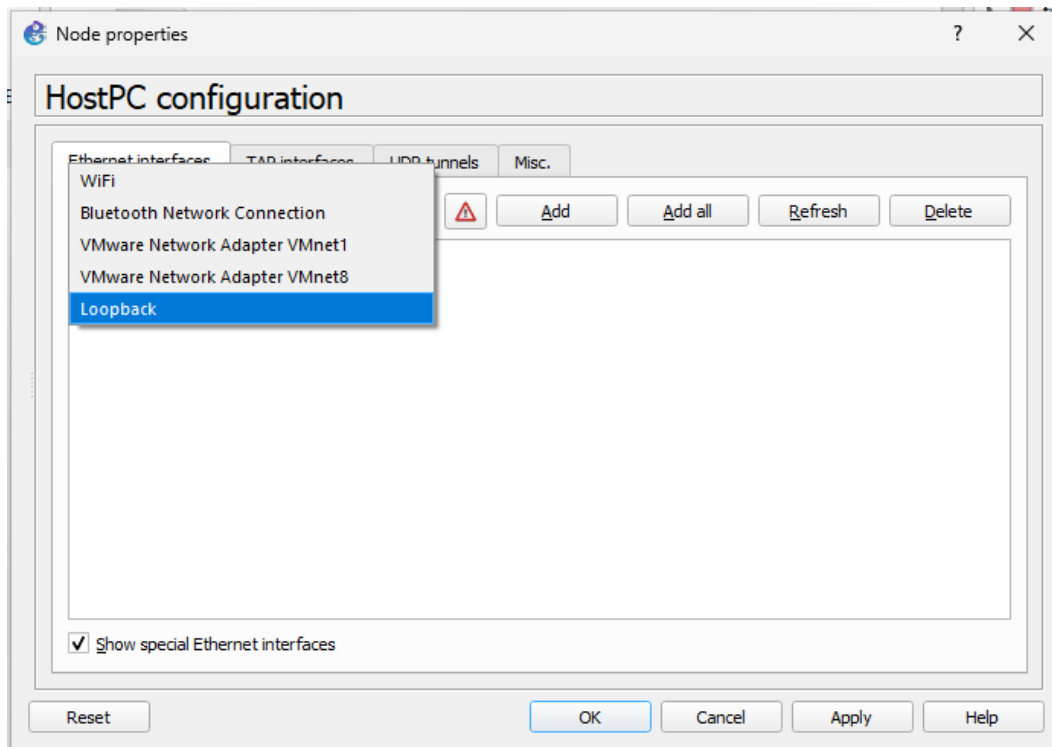
Connecting Host PC to GNS3 VM

Now continue to GNS3 configuration and connection validations.

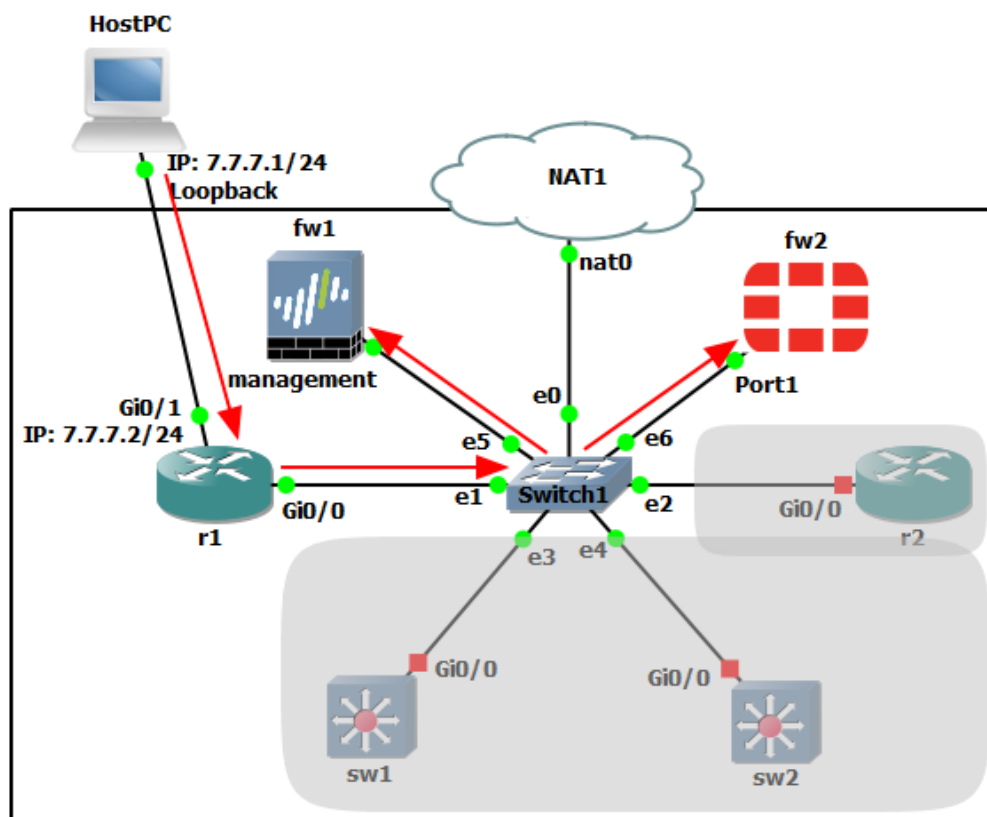
Step 1: Go to GNS3 and drag and drop a Cloud from the "All devices" menu. Make sure you select the correct cloud, as this is just a cloud and not the NAT.



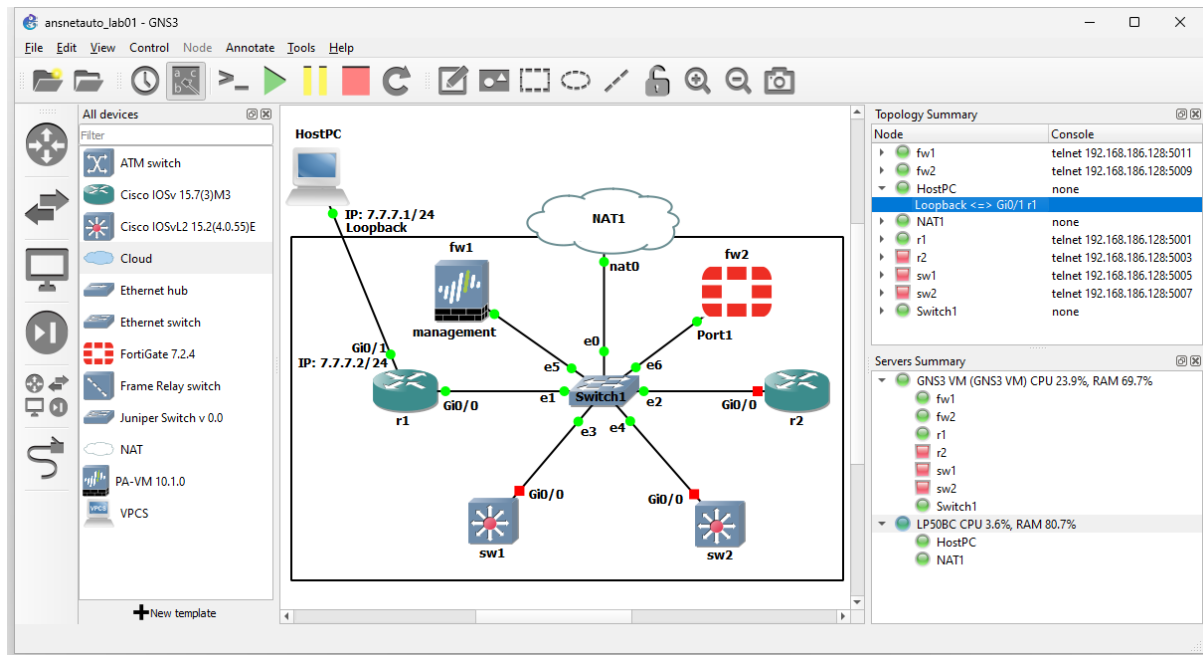
Step 2: After placing the Cloud on the GNS3 Topology canvas, position your mouse cursor over the icon and right-click to open the "Configure" (Node properties) menu. Make sure to checkmark "Show special Ethernet interfaces," then use the dropdown menu to select "Loopback" and add the interface. Optionally, you can remove the original Ethernet interface.



Step 3: Referring to the following GNS3 Topology, we are focusing on the Host PC, r1, fw1, and fw2. We will utilize ICMP and HTTPS to test our communication.



Step 4: Additionally, refer to the Topology Summary and Server Summary for further reference.



Step 5: Double-click on the r1 icon to open a PuTTY session, allowing you to configure the device using the provided configuration file.

```
!
conf t
hostname r1
!
ip domain name ansnetauto.net
ip name-server 192.168.127.2
!
username jdoe privilege 15 secret Super5cret9assw0rd
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.127.2
!
line vty 0 15
login local
transport input ssh
logging synchronous
exit
!
! This is required configuration!
interface GigabitEthernet0/0
ip address 192.168.127.11 255.255.255.0
no shut
!
exit
!
crypto key generate rsa
1024
ip ssh time-out 60
ip ssh authentication-retries 2
```

```
!  
! This is required configuration!  
conf t  
interface GigabitEthernet0/1  
ip address 7.7.7.2 255.255.255.0  
no shut  
!  
end  
!  
write memory  
!  
!
```

Step 6: Now, perform the ICMP (ping) and traceroute tests to the two firewalls: PA-VM (fw1) at 192.168.127.31 and FortiGate (fw2) at 192.168.127.31.

```
C:\Users\brend>ping 192.168.127.31  
  
Pinging 192.168.127.31 with 32 bytes of data:  
Reply from 192.168.127.31: bytes=32 time=1ms TTL=64  
Reply from 192.168.127.31: bytes=32 time<1ms TTL=64  
Reply from 192.168.127.31: bytes=32 time=1ms TTL=64  
Reply from 192.168.127.31: bytes=32 time=1ms TTL=64  
  
Ping statistics for 192.168.127.31:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
C:\Users\brend>tracert 192.168.127.31  
  
Tracing route to 192.168.127.31 over a maximum of 30 hops  
  
  0  1 ms  <1 ms  <1 ms  192.168.127.31  
  
Trace complete.  
  
C:\Users\brend>ping 192.168.127.32  
  
Pinging 192.168.127.32 with 32 bytes of data:  
Reply from 192.168.127.32: bytes=32 time=1ms TTL=255  
Reply from 192.168.127.32: bytes=32 time=1ms TTL=255  
Reply from 192.168.127.32: bytes=32 time=1ms TTL=255  
Reply from 192.168.127.32: bytes=32 time=1ms TTL=255  
  
Ping statistics for 192.168.127.32:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 1ms, Maximum = 1ms, Average = 1ms  
  
C:\Users\brend>tracert 192.168.127.32
```


Tracing route to 192.168.127.32 over a maximum of 30 hops

1 2 ms 1 ms 1 ms 192.168.127.32

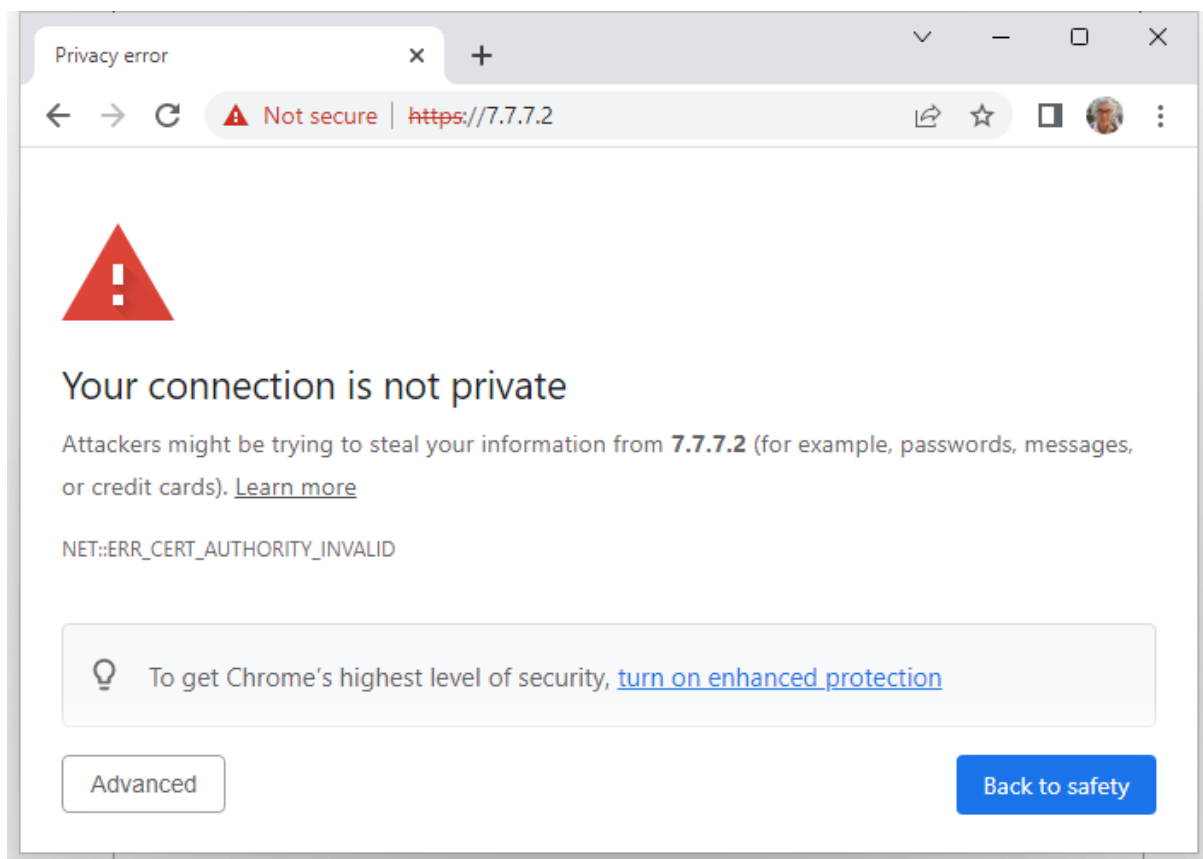
Trace complete.

Step 7: Perform the HTTPS server connectivity from the Cisco router (7.7.7.2) to the two firewalls (192.168.127.31 and 192.168.127.32).

First, perform this task on r1.

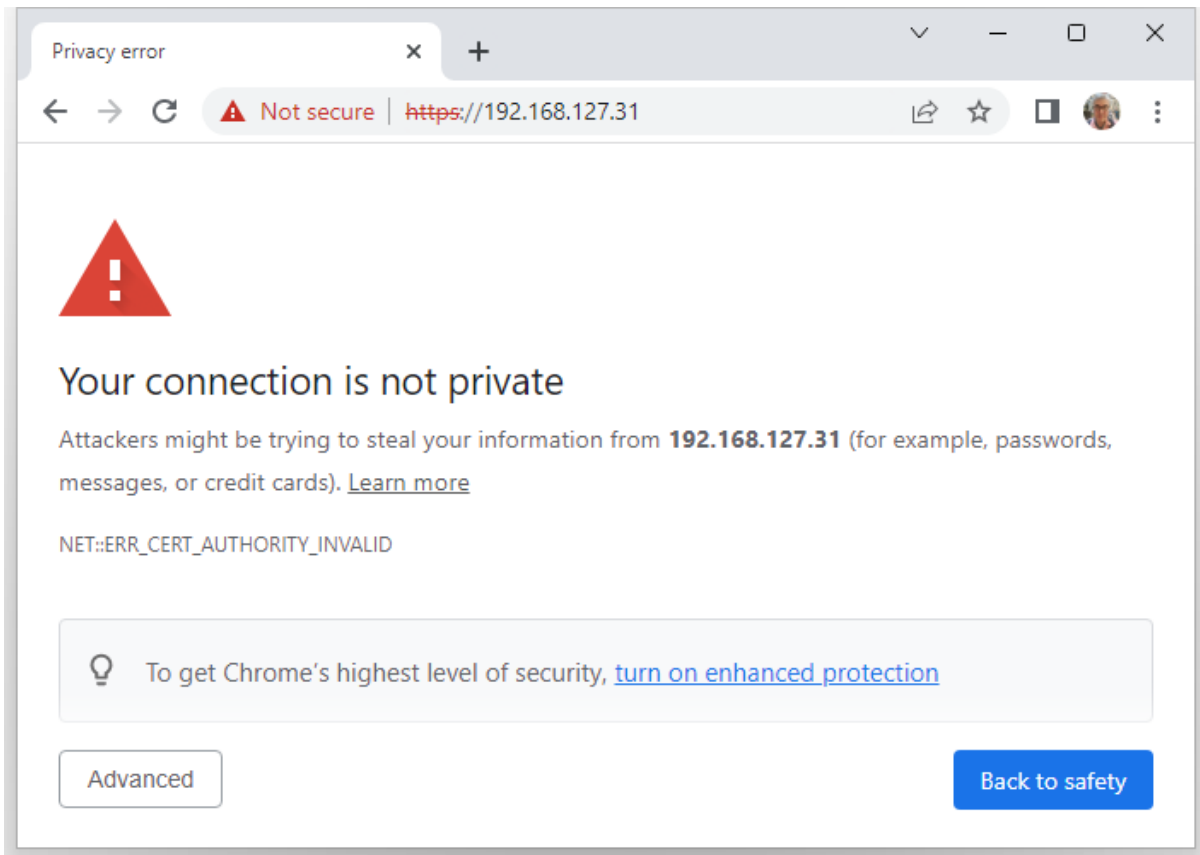
```
r1#conf t
r1(config)#ip http secure-server
CRYPTO_PKI: setting trustpoint policy TP-self-signed-4294967295 to use keypair TP-self-signed-4294967295% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
```

Use <https://7.7.7.2> to open it in the web browser. If you see the following screen, it means you are successfully connecting to the router's web interface.

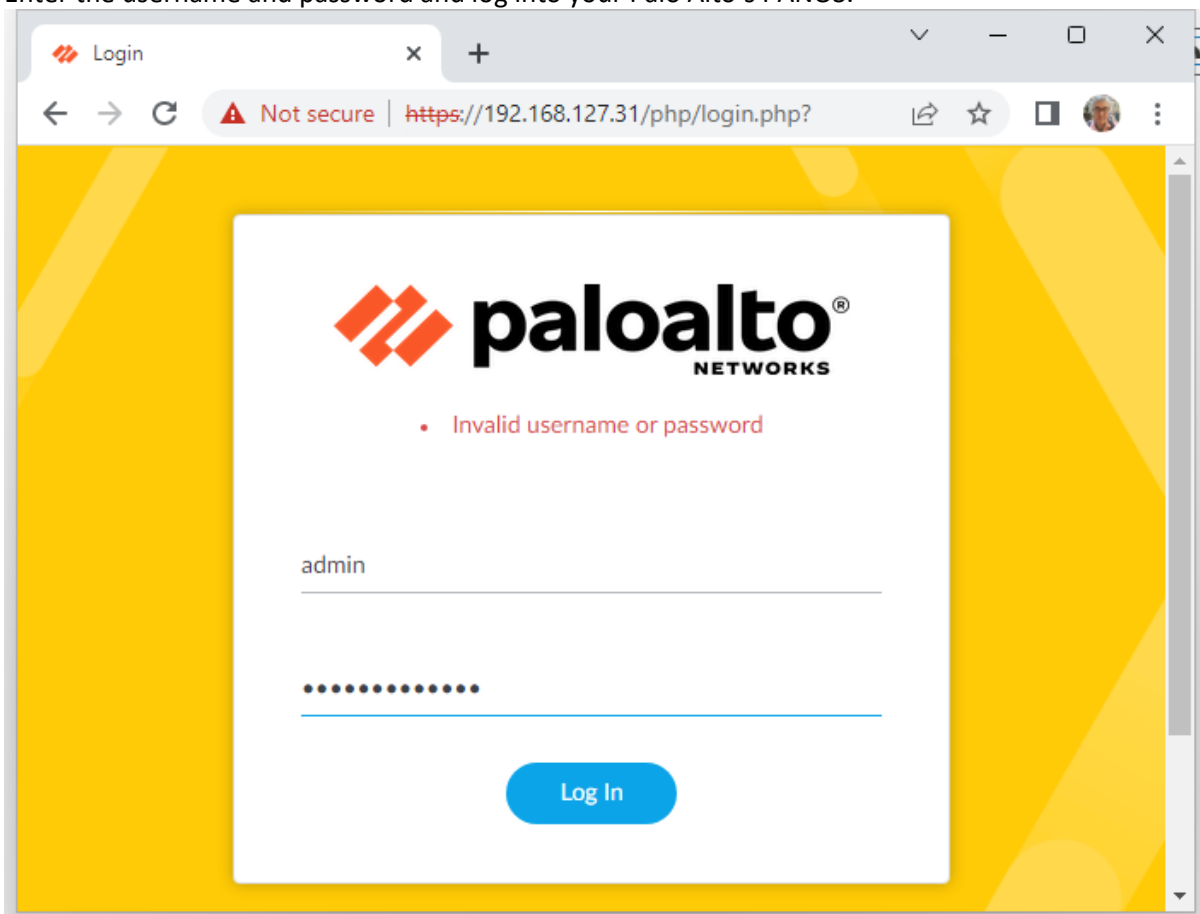


Step 8: Attempt to open the webpage of the Palo Alto PA-VM Firewall at 192.168.127.31 (This device has already been configured). Go to Advanced option and accept the risk to move to the main login page.

Access it via: <https://192.168.127.31/>



Enter the username and password and log into your Palo Alto's PANOS.



The screenshot displays the Palo Alto Networks PA-VM dashboard in a web browser. The browser address bar shows the URL `https://192.168.127.31/#dashboard:vsys1`. The dashboard is titled "Welcome to PAN-OS 10.1!" and includes a detailed announcement about the new release, highlighting features like App-ID Cloud Engine, SaaS Security Inline Subscription, and Advanced URL Filtering. Below the announcement, there is a "Close" button.

The dashboard itself is divided into several sections:

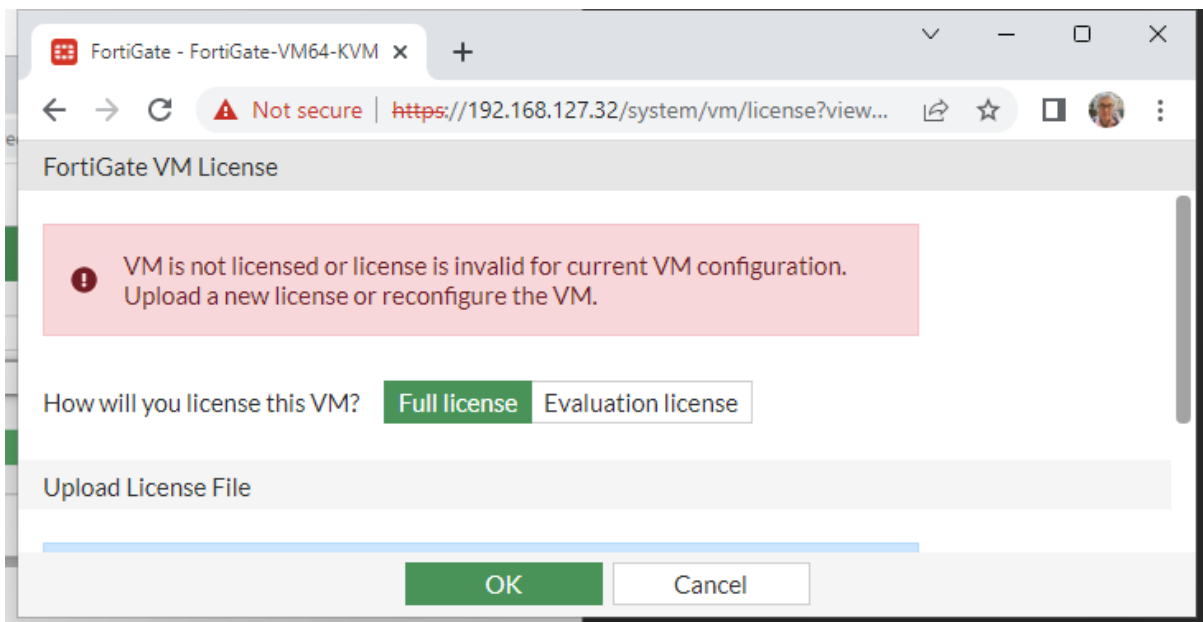
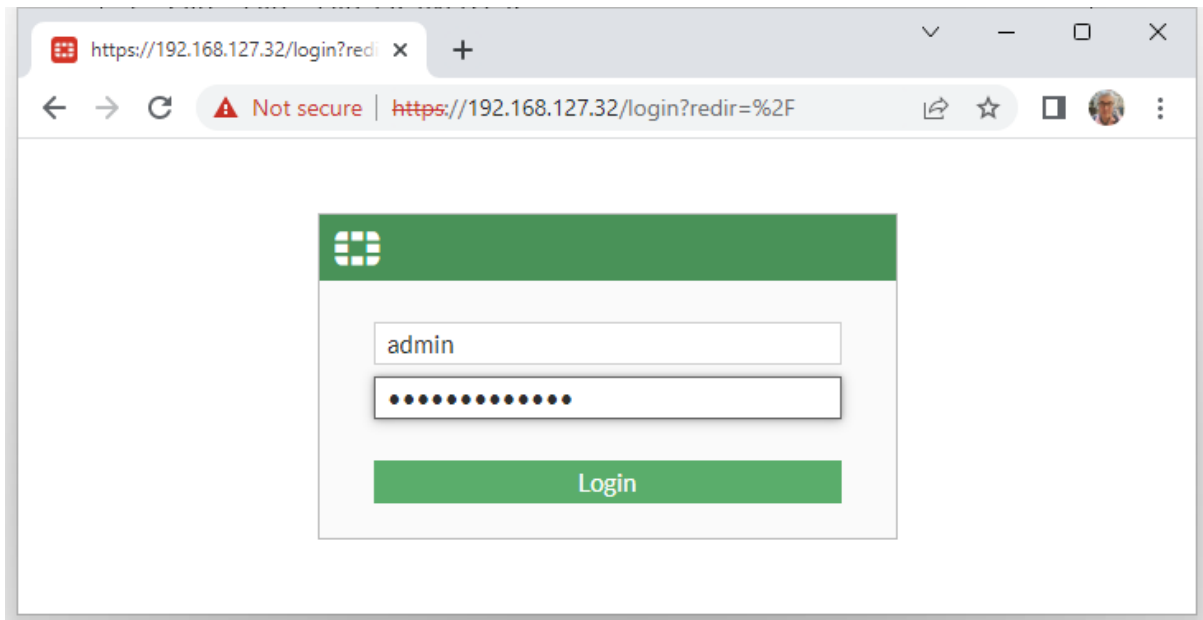
- General Information:** Displays device details for PA-VM, including MGT IP Address (192.168.127.31), MGT Netmask (255.255.255.0), MGT Default Gateway (192.168.127.2), MGT IPv6 Address (unknown), MGT IPv6 Link Local Address (fe80::e01:c8ff:fe03:0/64), MGT IPv6 Default Gateway, MGT MAC Address (0c:01:c8:03:00:00), Model (PA-VM), Serial # (unknown), CPU ID (KVM:63060000FDFB8B07), UUID (4501C803-ED30-4E36-BAE1-AF45D0390C8E), VM Cores (2), VM Memory (4031296), VM License (none), VM Capacity Tier (unknown), VM Mode (KVM), and Software Version (10.1.0).
- Logged In Admins:** A table showing active sessions for the 'admin' user from 192.168.127.1, with a session start time of 05/28 19:42:15 and an idle time of 00:00:00s.
- Data Logs:** A section indicating "No data available."
- System Logs:** A table of system events, including user logins, authentication failures for 'jdoe', and MLAV certificate failures.
- Config Logs:** A section indicating "No data available."
- Locks:** A section indicating "No locks found."
- ACC Risk Factor (Last 60 minutes):** A gauge showing a risk factor of 0.0.

The dashboard footer shows the user 'admin' is logged in, with a last login time of 05/28/2023 09:19:30 and a session expire time of 06/27/2023 19:42:15. The Palo Alto Networks logo is visible in the bottom right corner.

Step 9: Attempt to open the webpage of the FortiGate Firewall at 192.168.127.32 (This device has already been configured).

Access it via: <https://192.168.127.32/>

If you can reach the following login page and successfully log in, then you have completed the HTTPS connection test.



Now, you have successfully completed the installation and testing of Microsoft Loopback and established connections to the GNS3 VM devices. You should now be able to control the devices running on the GNS3 VMs from your Host PC/Laptop. Study hard and have fun!