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:	25/Jun/2023
Download URL:	https://github.com/ansnetauto/appress_ansnetauto
Applicable to:	Chapter 11 & 12-15

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.

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 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.

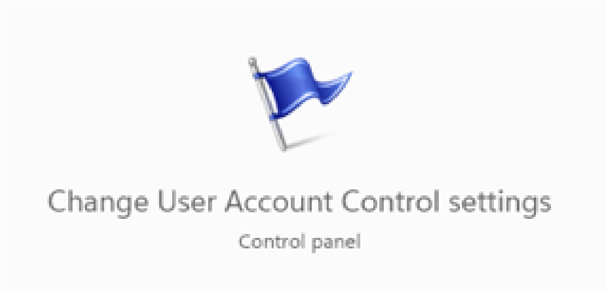
Contents

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:

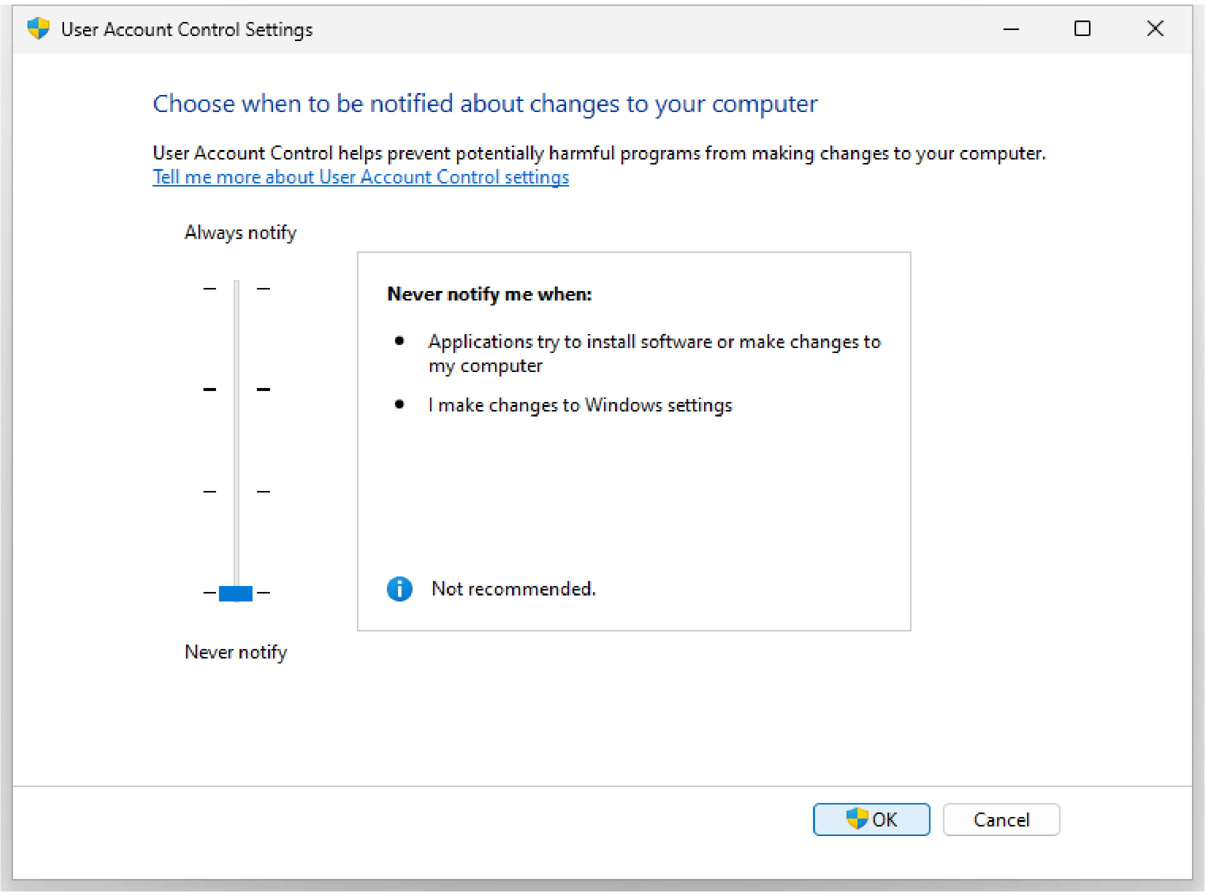
In this section, we will guide you through the installation process of the Microsoft Loopback Adapter. This adapter enables seamless communication between your Host PC and GNS3 VMs, including popular virtual appliances such as Palo Alto PA-VM and Fortinet FortiGate. Follow these steps to set it up successfully.

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".



Change User Account Control settings
Control panel

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



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Never notify me when:

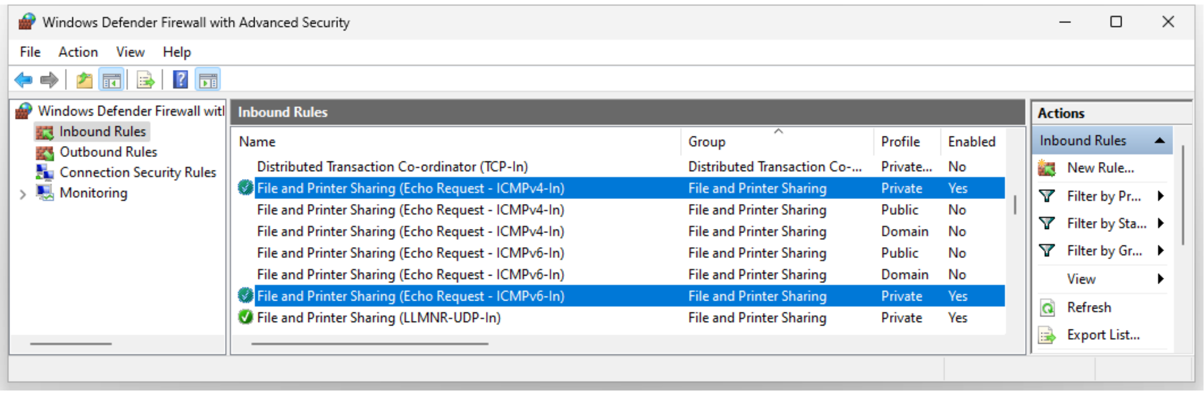
- Applications try to install software or make changes to my computer
- I make changes to Windows settings

Not recommended.

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.

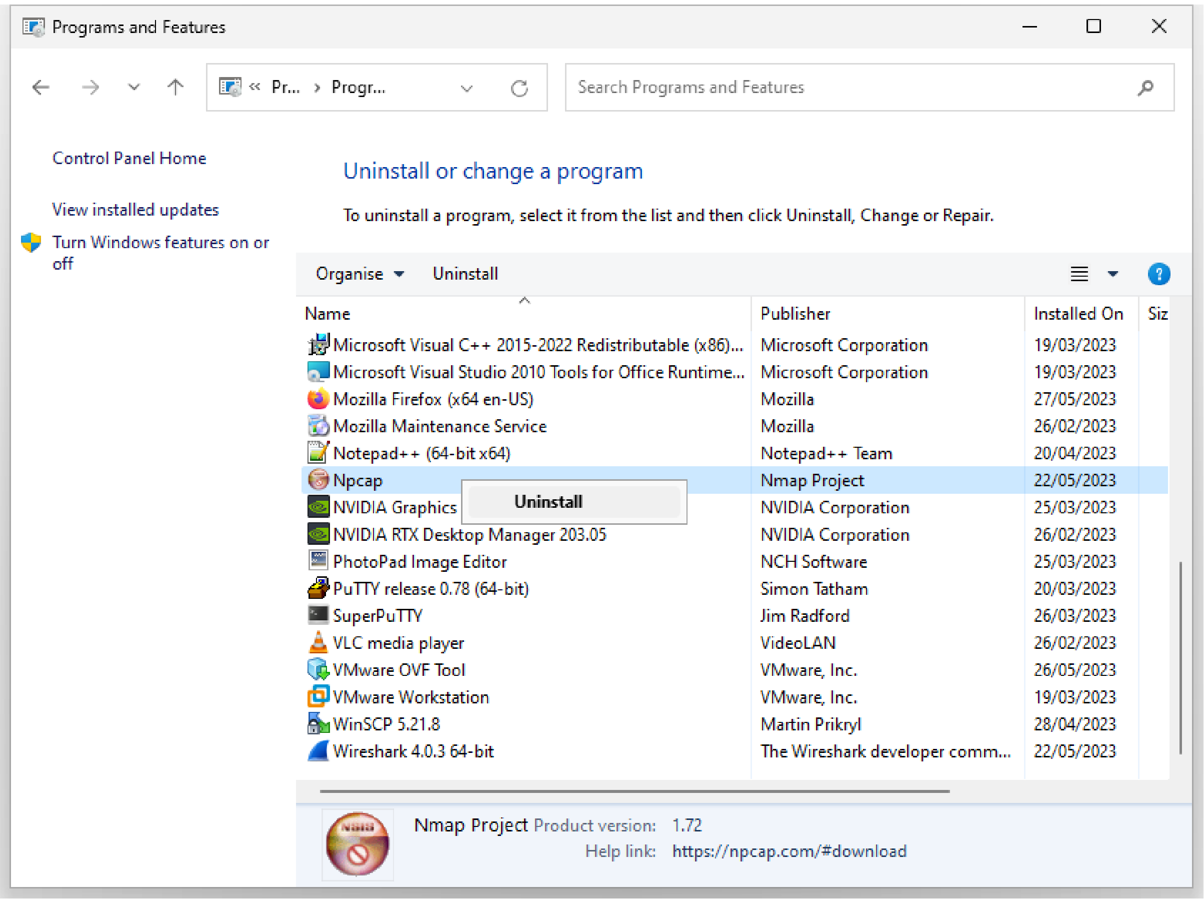
- File and Printer Sharing (Echo Request – CIMPv4-In) for Private Profile.
- File and Printer Sharing (Echo Request – CIMPv6-In) for Private Profile.



Inbound Rules

Name	Group	Profile	Enabled
Distributed Transaction Co-ordinator (TCP-In)	Distributed Transaction Co-...	Private...	No
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private	Yes
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Public	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Public	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No
✓ File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private	Yes
✓ File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Private	Yes

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.

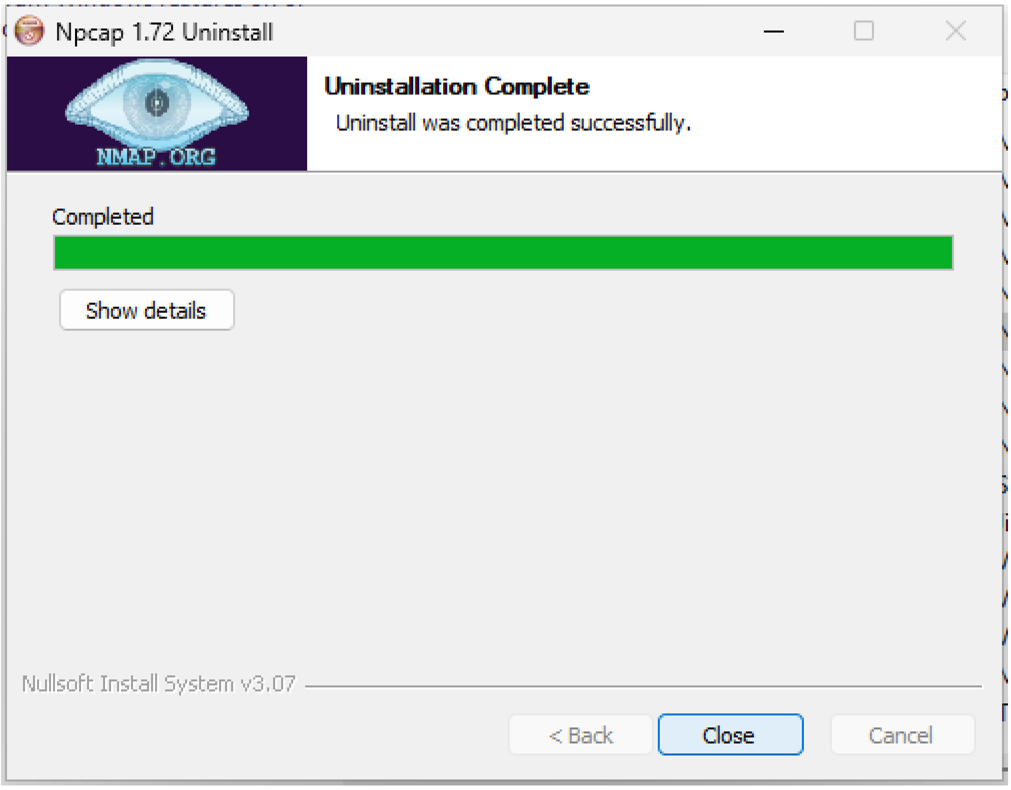


Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change or Repair.

Name	Publisher	Installed On	Siz
Microsoft Visual C++ 2015-2022 Redistributable (x86)...	Microsoft Corporation	19/03/2023	
Microsoft Visual Studio 2010 Tools for Office Runtime...	Microsoft Corporation	19/03/2023	
Mozilla Firefox (x64 en-US)	Mozilla	27/05/2023	
Mozilla Maintenance Service	Mozilla	26/02/2023	
Notepad++ (64-bit x64)	Notepad++ Team	20/04/2023	
Npcap	Nmap Project	22/05/2023	
NVIDIA Graphics	NVIDIA Corporation	25/03/2023	
NVIDIA RTX Desktop Manager 203.05	NVIDIA Corporation	26/02/2023	
PhotoPad Image Editor	NCH Software	25/03/2023	
PuTTY release 0.78 (64-bit)	Simon Tatham	20/03/2023	
SuperPuTTY	Jim Radford	26/03/2023	
VLC media player	VideoLAN	26/02/2023	
VMware OVF Tool	VMware, Inc.	26/05/2023	
VMware Workstation	VMware, Inc.	19/03/2023	
WinSCP 5.21.8	Martin Prikryl	28/04/2023	
Wireshark 4.0.3 64-bit	The Wireshark developer comm...	22/05/2023	

Nmap Project Product version: 1.72
Help link: https://npcap.com/#download



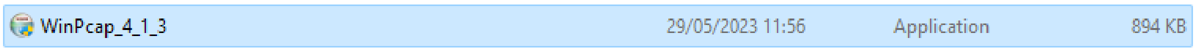
Npcap 1.72 Uninstall

Uninstallation Complete

Uninstall was completed successfully.

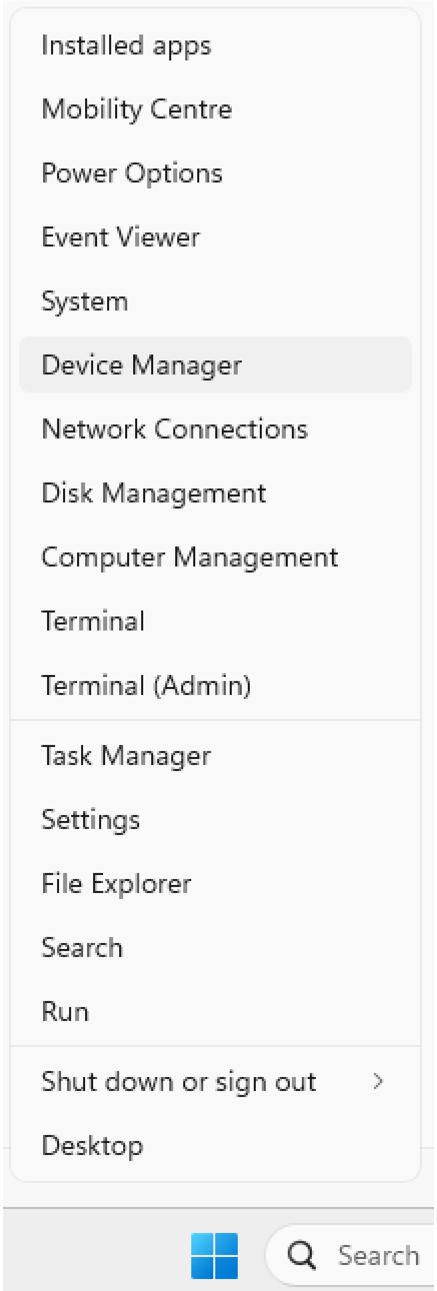
Completed

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.

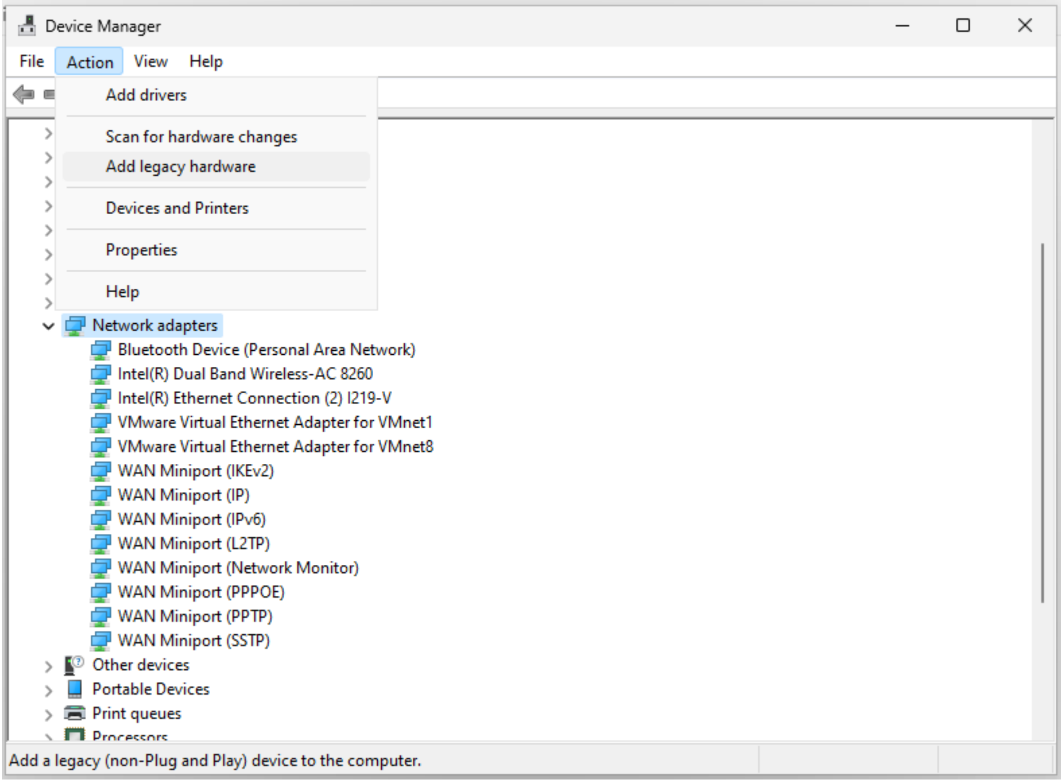


WinPcap_4_1_3 29/05/2023 11:56 Application 894 KB

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

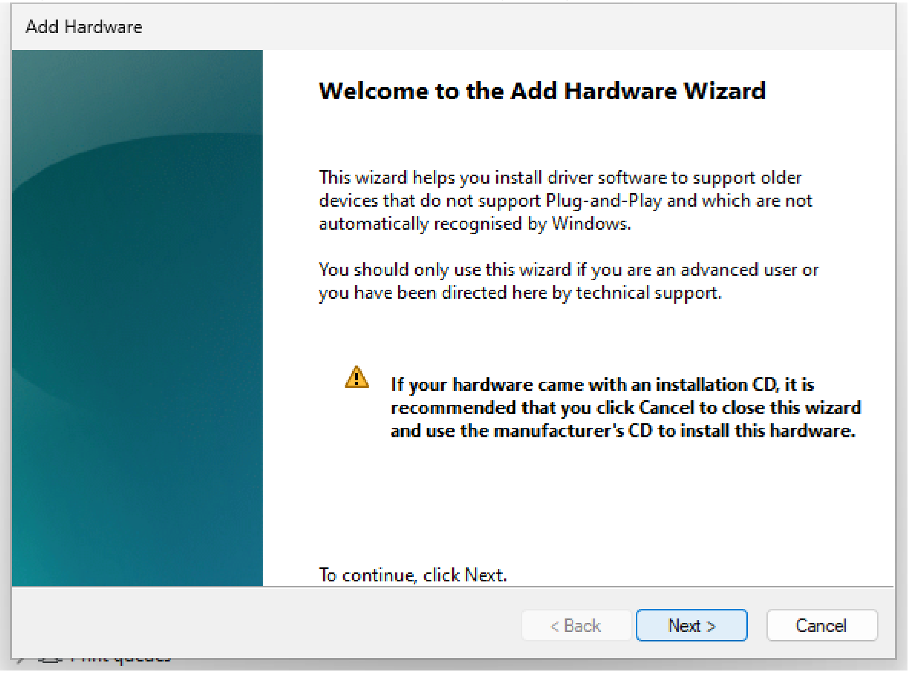


Step 6: Highlight the Network adapters, and then click on Action > Add legacy hardware.



Add a legacy (non-Plug and Play) device to the computer.

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



Welcome to the Add Hardware Wizard

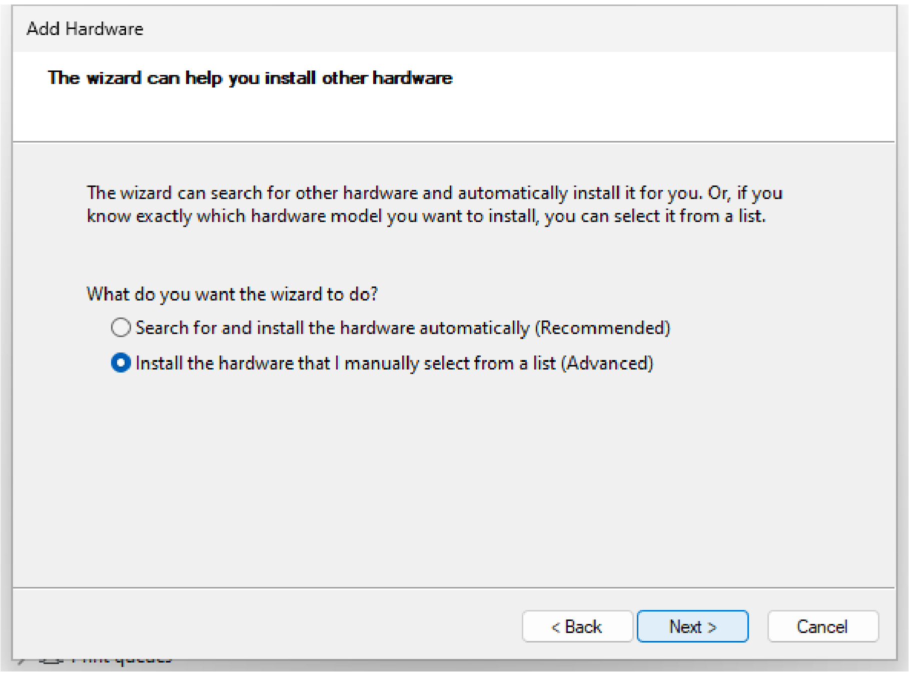
This wizard helps you install driver software to support older devices that do not support Plug-and-Play and which are not automatically recognised by Windows.

You should only use this wizard if you are an advanced user or you have been directed here by technical support.

If your hardware came with an installation CD, it is recommended that you click Cancel to close this wizard and use the manufacturer's CD to install this hardware.

To continue, click Next.

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



Add Hardware

The wizard can help you install other hardware

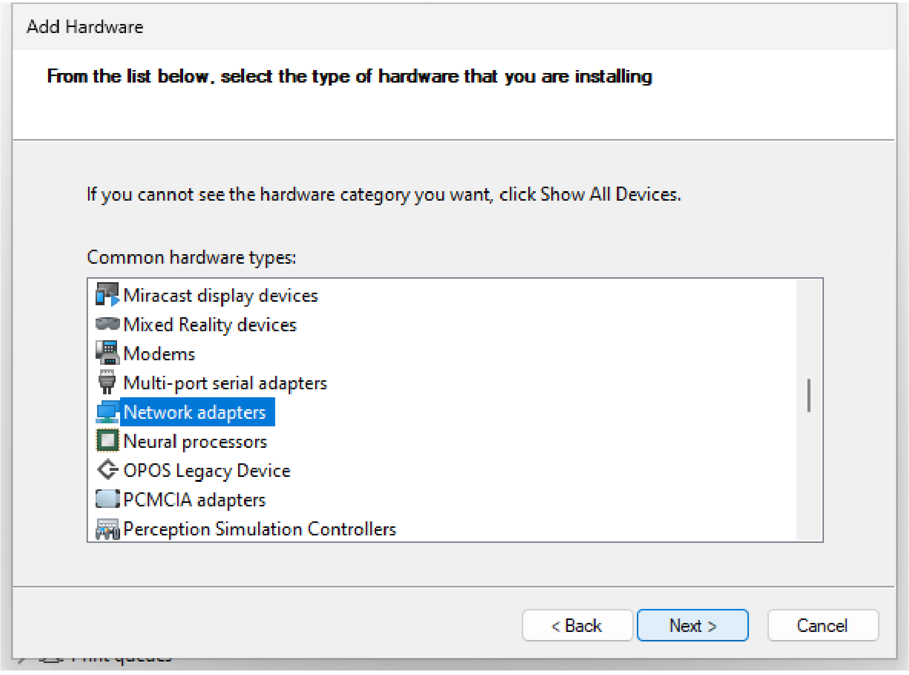
The wizard can search for other hardware and automatically install it for you. Or, if you know exactly which hardware model you want to install, you can select it from a list.

What do you want the wizard to do?

○ Search for and install the hardware automatically (Recommended)

● Install the hardware that I manually select from a list (Advanced)

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



Add Hardware

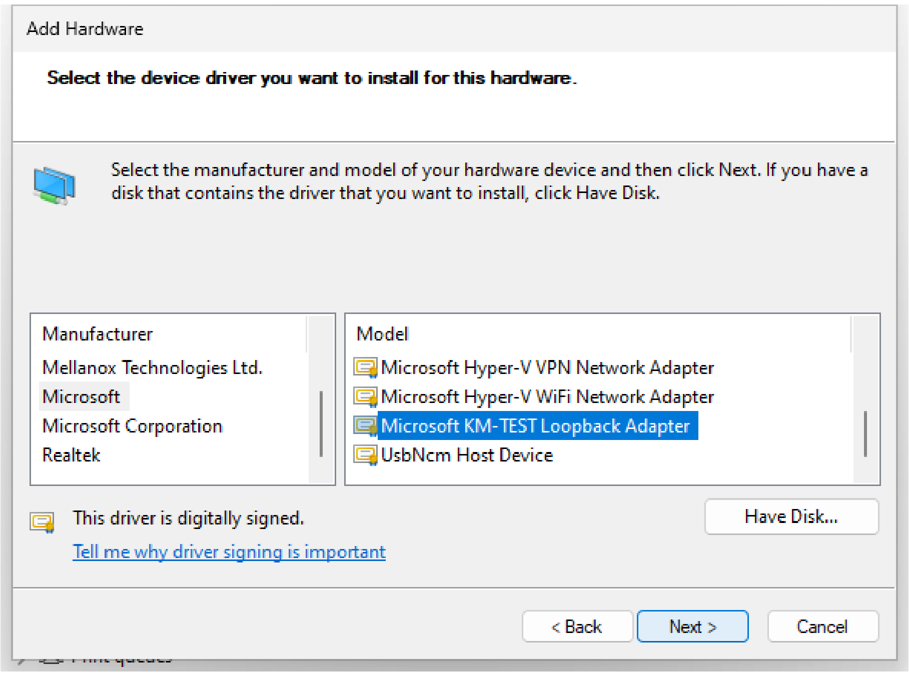
From the list below, select the type of hardware that you are installing

If you cannot see the hardware category you want, click Show All Devices.

Common hardware types:

- Miracast display devices
- Mixed Reality devices
- Modems
- Multi-port serial adapters
- Network adapters
- Neural processors
- OPOS Legacy Device
- PCMCIA adapters
- Perception Simulation Controllers

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.



Add Hardware

Select the device driver you want to install for this hardware.

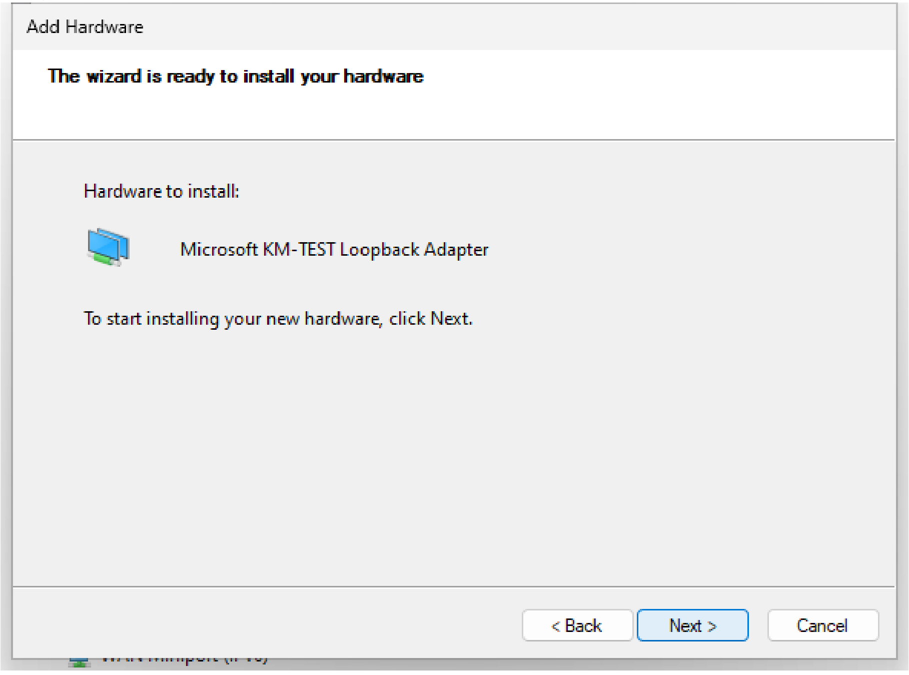
Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver that you want to install, click Have Disk.

Manufacturer	Model
Mellanox Technologies Ltd.	Microsoft Hyper-V VPN Network Adapter
Microsoft	Microsoft Hyper-V WiFi Network Adapter
Microsoft Corporation	Microsoft KM-TEST Loopback Adapter
Realtek	UsbNcm Host Device

This driver is digitally signed.

Tell me why driver signing is important

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



Add Hardware

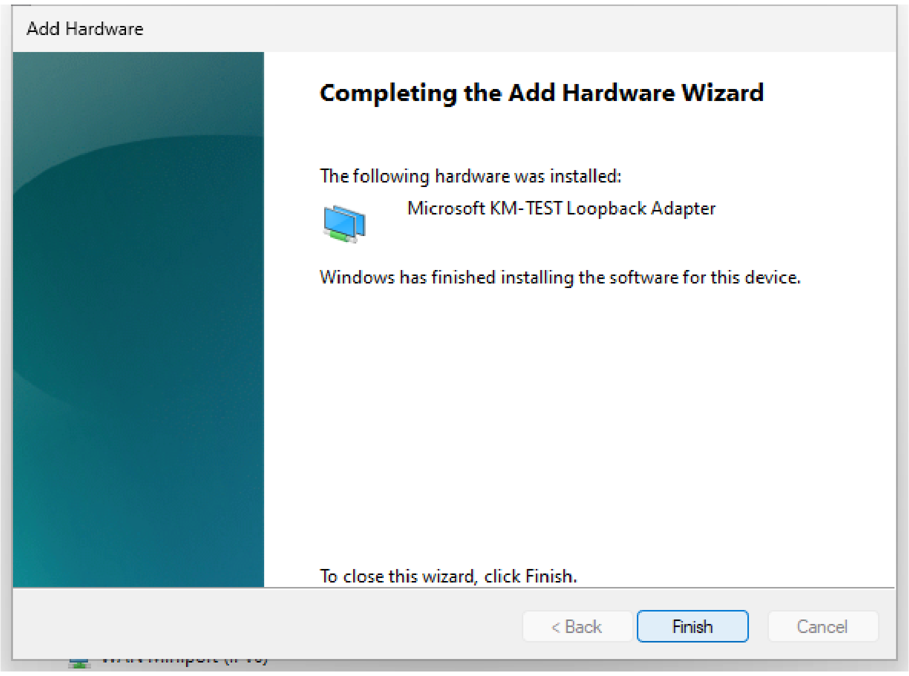
The wizard is ready to install your hardware

Hardware to install:

Microsoft KM-TEST Loopback Adapter

To start installing your new hardware, click Next.

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



Add Hardware

Completing the Add Hardware Wizard

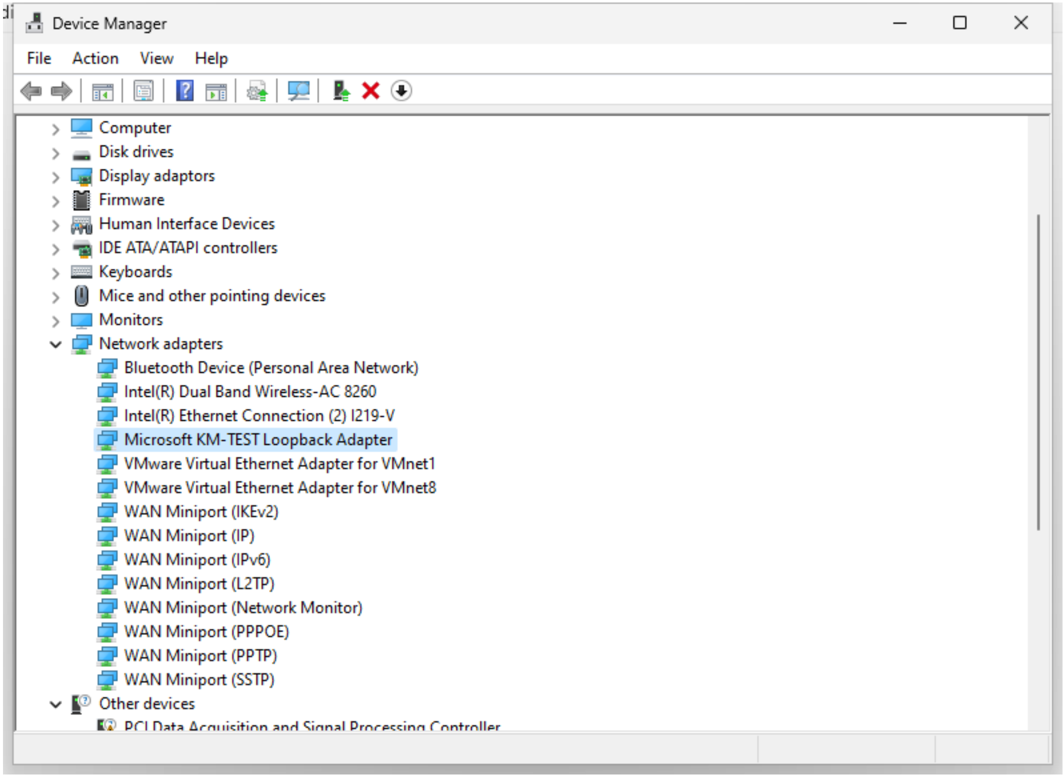
The following hardware was installed:

Microsoft KM-TEST Loopback Adapter

Windows has finished installing the software for this device.

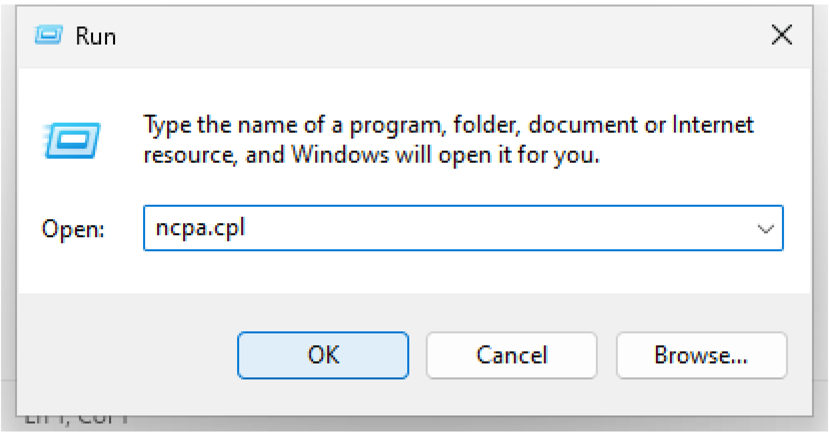
To close this wizard, click Finish.

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



- Computer
- Disk drives
- Display adaptors
- Firmware
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
  - Bluetooth Device (Personal Area Network)
  - Intel(R) Dual Band Wireless-AC 8260
  - Intel(R) Ethernet Connection (2) I219-V
  - Microsoft KM-TEST Loopback Adapter
  - VMware Virtual Ethernet Adapter for VMnet1
  - VMware Virtual Ethernet Adapter for VMnet8
  - WAN Miniport (IKEv2)
  - WAN Miniport (IP)
  - WAN Miniport (IPv6)
  - WAN Miniport (L2TP)
  - WAN Miniport (Network Monitor)
  - WAN Miniport (PPPOE)
  - WAN Miniport (PPTP)
  - WAN Miniport (SSTP)
- Other devices
  - PCI Data Acquisition and Signal Processing Controller

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.

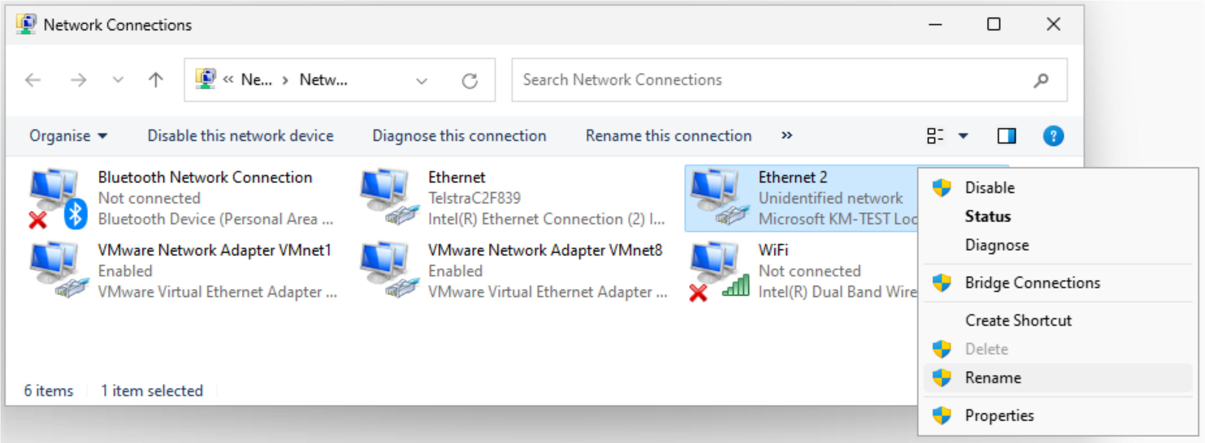


Run

Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: ncpa.cpl

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.



Network Connections

Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

Ethernet
TelstraC2F839
Intel(R) Ethernet Connection (2) I...

Ethernet 2
Unidentified network
Microsoft KM-TEST Loo

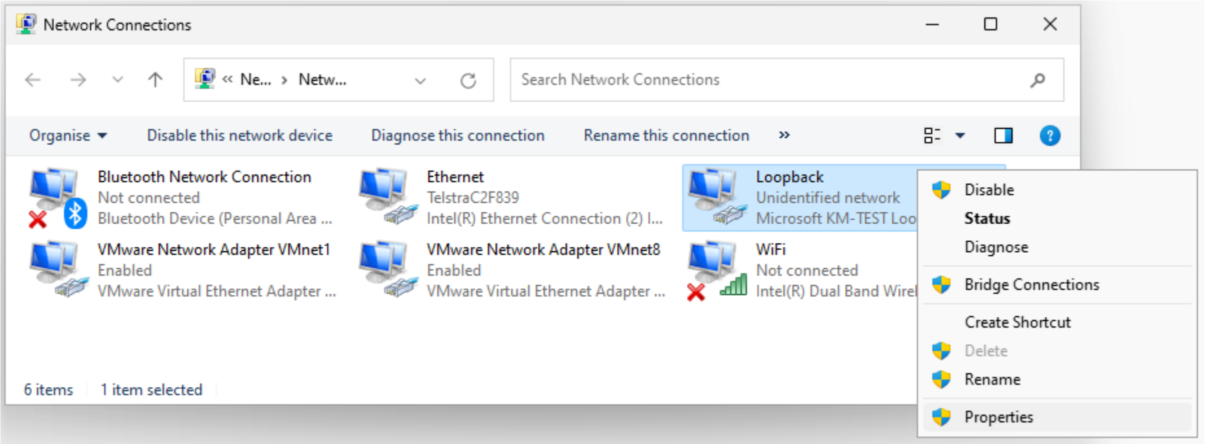
VMware Network Adapter VMnet1
Enabled
VMware Virtual Ethernet Adapter ...

VMware Network Adapter VMnet8
Enabled
VMware Virtual Ethernet Adapter ...

WiFi
Not connected
Intel(R) Dual Band Wire

6 items 1 item selected

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



Network Connections

Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

Ethernet
TelstraC2F839
Intel(R) Ethernet Connection (2) I...

Loopback
Unidentified network
Microsoft KM-TEST Loo

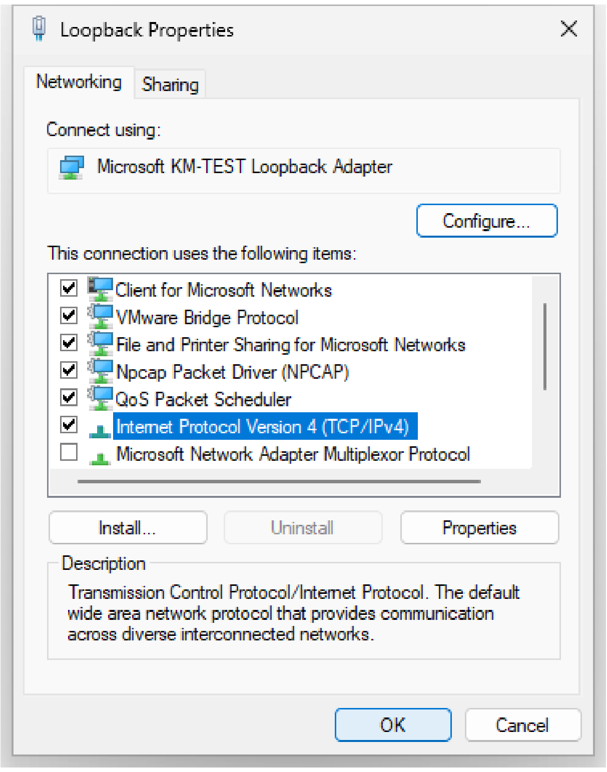
VMware Network Adapter VMnet1
Enabled
VMware Virtual Ethernet Adapter ...

VMware Network Adapter VMnet8
Enabled
VMware Virtual Ethernet Adapter ...

WiFi
Not connected
Intel(R) Dual Band Wire

6 items 1 item selected

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."



Loopback Properties

Networking | Sharing

Connect using:

Microsoft KM-TEST Loopback Adapter

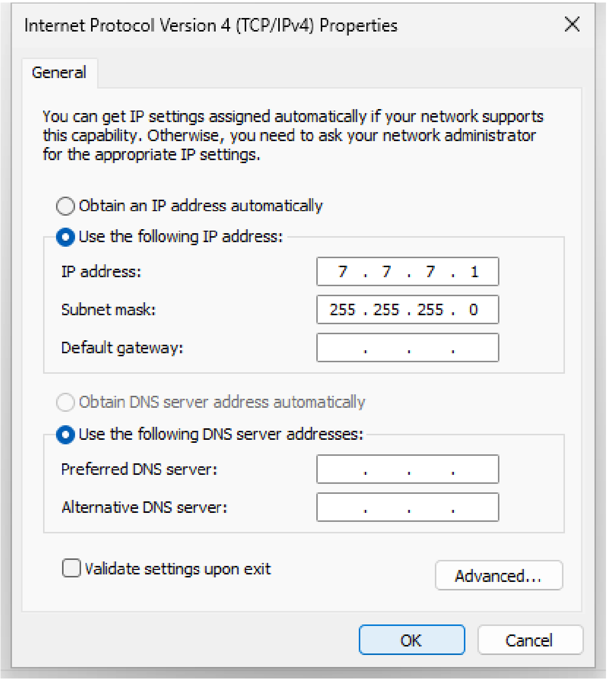
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports 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: 7 . 7 . 7 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

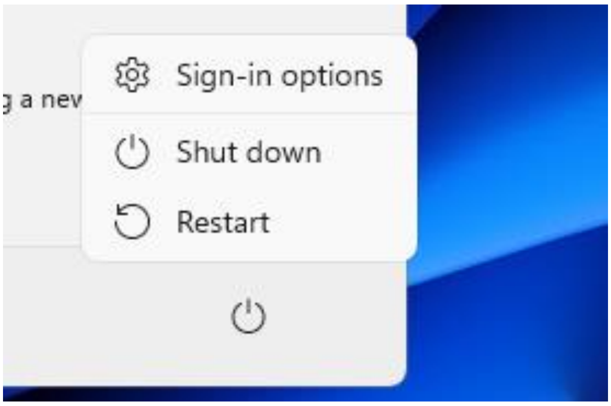
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

□ Validate settings upon exit

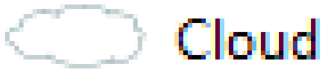
Step19 : Restart your PC to apply the new settings.

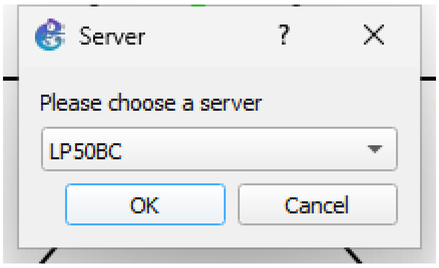

g a nev
Sign-in options
Shut down
Restart

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.

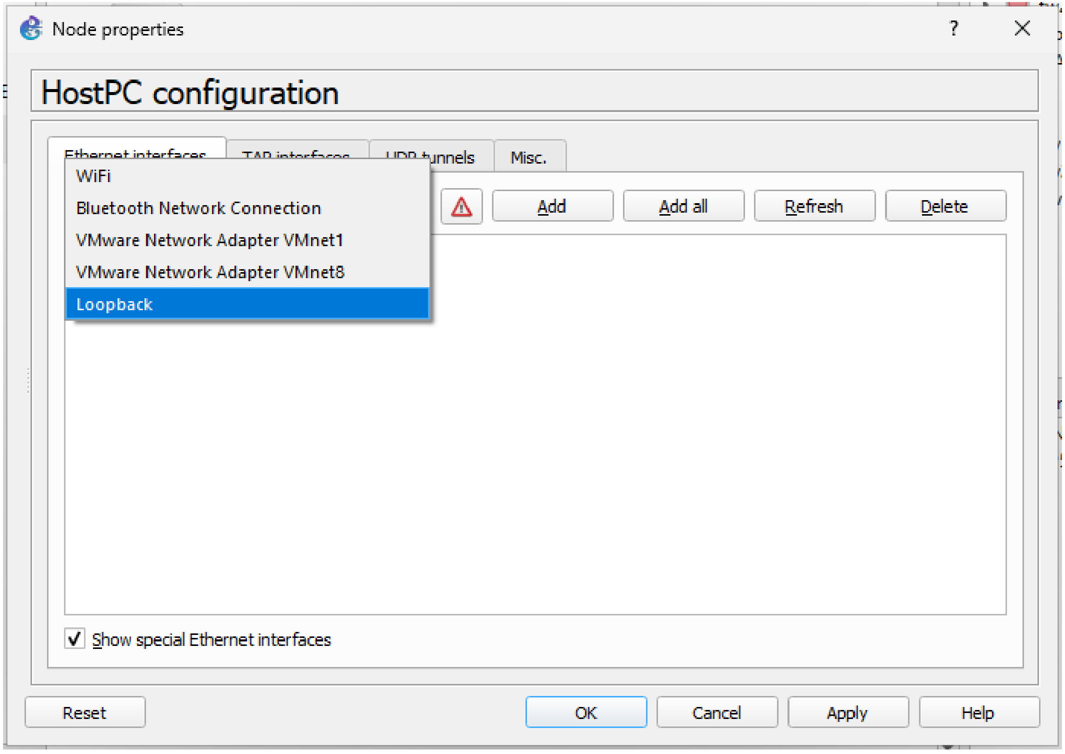



Server

Please choose a server

LP50BC

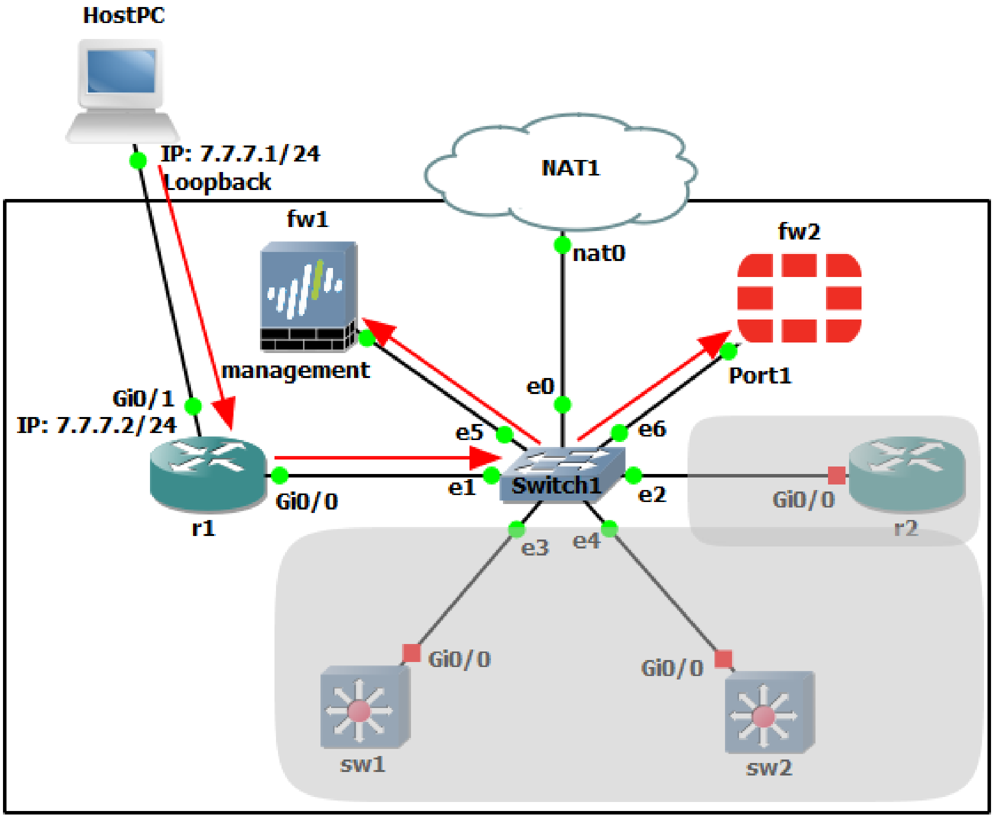
Step 2: After placing the Cloud on the GNS3 Topology canvas, position your mouse cursor over the icon and right-click to open the "Configure" (Node properties) menu. Make sure to checkmark "Show special Ethernet interfaces," then use the dropdown menu to select "Loopback" and add the interface. Optionally,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


Node properties

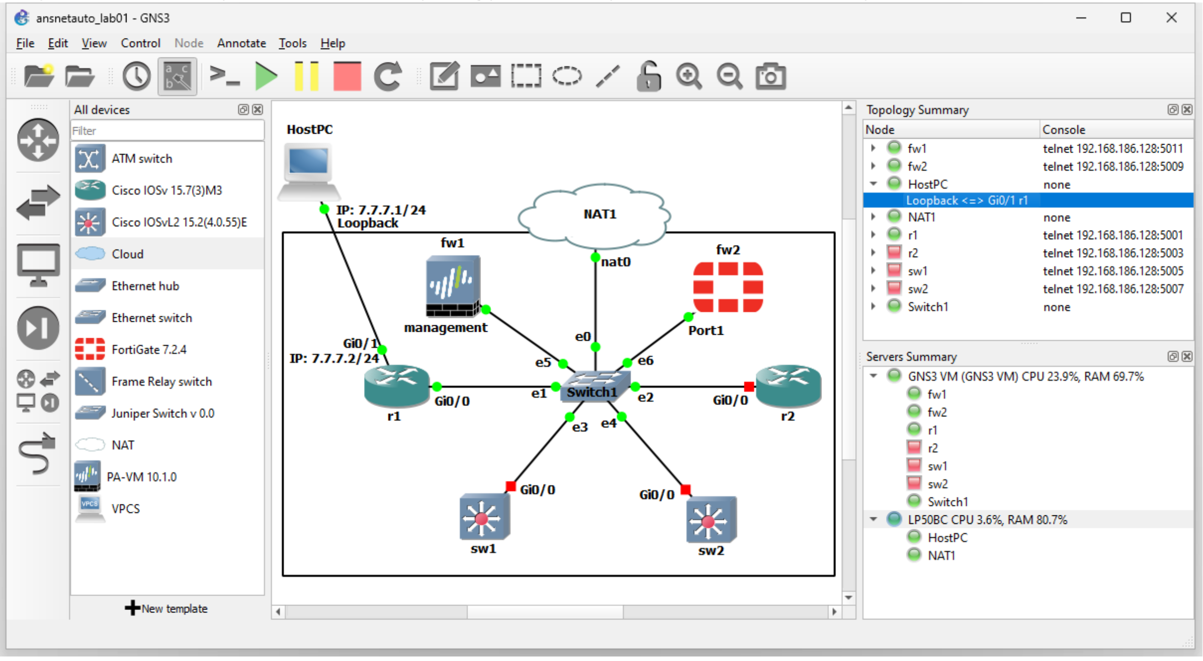
HostPC configuration

☑ Show special Ethernet interfaces

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.



Topology Summary

Node	Console
fw1	telnet 192.168.186.128:5011
fw2	telnet 192.168.186.128:5009
HostPC	none
Loopback <=> Gi0/1 r1	
NAT1	none
r1	telnet 192.168.186.128:5001
r2	telnet 192.168.186.128:5003
sw1	telnet 192.168.186.128:5005
sw2	telnet 192.168.186.128:5007
Switch1	none

Servers Summary

- GNS3 VM (GNS3 VM) CPU 23.9%, RAM 69.7%
  - fw1
  - fw2
  - r1
  - r2
  - sw1
  - sw2
  - Switch1
- LP50BC CPU 3.6%, RAM 80.7%
  - HostPC
  - NAT1

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 5uper5cret9assw0rd
!
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 tracert tests to the two firewalls: PA-VM (fw1) at 192.168.127.31 and FortiGate (fw2) at 192.168.127.31.

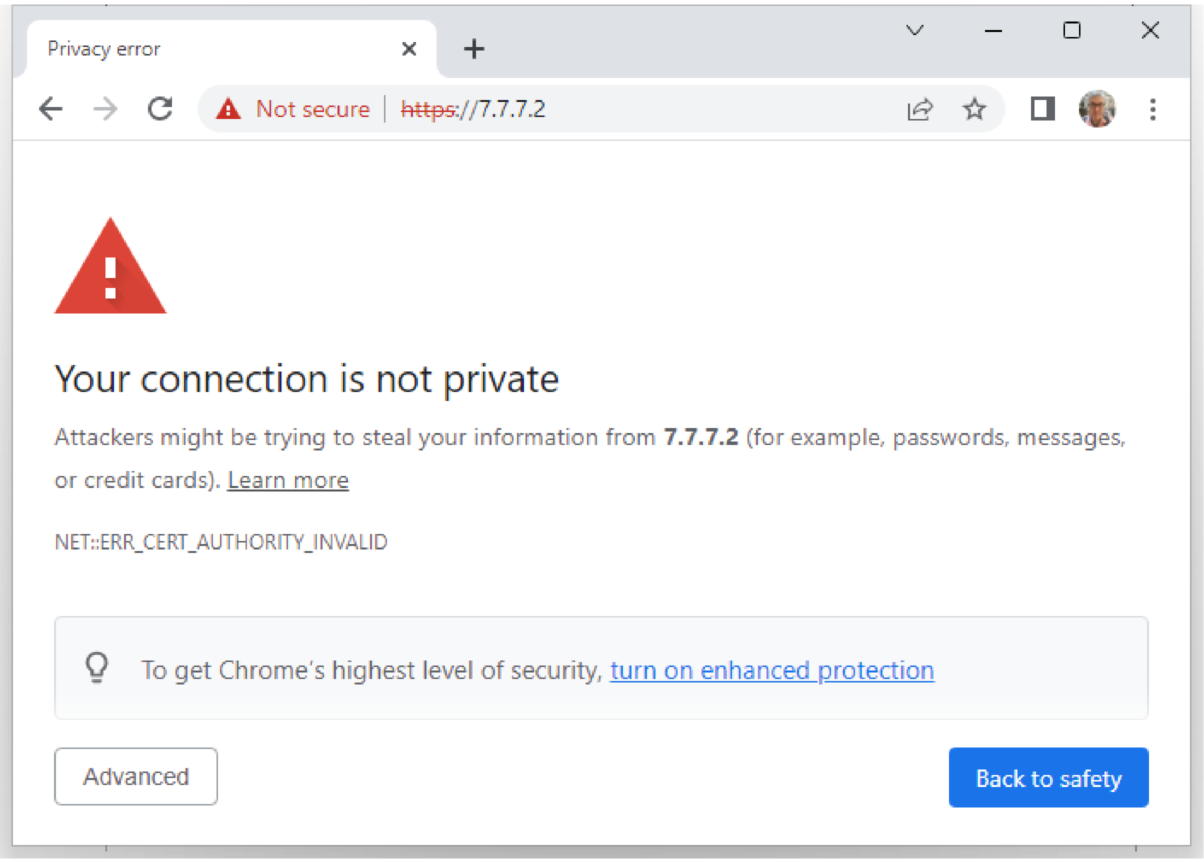
```
C:\Users\brend>ping 192.168.127.31

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

  1     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.



Your connection is not private

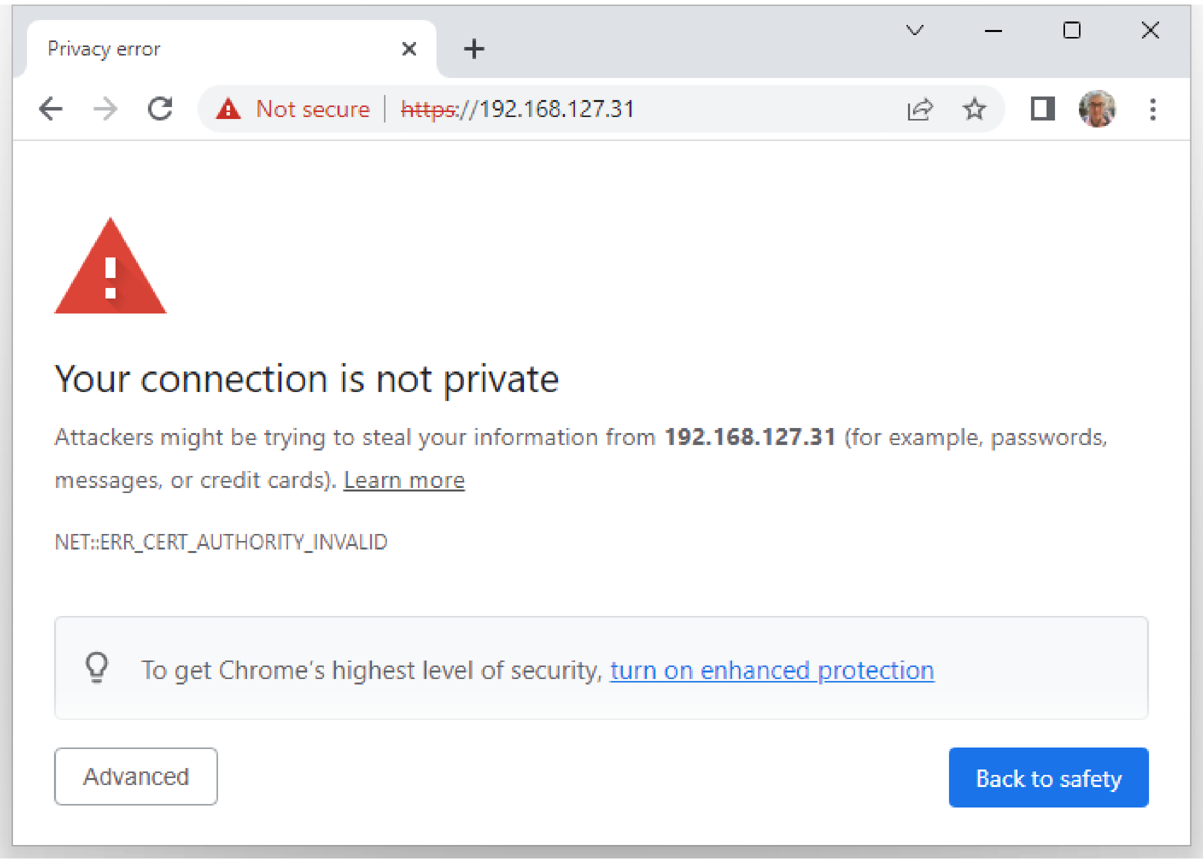
Attackers might be trying to steal your information from **7.7.7.2** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

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/



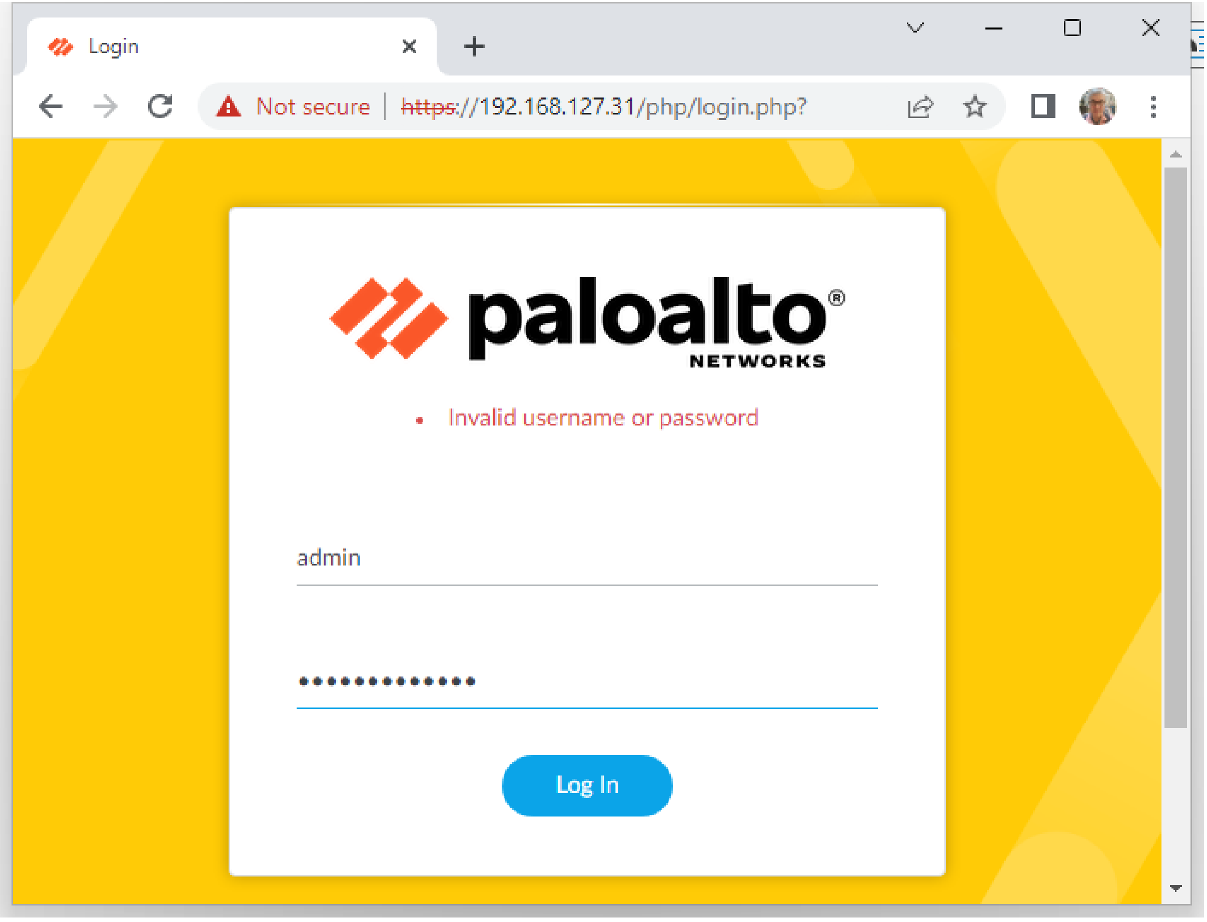
Your connection is not private

Attackers might be trying to steal your information from **192.168.127.31** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

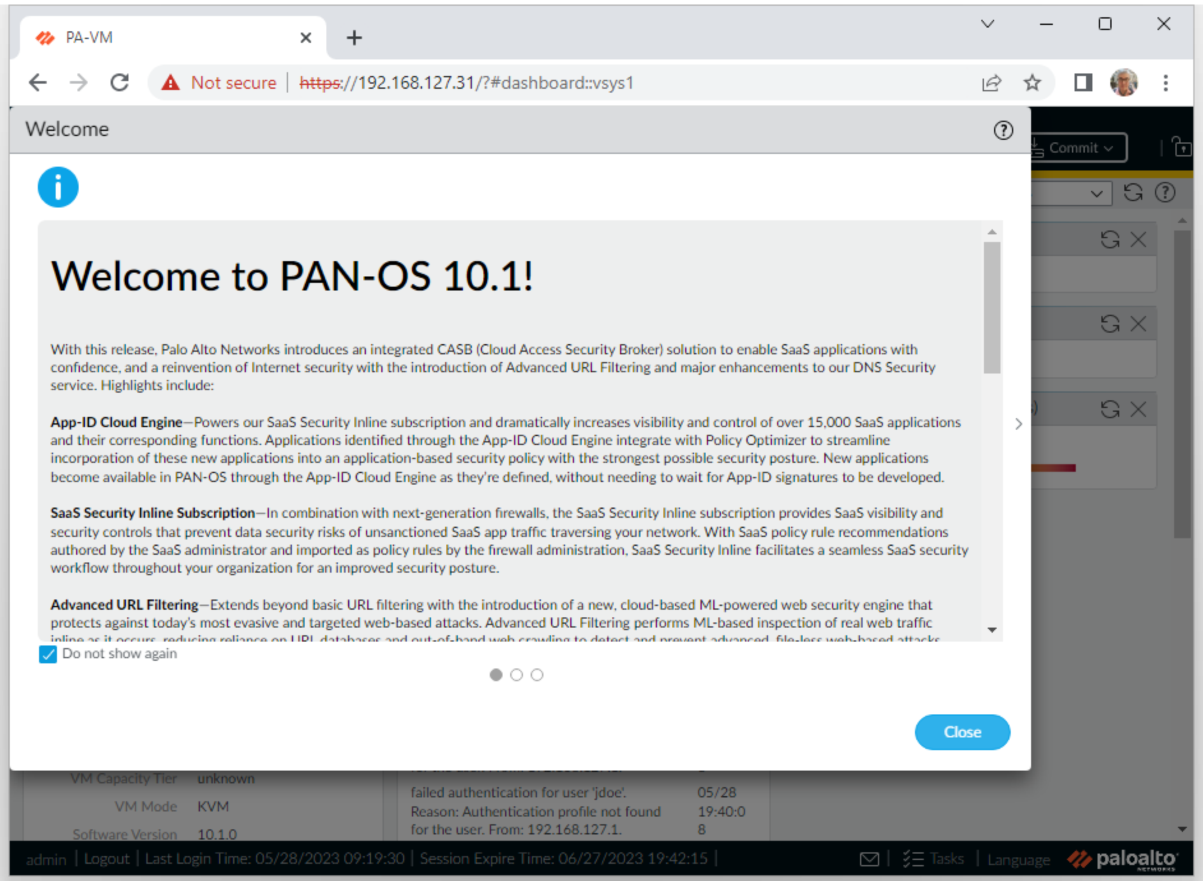
Enter the username and password and log into your Palo Alto's PANOS.



- Invalid username or password

admin

•••••••••••••



Welcome

Welcome to PAN-OS 10.1!

With this release, Palo Alto Networks introduces an integrated CASB (Cloud Access Security Broker) solution to enable SaaS applications with confidence, and a reinvention of Internet security with the introduction of Advanced URL Filtering and major enhancements to our DNS Security service. Highlights include:

App-ID Cloud Engine—Powers our SaaS Security Inline subscription and dramatically increases visibility and control of over 15,000 SaaS applications and their corresponding functions. Applications identified through the App-ID Cloud Engine integrate with Policy Optimizer to streamline incorporation of these new applications into an application-based security policy with the strongest possible security posture. New applications become available in PAN-OS through the App-ID Cloud Engine as they're defined, without needing to wait for App-ID signatures to be developed.

SaaS Security Inline Subscription—In combination with next-generation firewalls, the SaaS Security Inline subscription provides SaaS visibility and security controls that prevent data security risks of unsanctioned SaaS app traffic traversing your network. With SaaS policy rule recommendations authored by the SaaS administrator and imported as policy rules by the firewall administration, SaaS Security Inline facilitates a seamless SaaS security workflow throughout your organization for an improved security posture.

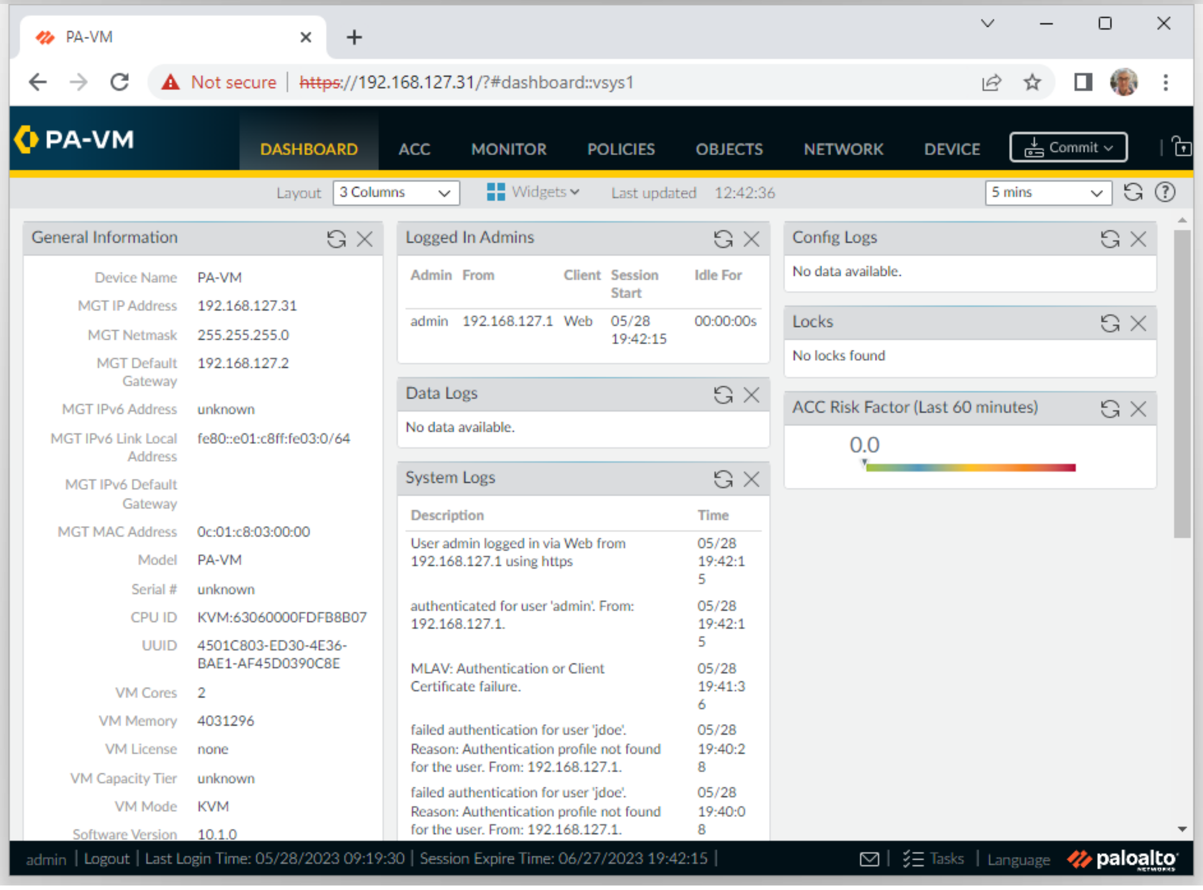
Advanced URL Filtering—Extends beyond basic URL filtering with the introduction of a new, cloud-based ML-powered web security engine that protects against today's most evasive and targeted web-based attacks. Advanced URL Filtering performs ML-based inspection of real web traffic inline as it occurs, reducing reliance on URL databases and out-of-band web crawling to detect and prevent advanced, file-less web-based attacks

☑ Do not show again

● ○ ○

Close

admin | Logout | Last Login Time: 05/28/2023 09:19:30 | Session Expire Time: 06/27/2023 19:42:15 |



Layout 3 Columns | Last updated 12:42:36 | 5 mins

General Information

Device Name	PA-VM
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
Software Version	10.1.0

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	192.168.127.1	Web	05/28 19:42:15	00:00:00s

Data Logs

No data available.

System Logs

Description	Time
User admin logged in via Web from 192.168.127.1 using https	05/28 19:42:15
authenticated for user 'admin'. From: 192.168.127.1.	05/28 19:42:15
MLAV: Authentication or Client Certificate failure.	05/28 19:41:36
failed authentication for user 'jdoe'. Reason: Authentication profile not found for the user. From: 192.168.127.1.	05/28 19:40:28
failed authentication for user 'jdoe'. Reason: Authentication profile not found for the user. From: 192.168.127.1.	05/28 19:40:08

Config Logs

No data available.

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

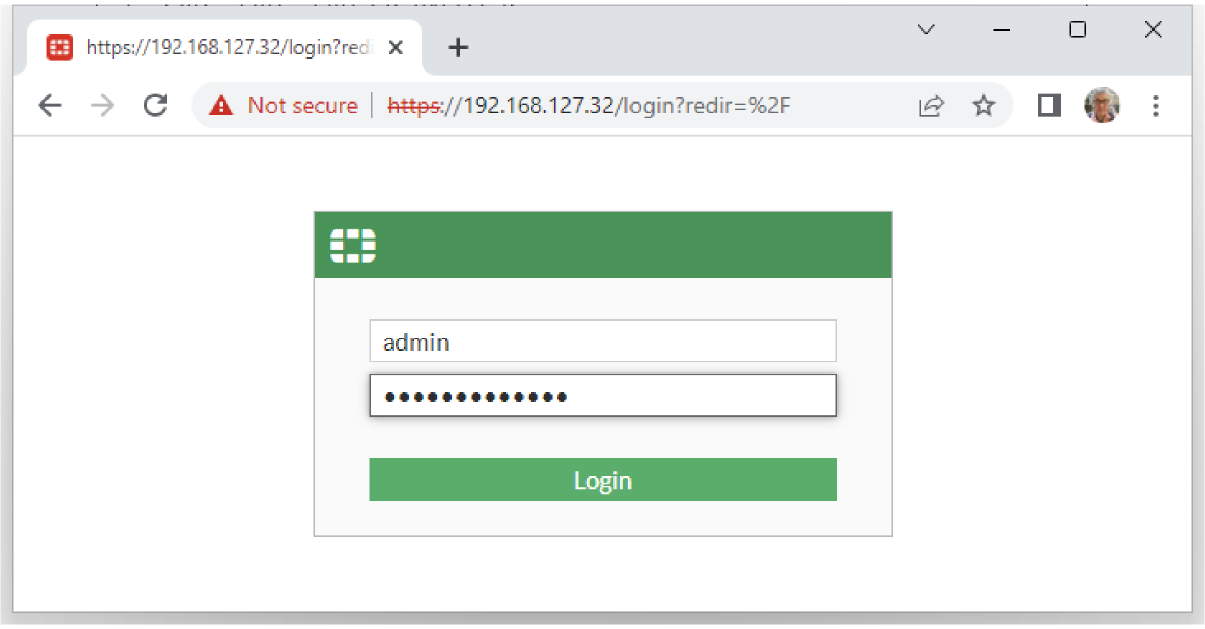
0.0

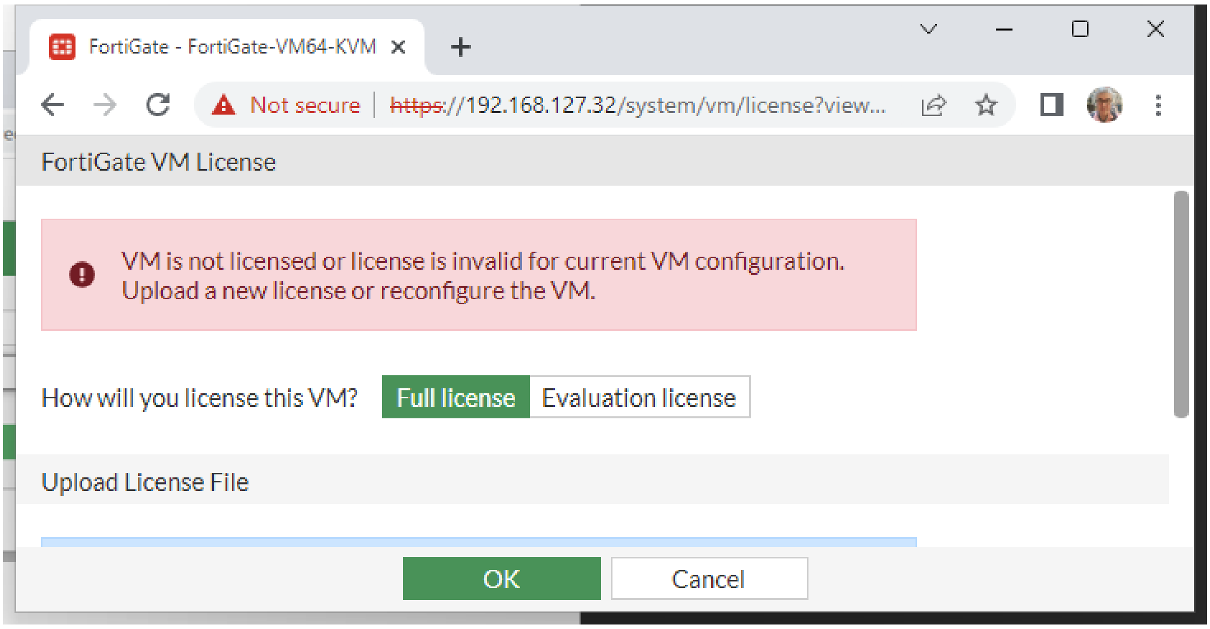
admin | Logout | Last Login Time: 05/28/2023 09:19:30 | Session Expire Time: 06/27/2023 19:42:15 |

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.


https://192.168.127.32/login?redi
Not secure
https://192.168.127.32/login?redir=%2F
admin
•••••••••••••
Login


FortiGate - FortiGate-VM64-KVM
Not secure
https://192.168.127.32/system/vm/license?view...
FortiGate VM License

VM is not licensed or license is invalid for current VM configuration.
Upload a new license or reconfigure the VM.

How will you license this VM? Full license Evaluation license

Upload License File
OK
Cancel

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!