Final Exam (Case Study)	
Name: Torrecampo, Juan Piolo S.	**Date Performed:** May 11, 2023
Course/Section: CPE 234 - CPE32S3	**Date Submitted:** May 16, 2023
Instructor: Engr. Taylar	**Semester and SY.** 2022-2023

Objectives

- Look for a medium-scale IT company that will allow you to provide a security plan for their infrastructure
- Describe their organizational structure, as well as their IT infrastructure
- Provide necessary hardware and software security based on their business policy
- Document everything. Your solution will only be a proposal and doesn't need to be implemented.

What is required?

- Document the security solution
- Simulation of the proposed solution using Virtual Machine/s. Include the playbook and successful run of the plays in your documentation.
- Justification of every solution you have proposed
- Conclusion and learning

Problem / Solution

Problem

The objective of this case study is to address the problem of online frauds targeting small enterprises. The aim of this research is to focus on sari-sari store owners who may encounter scams and frauds through online transactions. Since this is a small enterprise, we can also consider that this business does not have any network infrastructure currently running. Moreover, these bogus operations may attempt to penetrate via incoming traffic, such as fake links, spam emails, banking and online account scams, phishing, refund fraud and many more.

Solution

Since the small enterprise does not presently operate any kind of network, the solution that has been devised is to construct a *network* that has a *security*, which will protect the company from any threats that could cause identity theft and financial loss. The security of this network may include access lists in the router, turning off unused ports for both router and switches, installing Snort intrusion prevention

system in client computers, building CA with SSL, saving log files, and securing holes in the client computer.

Output

[1] SETTING UP GNS3

Setting up Wizard

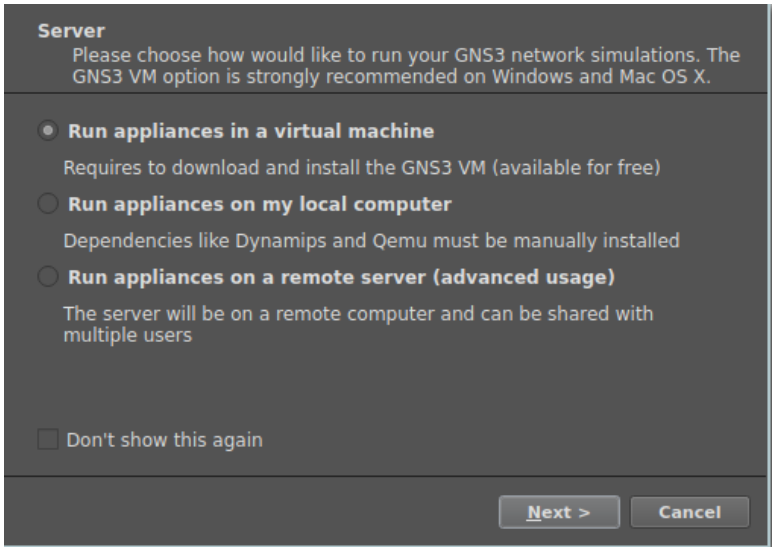


Figure 1.0. Selecting "Run appliance in a virtual machine" to make sure that the topology will run inside of the GNS3 VM.

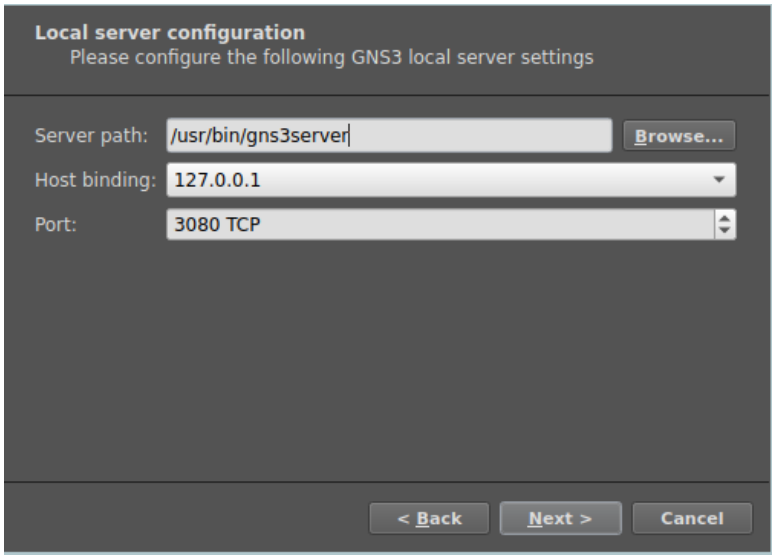


Figure 1.1. Choosing default setting in "Local server configuration".

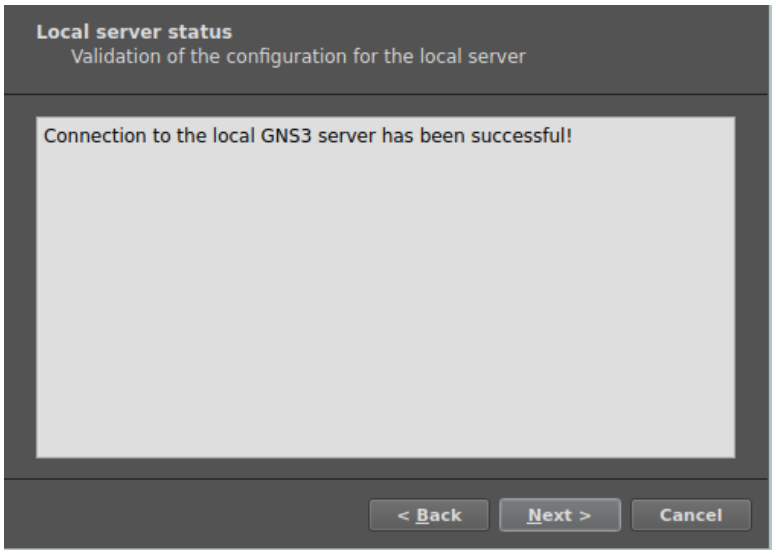


Figure 1.3. The screenshot above shows that the setting up of the local GNS3 server was successful.

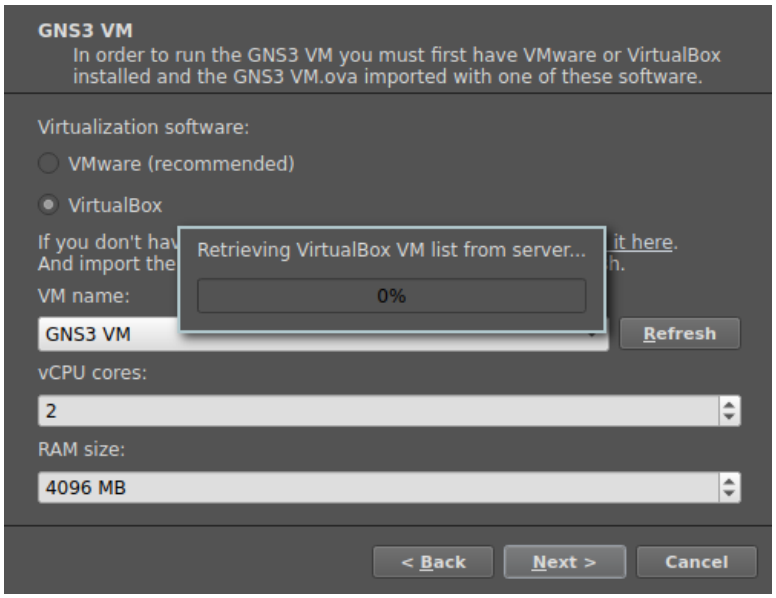


Figure 1.4. Selecting virtualbox as virtualization software and choosing GNS3 VM as the "VM name".

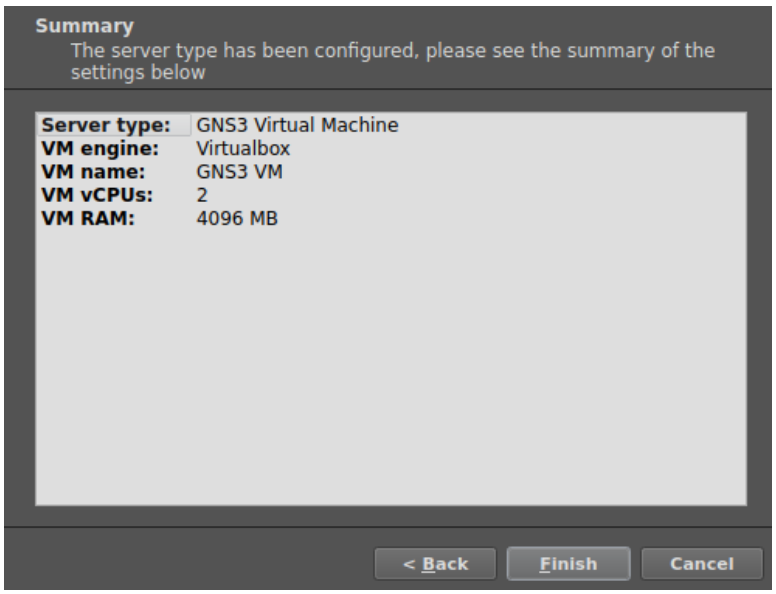


Figure 1.5. The screenshot above shows the summary of the configuration.

[2] CREATING A PROJECT

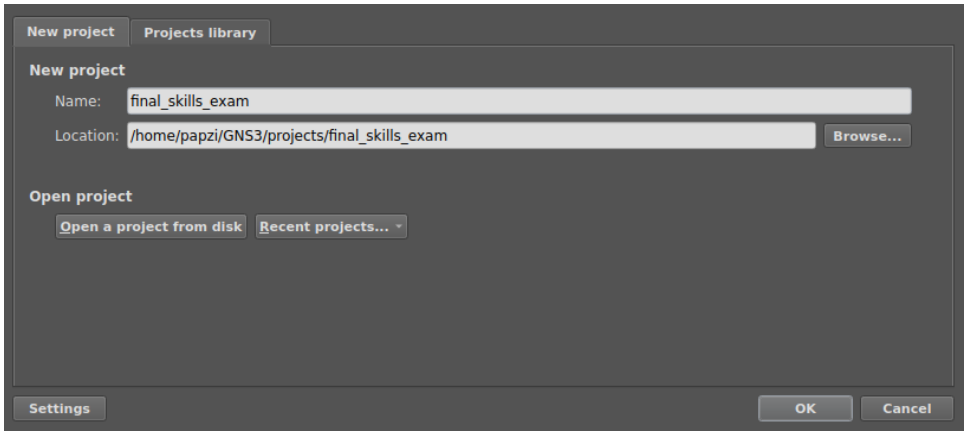


Figure 2.0. Creating a project in GNS3.

[3] SETTING UP DEVICES

ADDING CLOUD NODE

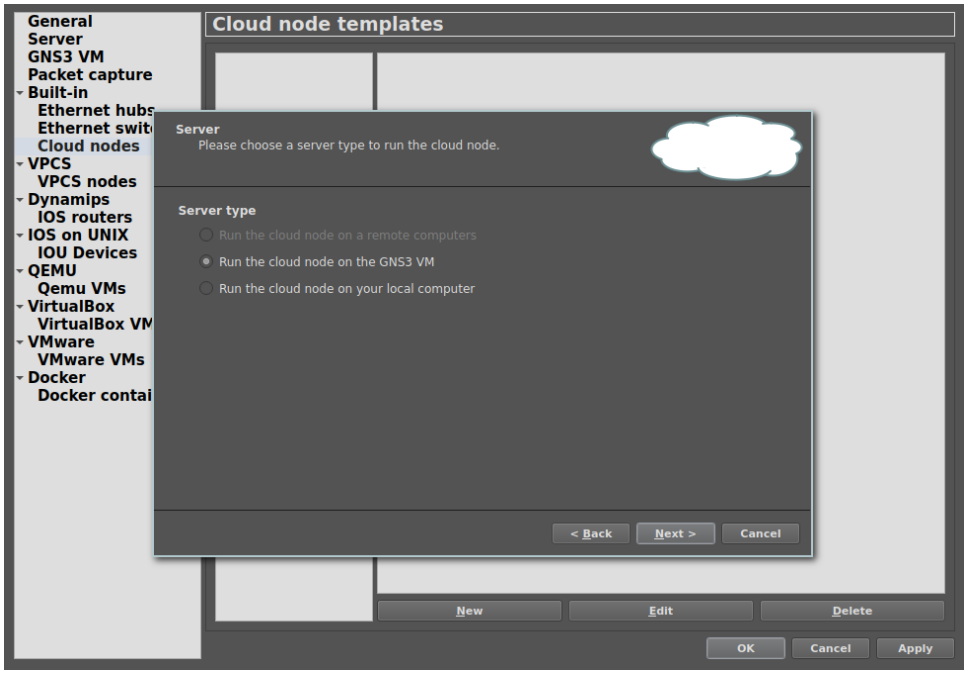


Figure 3.0. Adding cloud node under "Cloud Nodes" in "Preference" section. Selecting "Run the cloud node on the GNS3 VM".

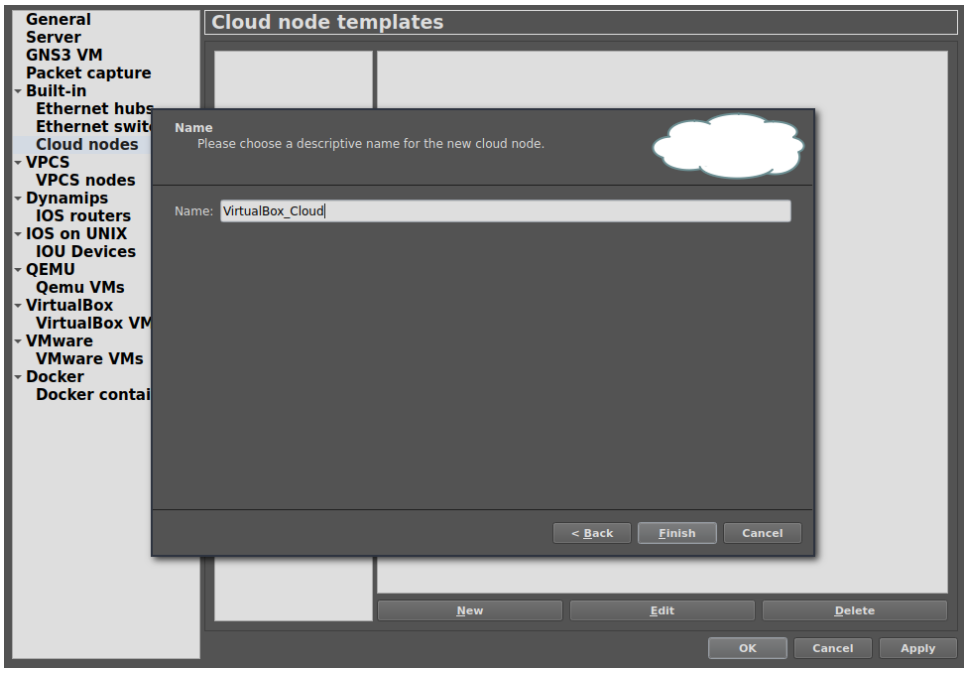


Figure 3.1. Adding a name in the cloud node.

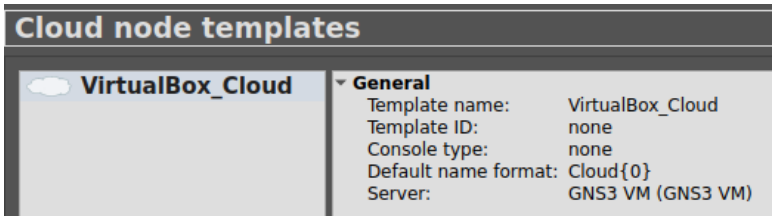


Figure 3.2. The screenshot above shows the summary of the recently created node.

ADDING CISCO ROUTER

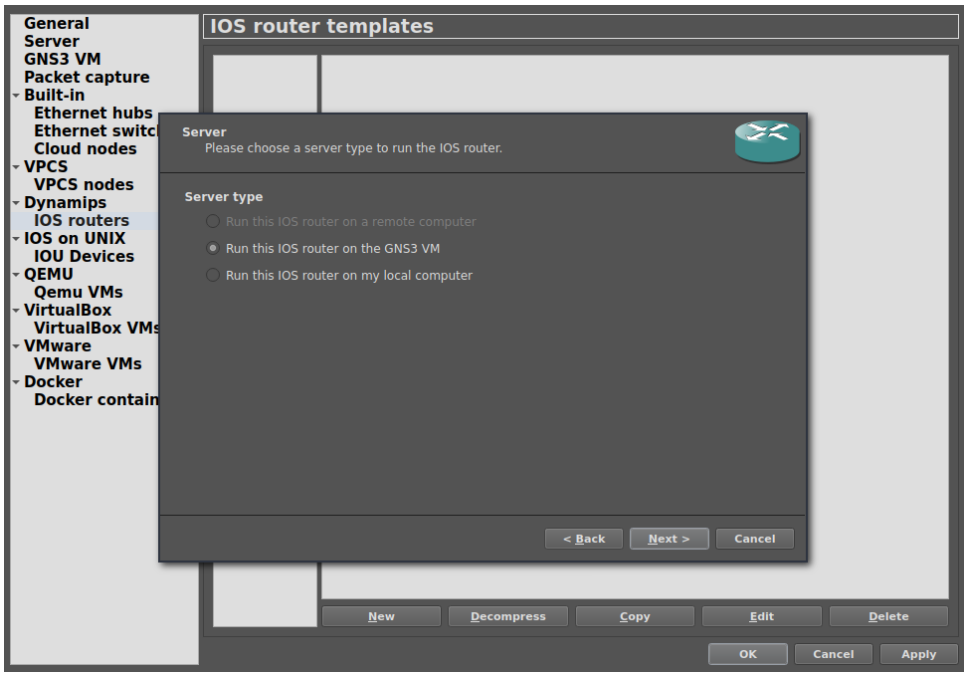


Figure 3.3. Selecting "Run this IOS router on the router on the GNS3 VM".

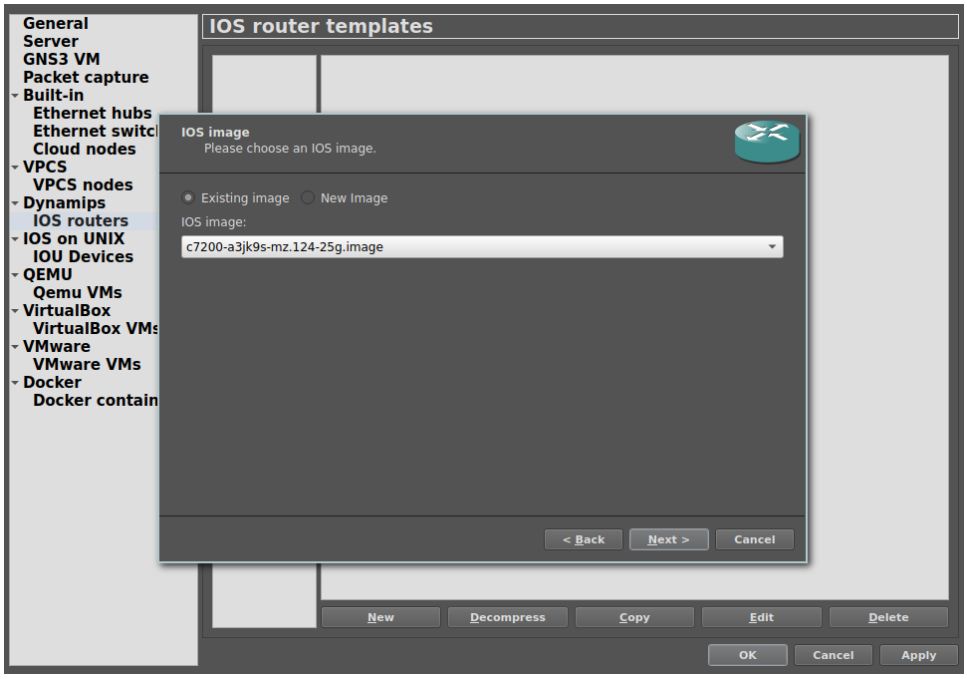


Figure 3.4. Choosing the cisco router 7200 image with the .bin extension.

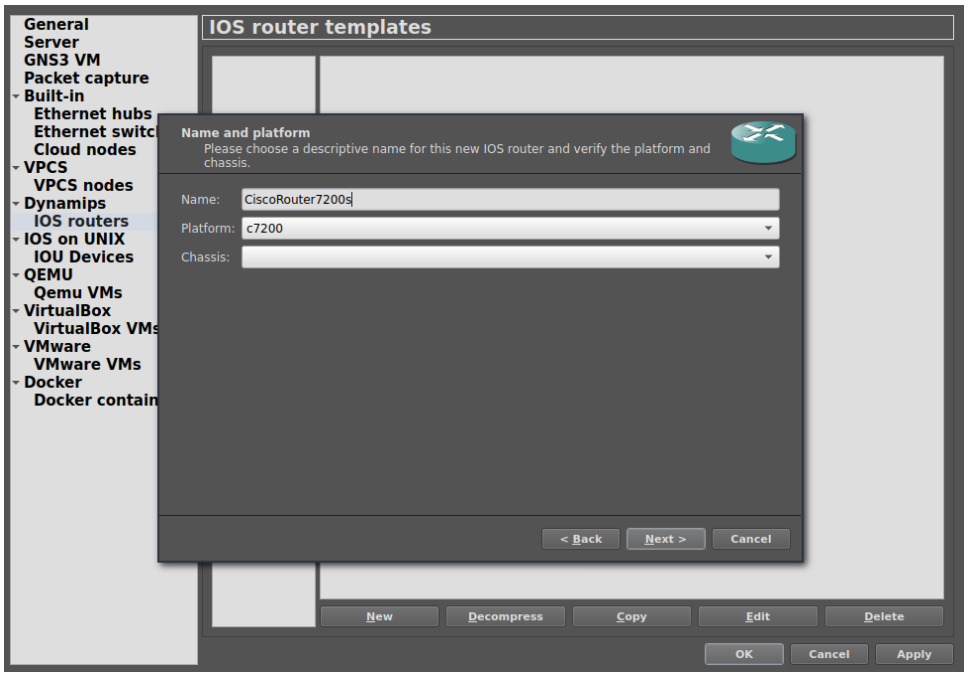


Figure 3.5. Naming and setting up the platform for Cisco router.

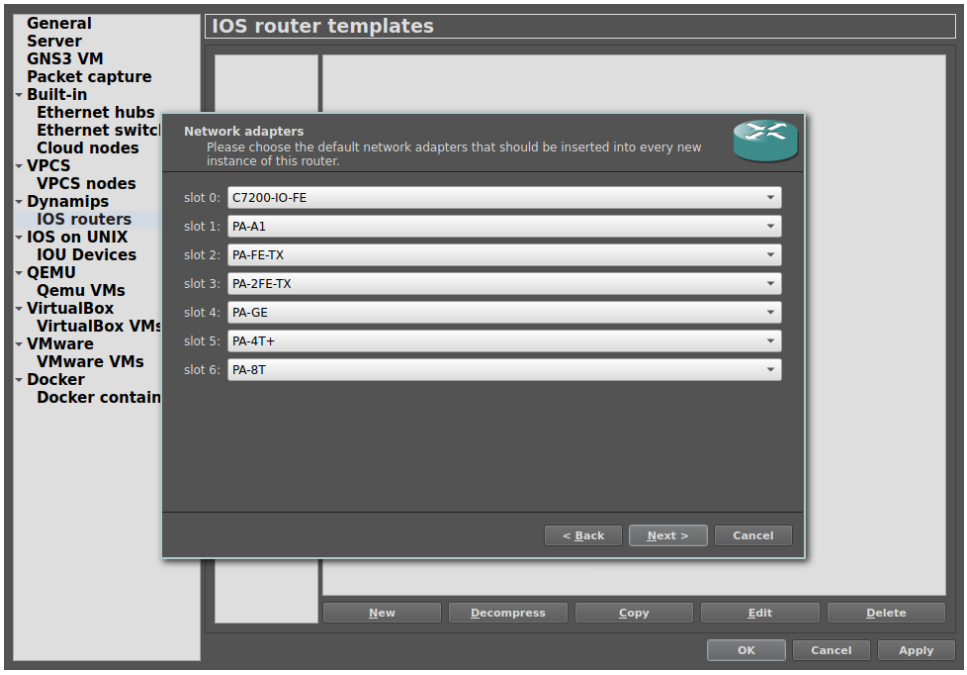


Figure 3.6. Selecting different NIC adapters for each slots.

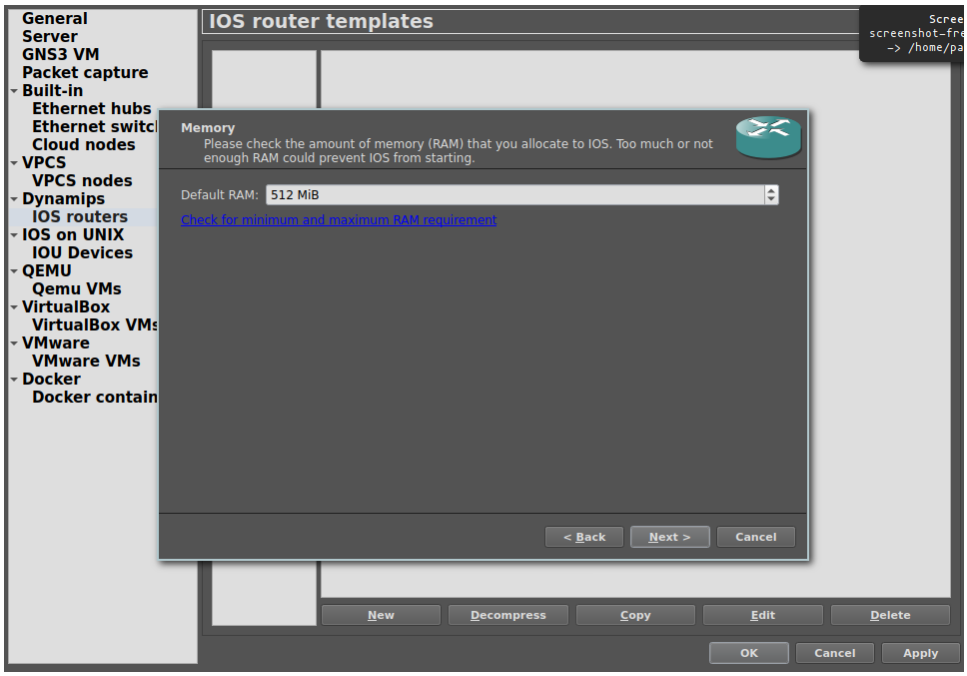


Figure 3.7. Choosing the default ram for the Cisco router.

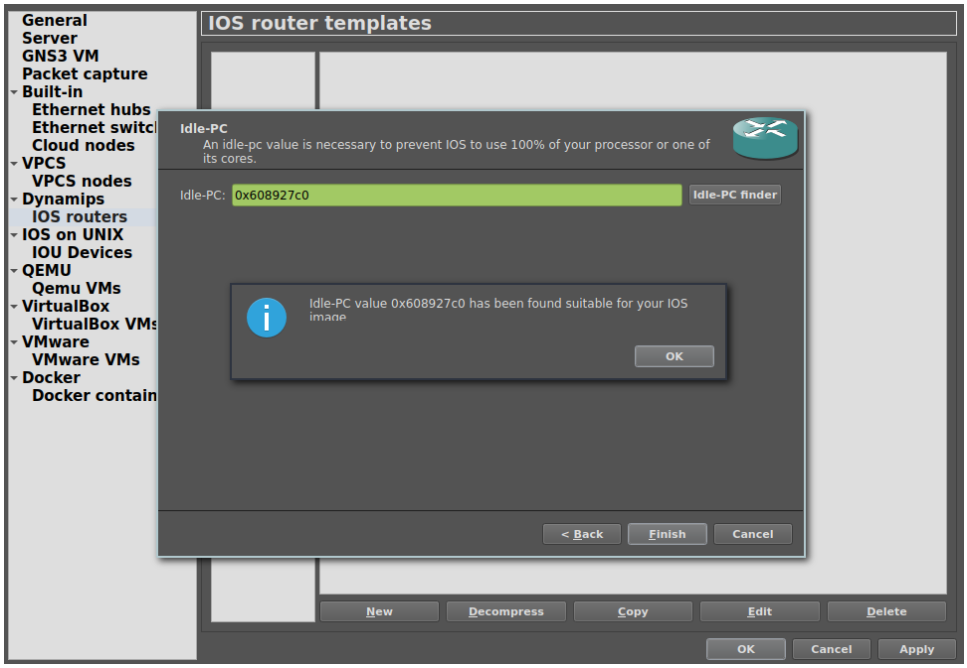


Figure 3.8. Clicking the "Idle-PC finder" to find the suitable Idle-PC value for the IOS image.

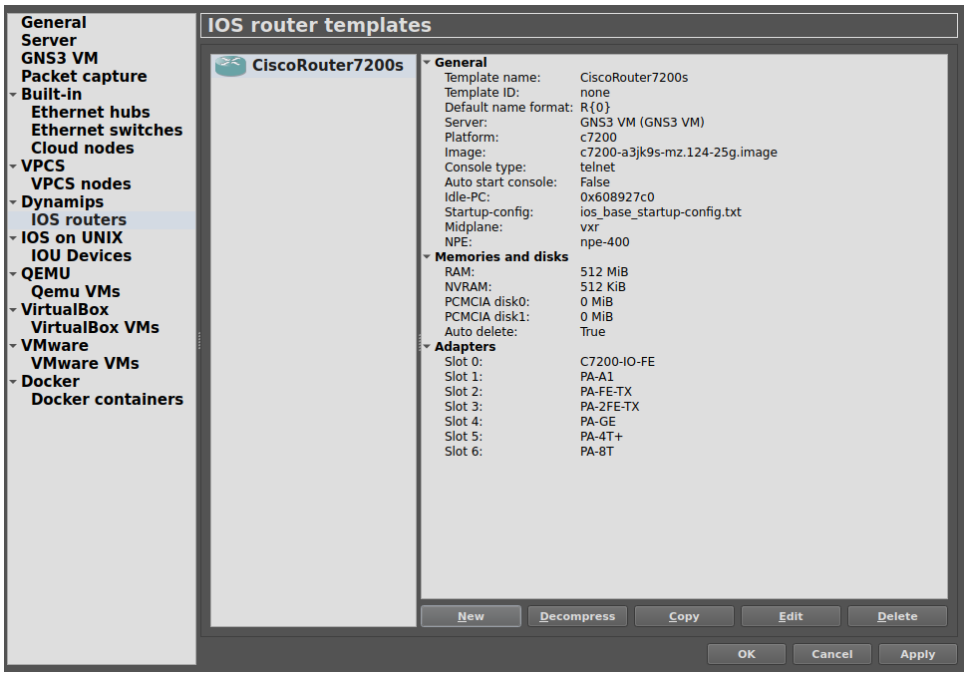


Figure 3.9. The screenshot above shows the summary of the Cisco router's current set up.

ADDING CISCO SWITCH

IOS. https://mega.nz/#!QB1gzayQ!ANSuffpwnf-I-FjYCJUIciaMpAEDL5POquGtPTX8KeA

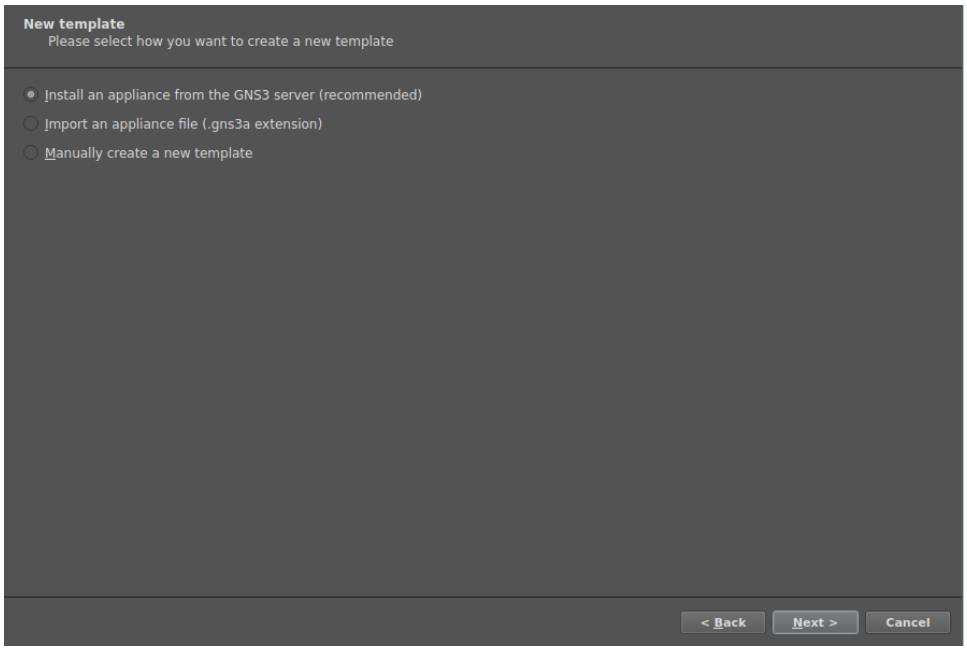


Figure 3.10. Clicking "New Template" and selecting "Install an appliance from the GNS3 server (recommended)."

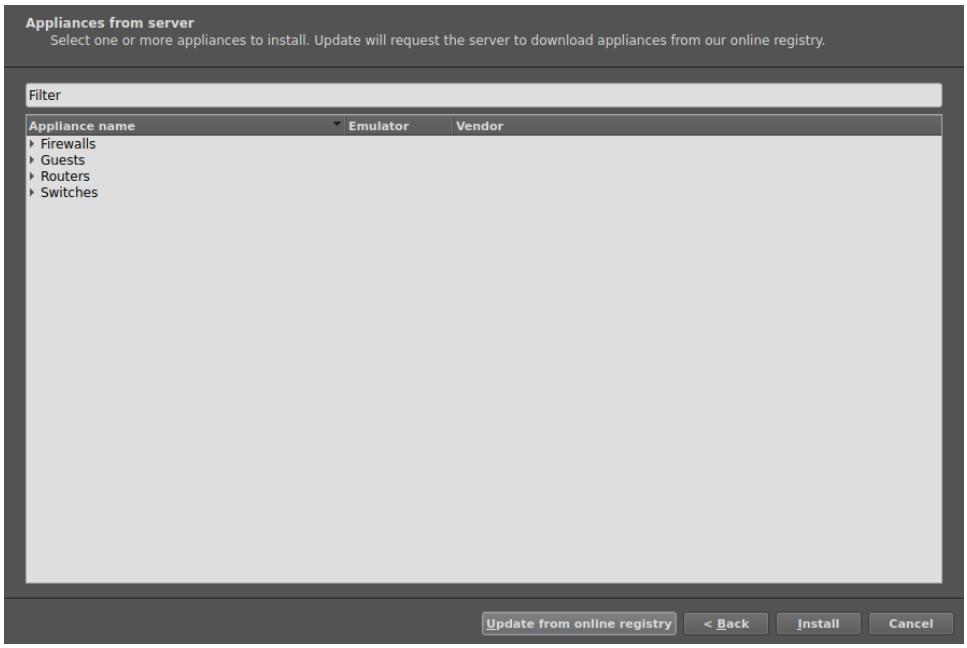


Figure 3.11. Clicking "Update from online registry" to update the repository of hardware devices.

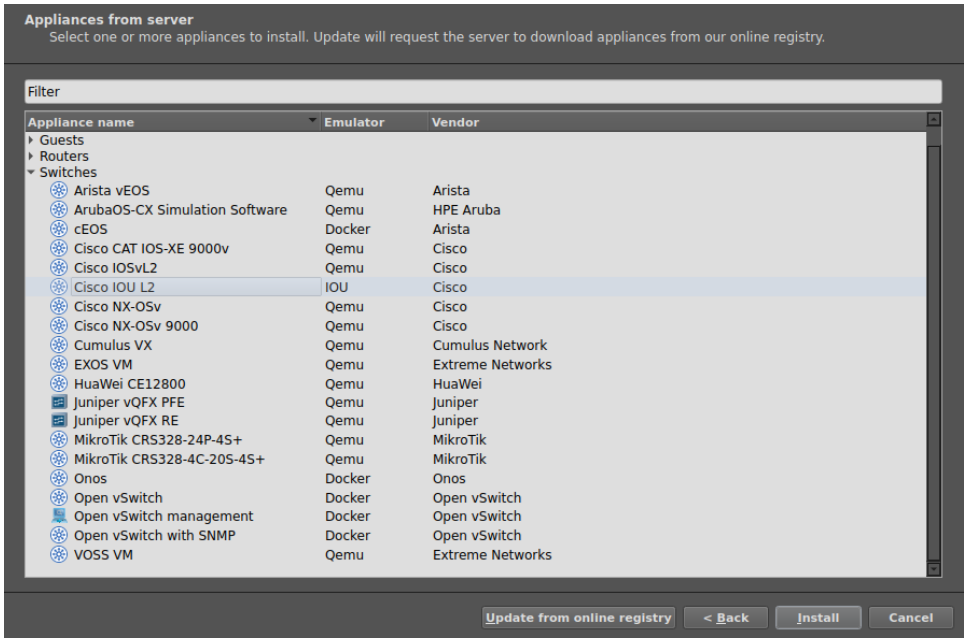


Figure 3.11. Choosing "Cisco IOU L2" to show available layer 2 switches.

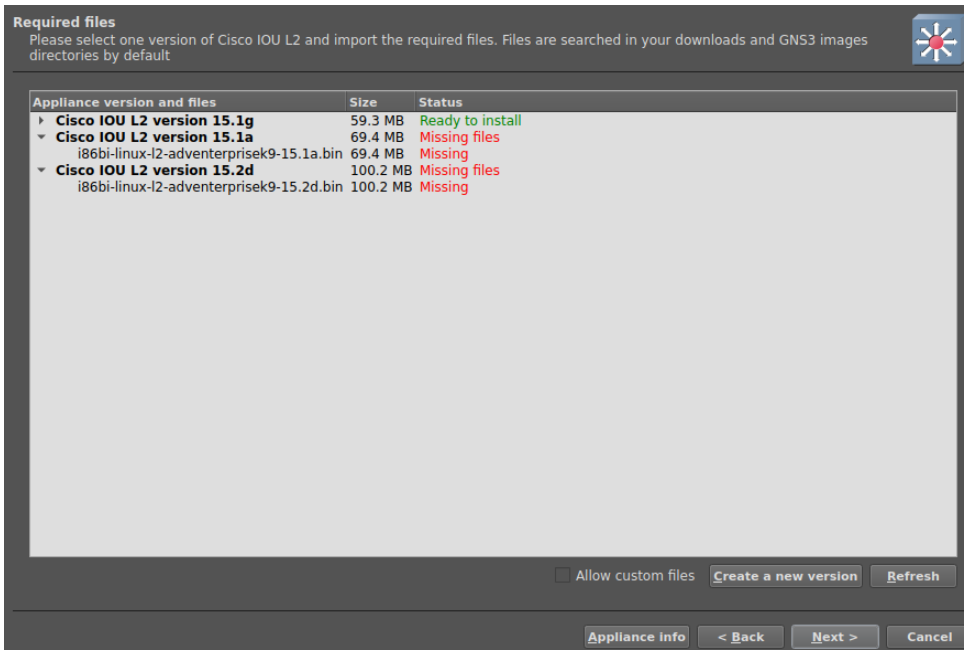


Figure 3.12. Choosing the first version of the choices.

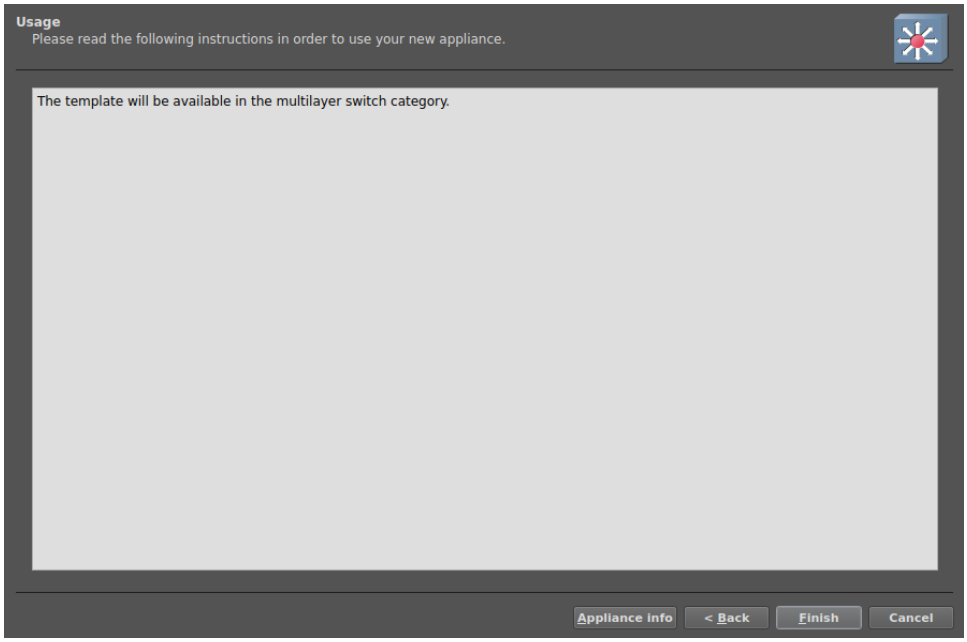


Figure 3.13. The screenshot above shows the prompt for the added switch in the multilayer switch category.

ADDING IOU LICENCE

```
[license]
gns3vm = 73635fd3b0a13ad0;
```

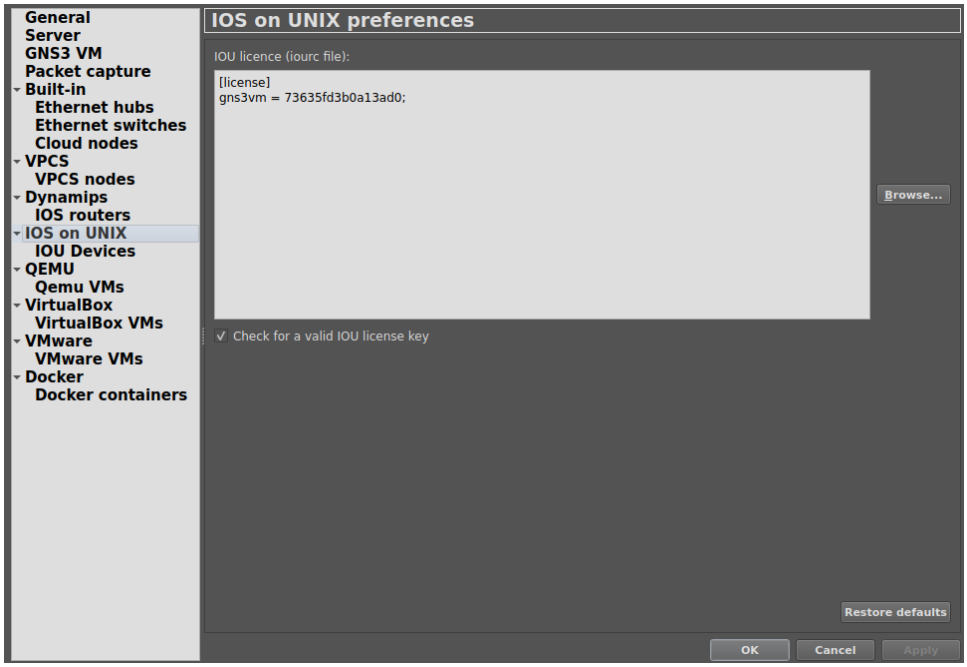


Figure 3.14. Adding an IOU license.

[4] CREATING THE TOPOLOGY

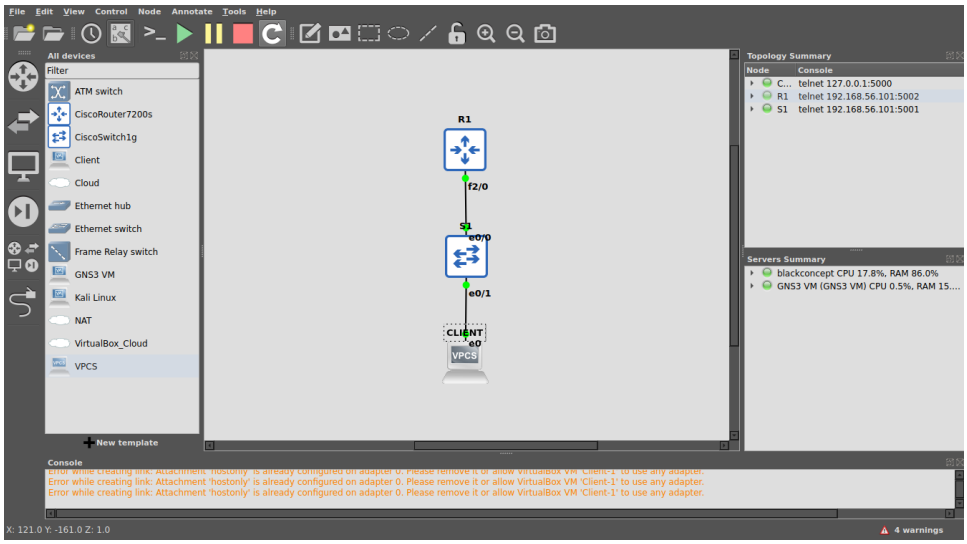


Figure 4.0. Setting up the topology.

[5] ROUTER ANSIBLE SECURITY AUTOMATION DEPLOYMENT

Basic Configuration to Access SSH

```
enable
configure terminal
int f 0/0
ip address 192.168.254.2 255.255.255.0
description R1_TO_NAT
no shut
ip domain-name www.tip.edu.ph
username cisco secret cisco
username cisco privilege 15
line vty 0 4
transport input all
login local
crypto key generate rsa
ip ssh version 2
do write
```

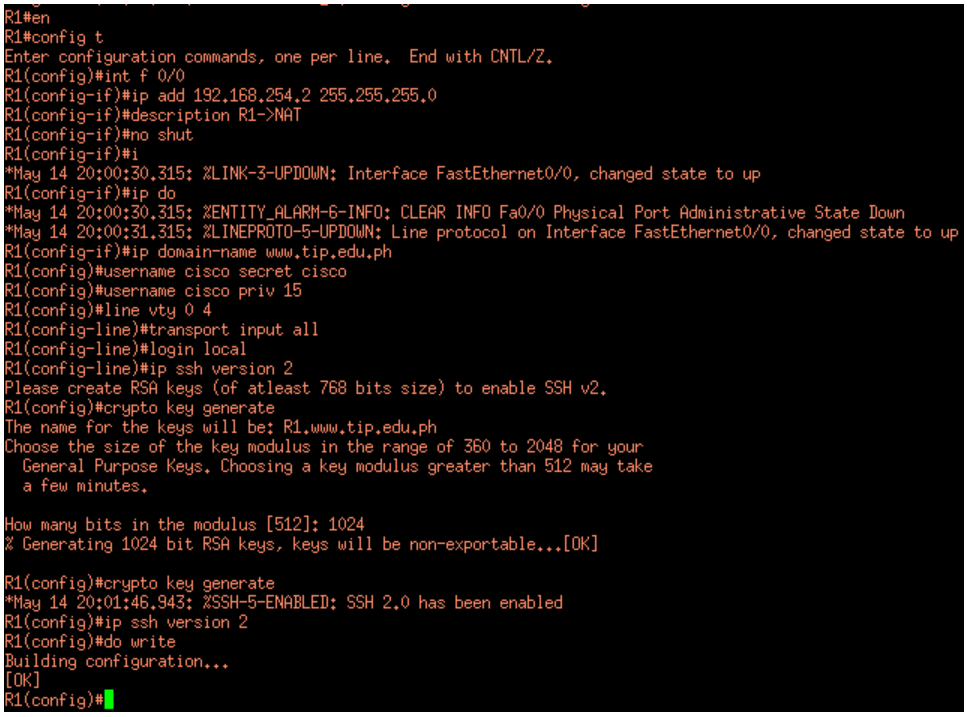


Figure 5. Configuring the router manually to enable SSH connection.

Configuring /home/papzi/.ssh/config

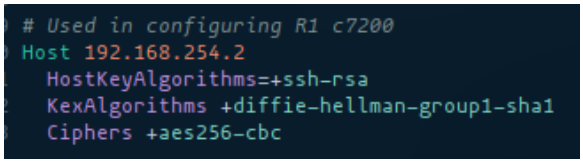


Figure 5.1. Configuring SSH config to use a certain algorithm for HostKeyAlgorithm, KexAlgorithms, and Ciphers.

Ping 192.168.254.2

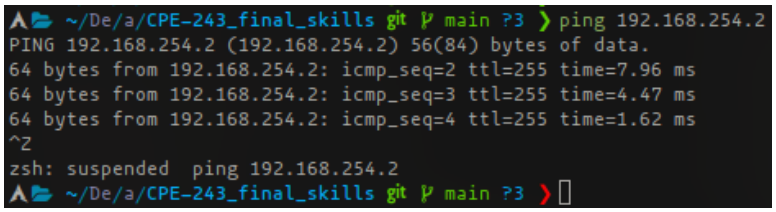


Figure 5.1. Checking if the workstation can ping the interface of the router.

SSH to 192.168.254.2

```
~/De/a/CPE-243_final_skills git  main ?3 ❯ ssh cisco@192.168.254.2
The authenticity of host '192.168.254.2 (192.168.254.2)' can't be established.
RSA key fingerprint is SHA256:6lX+e3RlT8Y1iDB+EIvnPyr8Oa53snYzfCXnk6DsSWQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.254.2' (RSA) to the list of known hosts.
(cisco@192.168.254.2) Password:

R1#
```

Figure 5.2. Trying to connect to the router using SSH.

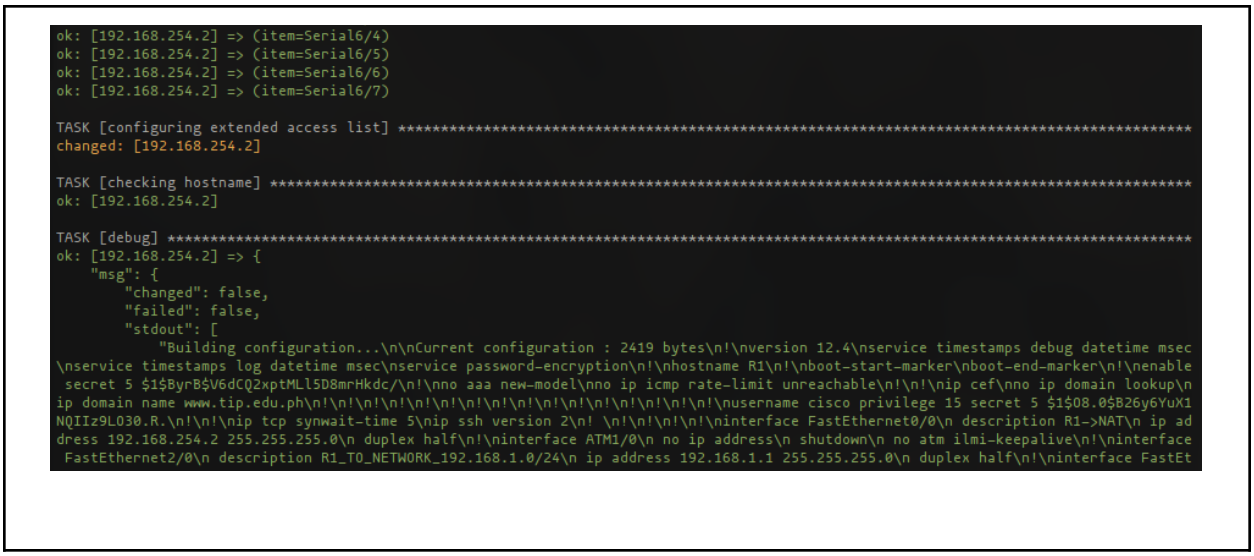
Installing ansible-pylibssh

```
~/De/a/CPE-243_final_skills git  main ?3 ❯ pip install ansible-pylibssh
Defaulting to user installation because normal site-packages is not writeable
Collecting ansible-pylibssh
  Downloading ansible_pylibssh-1.1.0-cp311-cp311-manylinux_2_24_x86_64.whl (2.3 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.3/2.3 MB 3.2 MB/s eta 0:00:00
Installing collected packages: ansible-pylibssh
Successfully installed ansible-pylibssh-1.1.0
```

Figure 5.3. Installing ansible-pylibssh using pip.

Executing Playbook

```
~/De/a/CPE-243_final_skills git  main ?5 ❯ ansible-playbook config_R1.yml -K                    44s  17:35:57
BECOME password:

PLAY [routers] ***************************************************************************************************************************

TASK [Apply the provided configuration] **************************************************************************************************
ok: [192.168.254.2]

TASK [configuring login banner] **********************************************************************************************************
ok: [192.168.254.2]

TASK [configuring domain name] ***********************************************************************************************************
ok: [192.168.254.2]

TASK [configuring line con 0] ************************************************************************************************************
[WARNING]: To ensure idempotency and correct diff the input configuration lines should be similar to how they appear if present in
the running configuration on device
changed: [192.168.254.2]

TASK [configuring privilege exec mode password] ******************************************************************************************
changed: [192.168.254.2]

TASK [saving running config to startup config] *******************************************************************************************
changed: [192.168.254.2]

TASK [configuring ip address in f2/0] ****************************************************************************************************
changed: [192.168.254.2]

TASK [configuring service password-encryption] *******************************************************************************************
ok: [192.168.254.2]

TASK [Shutdown interfaces] ***************************************************************************************************************
ok: [192.168.254.2] => (item=ATM1/0)
ok: [192.168.254.2] => (item=FastEthernet3/0)
ok: [192.168.254.2] => (item=FastEthernet3/1)
ok: [192.168.254.2] => (item=GigabitEthernet4/0)
ok: [192.168.254.2] => (item=Serial5/0)
ok: [192.168.254.2] => (item=Serial5/1)
ok: [192.168.254.2] => (item=Serial5/2)
ok: [192.168.254.2] => (item=Serial5/3)
ok: [192.168.254.2] => (item=Serial6/0)
ok: [192.168.254.2] => (item=Serial6/1)
ok: [192.168.254.2] => (item=Serial6/2)
ok: [192.168.254.2] => (item=Serial6/3)
```


ok: [192.168.254.2] => (item=Serial6/4)
ok: [192.168.254.2] => (item=Serial6/5)
ok: [192.168.254.2] => (item=Serial6/6)
ok: [192.168.254.2] => (item=Serial6/7)
TASK [configuring extended access list] ********
changed: [192.168.254.2]
TASK [checking hostname] ********
ok: [192.168.254.2]
TASK [debug] ********
ok: [192.168.254.2] => {
"msg": {
"changed": false,
"failed": false,
"stdout": [
"Building configuration...\n\nCurrent configuration : 2419 bytes\n!\nversion 12.4\nservice timestamps debug datetime msec
\nservice timestamps log datetime msec\nservice password-encryption\n!\nhostname R1\n!\nboot-start-marker\nboot-end-marker\n!\nenable
secret 5 1ByrB$V6dCQ2xptMLl5D8mrHkdc/\n!\nno aaa new-model\nno ip icmp rate-limit unreachable\n!\n!\nip cef\nno ip domain lookup\n
ip domain name www.tip.edu.ph\n!\n!\n!\n!\n!\n!\n!\n!\n!\n!\n!\n!\n!\n!\n!\n!\n!\nusername cisco privilege 15 secret 5 $1$08.0$B26y6YuX1
NQIIz9LO30.R.\n!\n!\nip tcp synwait-time 5\nip ssh version 2\n! \n!\n!\n!\n!\ninterface FastEthernet0/0\n description R1->NAT\n ip ad
dress 192.168.254.2 255.255.255.0\n duplex half\n!\ninterface ATM1/0\n no ip address\n shutdown\n no atm ilmi-keepalive\n!\ninterface
FastEthernet2/0\n description R1_TO_NETWORK_192.168.1.0/24\n ip address 192.168.1.1 255.255.255.0\n duplex half\n!\ninterface FastEt

```
o\n speed auto\n!\ninterface GigabitEthernet4/0\n no ip address\n shutdown\n negotiation auto\n!\ninterface Serial5/0\n no ip address
\n shutdown\n serial restart-delay 0\n!\ninterface Serial5/1\n no ip address\n shutdown\n serial restart-delay 0\n!\ninterface Serial
5/2\n no ip address\n shutdown\n serial restart-delay 0\n!\ninterface Serial5/3\n no ip address\n shutdown\n serial restart-delay 0\n
!\ninterface Serial6/0\n no ip address\n shutdown\n serial restart-delay 0\n!\ninterface Serial6/1\n no ip address\n shutdown\n seria
l restart-delay 0\n!\ninterface Serial6/2\n no ip address\n shutdown\n serial restart-delay 0\n!\ninterface Serial6/3\n no ip address
\n shutdown\n serial restart-delay 0\n!\ninterface Serial6/4\n no ip address\n shutdown\n serial restart-delay 0\n!\ninterface Serial
6/5\n no ip address\n shutdown\n serial restart-delay 0\n!\ninterface Serial6/6\n no ip address\n shutdown\n serial restart-delay 0\n
!\ninterface Serial6/7\n no ip address\n shutdown\n serial restart-delay 0\n!\n!\nip forward-protocol nd\n!\nno ip http server\nno ip
 http secure-server\n!\n!\n!\nip access-list extended ACL_SECURITY\naccess-list 100 permit tcp host 192.168.56.109 any eq 22\nno cdp
log mismatch duplex\n!\n!\n!\ncontrol-plane\n!\n!\n!\n!\n!\ngatekeeper\n shutdown\n!\nbanner motd ^C\nUnauthorized Personels are P
rohibited!\n^C\n!\nline con 0\n exec-timeout 0 0\n privilege level 15\n password 7 02050D480809\n logging synchronous\n login\n stopb
its 1\nline aux 0\n exec-timeout 0 0\n privilege level 15\n logging synchronous\n stopbits 1\nline vty 0 4\n login local\n transport
input all\n!\n!\nend"
        ],
        "stdout_lines": [
            [
                "Building configuration...",
                "",
                "Current configuration : 2419 bytes",
                "!",
                "version 12.4",
                "service timestamps debug datetime msec",
                "service timestamps log datetime msec",
                "service password-encryption",
                "!",
                "hostname R1",
                "!",
                "boot-start-marker",
                "boot-end-marker",
                "!",
                "enable secret 5 $1$ByrB$V6dCQ2xptMLl5D8mrHkdc/",
                "!",
                "no aaa new-model",
                "no ip icmp rate-limit unreachable",
                "!",
                "!",
                "ip cef",
                "no ip domain lookup",
                "ip domain name www.tip.edu.ph",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "!",
                "username cisco privilege 15 secret 5 $1$08.0$B26y6YuX1NQIIz9LO30.R.",
                "!",
                "!",
                "ip tcp synwait-time 5",
                "ip ssh version 2",
                "! ",
                "!",
                "!",
                "!",
                "!",
                "interface FastEthernet0/0",
                " description R1->NAT",
                " ip address 192.168.254.2 255.255.255.0",
                " duplex half",
                "!",
                "interface ATM1/0",
                " no ip address",
                " shutdown",
                " no atm ilmi-keepalive",
                "!",
                "interface FastEthernet2/0",
                " description R1_TO_NETWORK_192.168.1.0/24",
                " ip address 192.168.1.1 255.255.255.0",
                " duplex half",
                "!",
                "interface FastEthernet3/0",
                " no ip address",
                " shutdown",
                " duplex auto",
                " speed auto",
                "!",
```

```
"interface FastEthernet3/1",
" no ip address",
" shutdown",
" duplex auto",
" speed auto",
"!",
"interface GigabitEthernet4/0",
" no ip address",
" shutdown",
" negotiation auto",
"!",
"interface Serial5/0",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial5/1",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial5/2",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial5/3",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial6/0",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial6/1",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial6/2",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial6/3",
" no ip address",
" shutdown",
" serial restart-delay 0",
```

```
"!",
"interface Serial6/4",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial6/5",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial6/6",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"interface Serial6/7",
" no ip address",
" shutdown",
" serial restart-delay 0",
"!",
"!",
"ip forward-protocol nd",
"!",
"no ip http server",
"no ip http secure-server",
"!",
"!",
"!",
"ip access-list extended ACL_SECURITY",
"access-list 100 permit tcp host 192.168.56.109 any eq 22",
"no cdp log mismatch duplex",
"!",
"!",
"!",
"control-plane",
"!",
"!",
```

Figure 5.4. The screenshots above show the result after running the playbook.

[6] SWITCH ANSIBLE SECURITY AUTOMATION DEPLOYMENT

Basic Configuration to Access SSH

```
enable
configure terminal
int vlan 1
ip address 192.168.1.254 255.255.255.0
no shut
ip domain-name www.tip.edu.ph
username cisco secret cisco
username cisco privilege 15
line vty 0 4
transport input all
login local
crypto key generate rsa
ip ssh version 2
ip default-gateway 192.168.56.2
do copy running-config startup-config
```

Configuring /home/papzi/.ssh/config

```
# Used in configuring S1
Host 192.168.254.3
  HostKeyAlgorithms=+ssh-rsa
  KexAlgorithms +diffie-hellman-group1-sha1
  Ciphers +aes256-cbc
```

Figure 6. Configuring SSH config to use a certain algorithm for HostKeyAlgorithm, KexAlgorithms, and Ciphers.

Ping 192.168.254.3

```
~/De/a/CPE-243_final_skills git  main ?3 ❯ ping 192.168.254.3
PING 192.168.254.3 (192.168.254.3) 56(84) bytes of data.
64 bytes from 192.168.254.3: icmp_seq=1 ttl=255 time=0.967 ms
64 bytes from 192.168.254.3: icmp_seq=2 ttl=255 time=1.66 ms
64 bytes from 192.168.254.3: icmp_seq=3 ttl=255 time=0.716 ms
64 bytes from 192.168.254.3: icmp_seq=4 ttl=255 time=0.702 ms
^C
--- 192.168.254.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 0.702/1.012/1.663/0.390 ms
~/De/a/CPE-243_final_skills git  main ?3 ❯
```

Figure 6.2. Checking if the workstation can ping the interface of the switch.

SSH to 192.168.254.3

```
~/De/a/CPE-243_final_skills git  main ?3 ❯ ssh cisco@192.168.254.3
The authenticity of host '192.168.254.3 (192.168.254.3)' can't be established.
RSA key fingerprint is SHA256:8ze3YuQdmt15EDIfeu6gpYYoeFvDZQOnowyM1UYWP6E.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.254.3' (RSA) to the list of known hosts.
(cisco@192.168.254.3) Password:

S1#
```

Figure 6.3. Trying to connect to the router using SSH.

Executing Playbook

```
~/De/a/CPE-243_final_skills git main ?4 ❯ ansible-playbook basic_config_S1.yml -k                    lf 1 05:10:21
SSH password:

PLAY [switches] ***************************************************************************************************************************

TASK [Apply the provided configuration] ***************************************************************************************************
ok: [192.168.254.3]

TASK [configuring login banner] ***********************************************************************************************************
ok: [192.168.254.3]

TASK [configuring domain name] ************************************************************************************************************
ok: [192.168.254.3]

TASK [configuring line con 0] *************************************************************************************************************
[WARNING]: To ensure idempotency and correct diff the input configuration lines should be similar to how they appear if present in
the running configuration on device
changed: [192.168.254.3]

TASK [configuring privilege exec mode password] *******************************************************************************************
changed: [192.168.254.3]

TASK [saving running config to startup config] ********************************************************************************************
changed: [192.168.254.3]

TASK [configuring service password-encryption] ********************************************************************************************
ok: [192.168.254.3]

TASK [Shutdown interfaces] ****************************************************************************************************************
ok: [192.168.254.3] => (item=Ethernet0/3)
ok: [192.168.254.3] => (item=Ethernet1/0)
ok: [192.168.254.3] => (item=Ethernet1/1)
ok: [192.168.254.3] => (item=Ethernet1/2)
ok: [192.168.254.3] => (item=Ethernet1/3)
ok: [192.168.254.3] => (item=Ethernet2/0)
ok: [192.168.254.3] => (item=Ethernet2/1)
ok: [192.168.254.3] => (item=Ethernet2/2)
ok: [192.168.254.3] => (item=Ethernet2/3)
ok: [192.168.254.3] => (item=Ethernet3/0)
ok: [192.168.254.3] => (item=Ethernet3/1)
ok: [192.168.254.3] => (item=Ethernet3/2)
ok: [192.168.254.3] => (item=Ethernet3/3)

TASK [checking hostname] ******************************************************************************************************************
ok: [192.168.254.3]

TASK [debug] ******************************************************************************************************************************
ok: [192.168.254.3] => {
    "msg": {
        "changed": false,
        "failed": false,
        "stdout": [
            "Building configuration...\n\nCurrent configuration : 2007 bytes\n!\n! Last configuration change at 21:10:33 UTC Sun May
14 2023 by cisco\n!\nversion 15.1\nservice timestamps debug datetime msec\nservice timestamps log datetime msec\nservice password-enc
ryption\nservice compress-config\n!\nhostname S1\n!\nboot-start-marker\nboot-end-marker\n!\n!\nlogging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL \nlogging buffered 50000\nlogging console discriminator EXCESS\nenable secret 4 06YFDUHH61wAE/kLkDq
9BGho1QM5EnRtoyr8cHAUg.2\n!\nusername cisco privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY\nno aaa new-model\nno i
pv6 cef\nipv6 multicast rpf use-bgp\nno ip icmp rate-limit unreachable\n!\nno ip domain-lookup\nip domain-name www.tip.edu.ph\nip cef
\n!\n!\n!\n!\nspanning-tree mode pvst\nspanning-tree extend system-id\n!\n!\n!\n!\nvlan internal allocation policy ascending\n!\nip t
cp synwait-time 5\nip ssh version 2\n! \n!\n!\n!\n!\n!\n!\n!\ninterface Ethernet0/0\n duplex auto\n!\ninterface Ethernet0/1\n dupl
ex auto\n!\ninterface Ethernet0/2\n duplex auto\n!\ninterface Ethernet0/3\n shutdown\n duplex auto\n!\ninterface Ethernet1/0\n shutdo
wn\n duplex auto\n!\ninterface Ethernet1/1\n shutdown\n duplex auto\n!\ninterface Ethernet1/2\n shutdown\n duplex auto\n!\ninterface
Ethernet1/3\n shutdown\n duplex auto\n!\ninterface Ethernet2/0\n shutdown\n duplex auto\n!\ninterface Ethernet2/1\n shutdown\n duplex
 auto\n!\ninterface Ethernet2/2\n shutdown\n duplex auto\n!\ninterface Ethernet2/3\n shutdown\n duplex auto\n!\ninterface Ethernet3/0
\n shutdown\n duplex auto\n!\ninterface Ethernet3/1\n shutdown\n duplex auto\n!\ninterface Ethernet3/2\n shutdown\n duplex auto\n!\ni
nterface Ethernet3/3\n shutdown\n duplex auto\n!\ninterface Vlan1\n ip address 192.168.254.3 255.255.255.0\n!\nip default-gateway 192
.168.56.1\n!\nno ip http server\n!\n!\n!\n!\n!\ncontrol-plane\n!\nbanner motd ^C\nUnauthorized Personels are Prohibited!\n^C\n!\nline
 con 0\n exec-timeout 0 0\n privilege level 15\n password 7 104D000A0618\n logging synchronous\n login\nline aux 0\n exec-timeout 0 0
\n privilege level 15\n logging synchronous\nline vty 0 4\n login local\n transport input all\n!\nend"
        ],
        "stdout_lines": [
            [
                "Building configuration...",
                "",
                "Current configuration : 2007 bytes",
                "!",
                "! Last configuration change at 21:10:33 UTC Sun May 14 2023 by cisco",
                "!",
                "version 15.1",
                "service timestamps debug datetime msec",
                "service timestamps log datetime msec",
                "service password-encryption",
```

```
"service compress-config",
"!",
"hostname S1",
"!",
"boot-start-marker",
"boot-end-marker",
"!",
"!",
"logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL ",
"logging buffered 50000",
"logging console discriminator EXCESS",
"enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2",
"!",
"username cisco privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY",
"no aaa new-model",
"no ipv6 cef",
"ipv6 multicast rpf use-bgp",
"no ip icmp rate-limit unreachable",
"!",
"no ip domain-lookup",
"ip domain-name www.tip.edu.ph",
"ip cef",
"!",
"!",
"!",
"!",
"!",
"spanning-tree mode pvst",
"spanning-tree extend system-id",
"!",
"!",
"!",
"!",
"!",
"vlan internal allocation policy ascending",
"!",
"ip tcp synwait-time 5",
"ip ssh version 2",
"! ",
"!",
"!",
"!",
"!",
"!",
"!",
"!",
"!",
"!",
"interface Ethernet0/0",
" duplex auto",
"!",
"interface Ethernet0/1",
" duplex auto",
"!",
"interface Ethernet0/2",
" duplex auto",
"!",
```

```
" duplex auto",
"!",
"interface Ethernet1/0",
" shutdown",
" duplex auto",
"!",
"interface Ethernet1/1",
" shutdown",
" duplex auto",
"!",
"interface Ethernet1/2",
" shutdown",
" duplex auto",
"!",
"interface Ethernet1/3",
" shutdown",
" duplex auto",
"!",
"interface Ethernet2/0",
" shutdown",
" duplex auto",
"!",
"interface Ethernet2/1",
" shutdown",
" duplex auto",
"!",
"interface Ethernet2/2",
" shutdown",
" duplex auto",
"!",
"interface Ethernet2/3",
" shutdown",
" duplex auto",
"!",
"interface Ethernet3/0",
```

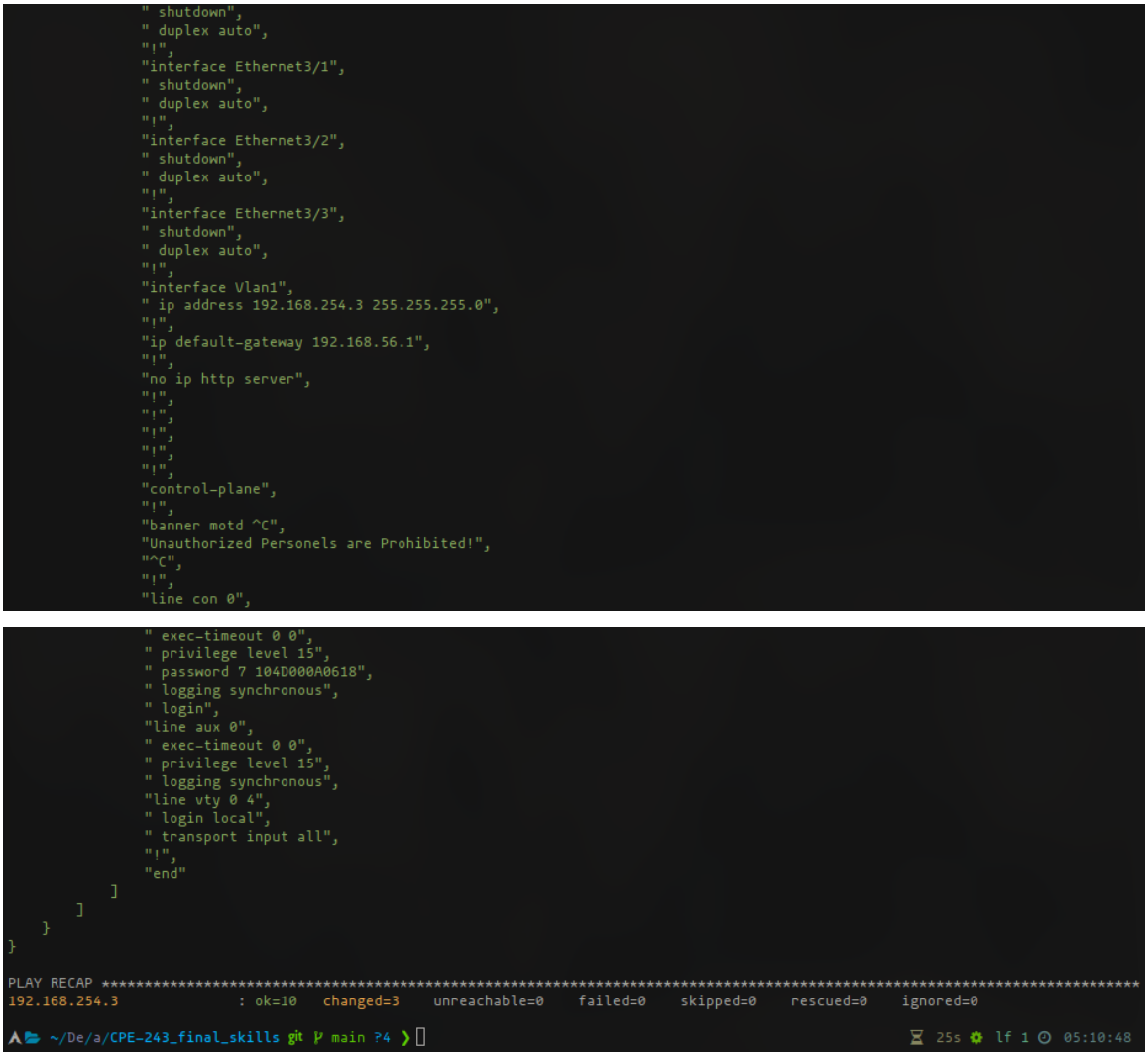


Figure 6.4. The screenshots above show the result after running the playbook.

[7] CONFIGURING CLIENT PC WITH IMPLEMENTED SECURITY

Checking connection between Workstation and Client PC

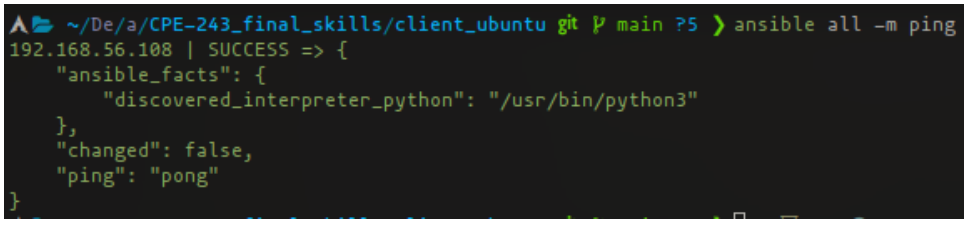


Figure 7.1. The screenshot above shows that the connection between workstation and client PC is successful.

Executing Playbook

```
~/De/a/CPE-243_final_skills/client_ubuntu git  main ?5 ❯ ansible-playbook main.yml -K
BECOME password:

PLAY [all] *********************************************************************

TASK [Gathering Facts] *********************************************************
^Z
zsh: suspended  ansible-playbook main.yml -K
~/De/a/CPE-243_final_skills/client_ubuntu git  main ?5 ❯ ansible-playbook main.yml -K
BECOME password:

PLAY [all] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.56.109]

TASK [Dpkg fixing in ubuntu servers] *******************************************
changed: [192.168.56.109]

TASK [Updating Ubuntu] *********************************************************
changed: [192.168.56.109]

TASK [Perform full patching] ***************************************************
ok: [192.168.56.109]

TASK [Add admin group] *********************************************************
changed: [192.168.56.109]

TASK [Add local user] **********************************************************
changed: [192.168.56.109]

TASK [Add SSH public key for user] *********************************************
changed: [192.168.56.109]

TASK [Add sudoer role for local user] ******************************************
changed: [192.168.56.109]

TASK [Add hardened SSH config] *************************************************
changed: [192.168.56.109]

TASK [Installing firewalld in ubuntu] ******************************************
changed: [192.168.56.109]

TASK [Add SSH port to internal zone] *******************************************
ok: [192.168.56.109]

TASK [Add permitted networks to internal zone] *********************************
changed: [192.168.56.109] => (item=192.168.56.0/24)
changed: [192.168.56.109] => (item=192.168.254.0/24)
changed: [192.168.56.109] => (item=10.0.3.0/24)

TASK [Drop ssh from the public zone] *******************************************
changed: [192.168.56.109]

TASK [Remove undesirable packages] *********************************************
changed: [192.168.56.109]

TASK [Stop and disable unnecessary services] ***********************************
failed: [192.168.56.109] (item=postfix) => {"ansible_loop_var": "item", "changed": f
alse, "item": "postfix", "msg": "Could not find the requested service postfix: host"
}
failed: [192.168.56.109] (item=telnet) => {"ansible_loop_var": "item", "changed": fa
lse, "item": "telnet", "msg": "Could not find the requested service telnet: host"}
...ignoring

TASK [Set a message of the day] ************************************************
```

```
TASK [Set a login hammer] ******************************************************
changed: [192.168.56.109] => (item=/etc/issue)
changed: [192.168.56.109] => (item=/etc/issue.net)

TASK [Installing Snort] ********************************************************
changed: [192.168.56.109]

TASK [Starting Snort service] **************************************************
ok: [192.168.56.109]

TASK [Enabling Snort service] **************************************************
fatal: [192.168.56.109]: FAILED! => {"changed": false, "msg": "value of state must b
e one of: reloaded, restarted, started, stopped, got: enabled"}
...ignoring

TASK [Installing openssl] ******************************************************
ok: [192.168.56.109]

TASK [Creating folder for CA] **************************************************
changed: [192.168.56.109] => (item=ca)
changed: [192.168.56.109] => (item=ca/certs)
changed: [192.168.56.109] => (item=ca/newcerts)
changed: [192.168.56.109] => (item=ca/private)

TASK [Creating index.txt] ******************************************************
changed: [192.168.56.109]

TASK [Duplicating openssl.cnf] *************************************************
changed: [192.168.56.109]

TASK [Generating private key] **************************************************
changed: [192.168.56.109]

TASK [Generating certificate signing request] **********************************
changed: [192.168.56.109]

TASK [Generating selfsigned certificate] ***************************************
changed: [192.168.56.109]

TASK [Creating folder in control node] *****************************************
changed: [192.168.56.109]

TASK [Copying log files] *******************************************************
changed: [192.168.56.109] => (item=alternatives.log)
changed: [192.168.56.109] => (item=auth.log)
changed: [192.168.56.109] => (item=bootstrap.log)
changed: [192.168.56.109] => (item=btmp)
changed: [192.168.56.109] => (item=dpkg.log)
changed: [192.168.56.109] => (item=faillog)
failed: [192.168.56.109] (item=fontconfig.log) => {"ansible_loop_var": "item", "chan
ged": false, "item": "fontconfig.log", "msg": "the remote file does not exist, not t
ransferring, ignored"}
failed: [192.168.56.109] (item=gpu-manager.log) => {"ansible_loop_var": "item", "cha
nged": false, "item": "gpu-manager.log", "msg": "the remote file does not exist, not
 transferring, ignored"}
changed: [192.168.56.109] => (item=kern.log)
changed: [192.168.56.109] => (item=lastlog)
changed: [192.168.56.109] => (item=syslog)
failed: [192.168.56.109] (item=syslog.1) => {"ansible_loop_var": "item", "changed":
false, "item": "syslog.1", "msg": "the remote file does not exist, not transferring,
 ignored"}
failed: [192.168.56.109] (item=tallylog) => {"ansible_loop_var": "item", "changed":
false, "item": "tallylog", "msg": "the remote file does not exist, not transferring,
 ignored"}
changed: [192.168.56.109] => (item=ubuntu-advantage.log)
changed: [192.168.56.109] => (item=ubuntu-advantage-timer.log)
failed: [192.168.56.109] (item=vboxpostinstall.log) => {"ansible_loop_var": "item",
"changed": false, "item": "vboxpostinstall.log", "msg": "the remote file does not ex
```

```
changed: [192.168.56.109] => (item=ubuntu-advantage.log)
changed: [192.168.56.109] => (item=ubuntu-advantage-timer.log)
failed: [192.168.56.109] (item=vboxpostinstall.log) => {"ansible_loop_var": "item",
"changed": false, "item": "vboxpostinstall.log", "msg": "the remote file does not ex
ist, not transferring, ignored"}
changed: [192.168.56.109] => (item=wtmp)
```

```
PLAY RECAP *********************************************************************
192.168.56.109             : ok=28   changed=21   unreachable=0    failed=1    skipp
ed=0    rescued=0    ignored=2
```

Figure 7.2. The screenshot above shows result after running the playbook.

Note. The warnings under the last task notifies that there are no log files with the current loop named in the Client PC and does not affect the executed tasks.

FILE & DIRECTORY STRUCTURE

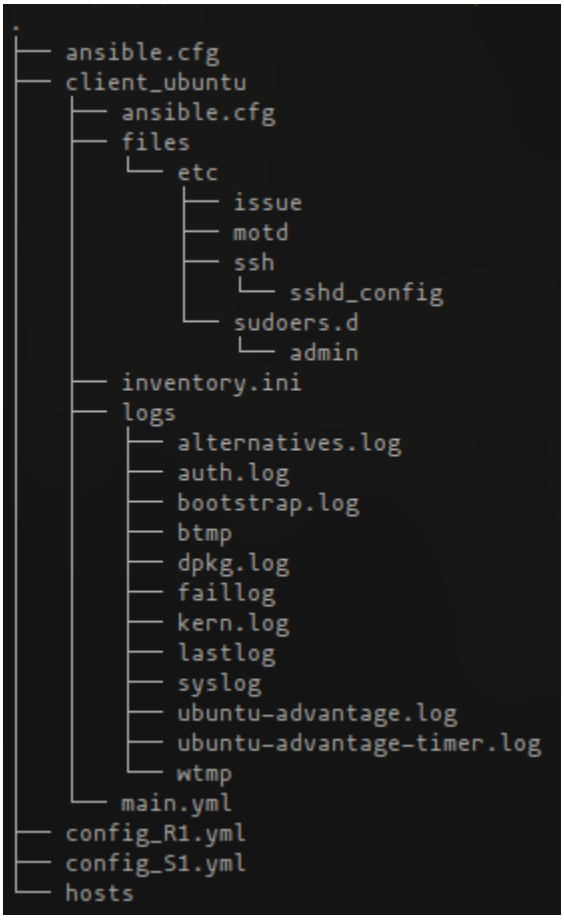


Figure 7.3. The screenshot above shows the file and directory structure of the ansible scripts.

CODE

ansible.cfg	~/De/a/CPE-243_final_skills git main ?5 ❯ cat ansible.cfg 06:47:33
	[defaults]
	
	inventory = hosts
	
	# dont worry about rsa fingerprints
	host_key_checking = False
	
	# disable gather facts
	gather = explicit
	
	# stating python interpreter_python
	interpreter_python = /usr/bin/python3
	
	deprecation_warnings = False
	
	# retry file = gather the node that are failed the excution and save in this file (good for large environment)
	# retry_files_enabled = False
	#
	ansible_connection = local

hosts	~/De/a/CPE-243_final_skills git main ?5 ❯ cat hosts [routers] 192.168.254.2 [switches] 192.168.254.3 [routers:vars] ansible_user=cisco ansible_password=cisco ansible_connection=network_cli ansible_network_os=ios #ansible_become=yes #ansible_become_method=enable [switches:vars] ansible_user=cisco ansible_password=cisco ansible_connection=network_cli ansible_network_os=ios #ansible_become=yes #ansible_become_method=enable

config_R1.yml	~/De/a/CPE-243_final_skills git main ?5 ❯ cat config_R1.yml
	--- 	
	
	- hosts: routers
	  become: true
	  gather_facts: no
	  tasks:
	
	  - name: Apply the provided configuration
	  cisco.ios.ios_hostname:
	  config:
	  hostname: R1
	  state: merged
	
	  - name: configuring login banner
	  cisco.ios.ios_banner:

```
      banner: motd
      text: |
        Unauthorized Personels are Prohibited!
      state: present

  - name: configuring domain name
    cisco.ios.ios_system:
      domain_name: www.tip.edu.ph
      state: present

  - name: configuring line con 0
    cisco.ios.ios_config:
      lines:
      - password cisco
      - login
      - logging synchronous
      parents: line console 0

  - name: configuring privilege exec mode password
    cisco.ios.ios_config:
      lines: enable secret class

  - name: saving running config to startup config
    cisco.ios.ios_config:
      save_when: modified

  - name: configuring ip address in f2/0
    cisco.ios.ios_config:
      lines:
      - description R1_TO_NETWORK_192.168.1.0/24
      - ip address 192.168.1.1 255.255.255.0
      - no shutdown
      parents: interface FastEthernet2/0

  # implementing security
  - name: configuring service password-encryption
    cisco.ios.ios_config:
      lines:
      - service password-encryption

  - name: Shutdown interfaces
    cisco.ios.ios_config:
      lines:
        - shutdown
      parents: "interface {{ item }}"
    with_items:
      - ATM1/0
      - FastEthernet3/0
      - FastEthernet3/1
      - GigabitEthernet4/0
      - Serial5/0
      - Serial5/1
```

config_S1.yml	~/De/a/CPE-243_final_skills git main ?5 ❯ cat config_S1.yml 06:49:34
	--- 	
	
	- hosts: switches
	  become: true
	  gather_facts: no
	  tasks:
	
	  - name: Apply the provided configuration
	  cisco.ios.ios_hostname:
	  config:
	  hostname: S1
	  state: merged
	
	  - name: configuring login banner
	  cisco.ios.ios_banner:
	  banner: motd
	  text: |
	  Unauthorized Personels are Prohibited!
	  state: present
	
	  - name: configuring domain name
	  cisco.ios.ios_system:
	  domain_name: www.tip.edu.ph
	  state: present
	
	  - name: configuring line con 0
	  cisco.ios.ios_config:
	  lines:
	  - password cisco
	  - login
	  - logging synchronous
	  parents: line console 0
	
	  - name: configuring privilege exec mode password
	  cisco.ios.ios_config:
	  lines: enable secret class
	
	  - name: saving running config to startup config
	  cisco.ios.ios_config:
	  save_when: modified
	
	  # implementing security
	  - name: configuring service password-encryption
	  cisco.ios.ios_config:
	  lines:
	  - service password-encryption
	
	  - name: Shutdown interfaces
	  cisco.ios.ios_config:
	  lines:
	  - shutdown
	  parents: "interface {{ item }}"
	  with_items:
	
	  # displaying current config
	  - block:
	
	  - name: checking hostname
	  cisco.ios.ios_command:
	  commands: show run
	  register: output_run
	
	  - debug:
	  msg="{{ output_run }}"

client_ubuntu/ansible.cfg	~/De/a/CPE-243_final_skills/client_ubuntu git main ?5 ❯ cat ansible.cfg [defaults] inventory = inventory.ini host_key_checking = False deprecation_warnings = False private_key_file = ~/.ssh/id_rsa ansible_python_interpreter = /usr/bin/python3
client_ubuntu/inventory.ini	~/De/a/CPE-243_final_skills/client_ubuntu git main ?5 ❯ cat inventory.ini [ubuntu] 192.168.56.109 ansible_user=client

Table 1. The table above shows the code that is used in the entire network infrastructure with security policy implemented.

Justification in Implemented Security Measures

R1

- Shutdown unused ports:
    - This will prevent hackers from penetrating or tapping the open ports.
- Declaring passwords in console and VTY ports:
    - This will prevent hackers to configure the router.
- Using extended access list to restrict unwanted packets:
    - This will ensure that the traffic is all valid between the incoming packets and receiving packets.
- Using service password-encryption:
    - Encrypting password and preventing plain text passwords in show commands.
- Applying banner MOTD
    - Notify the non authorized personnel to not enter the network infrastructure premises.

S1

- Shutdown unused ports:
    - This will prevent hackers from penetrating or tapping the open ports.
- Declaring passwords in console and VTY ports:
    - This will prevent hackers from configuring the router.
- Using service password-encryption:
    - Encrypting password and preventing plain text passwords in show commands.
- Applying banner MOTD
    - Notify the non authorized personnel to not enter the network infrastructure premises.

CLIENT PC

- Installing Snort IPS
    - This will ensure monitor network traffic and detect potential security threats or malicious activities.
- Saving Log File
    - This will help in determining if there is a threat or penetration happening to the network.
- Uninstalling applications that can used as backend of the hackers
    - This will ensure that there is a little chance of the threat to use an application as its backdoor.
- Installing firewall
    - The firewall will only allow the filtered packets to pass through the system.
- Implementing much secured SSH with custom config
    - Ensuring that the SSH is robust and secure that will only allow permitted devices.

Conclusion

In conclusion, the proposed security solution for the medium-scale IT company's infrastructure aims to protect against online fraud and security threats. By implementing robust hardware and software security measures, including access lists, disabled unused ports, Snort intrusion prevention system (IPS), and a Certificate Authority (CA) with SSL, the company can establish a secure network infrastructure. This solution prioritizes the protection of sensitive data, prevents unauthorized access, and reduces the risk of financial losses. Regular monitoring and analysis of log files are recommended to detect and respond to security incidents promptly. Overall, the solution emphasizes proactive security measures, a defense-in-depth approach, and the collaboration of hardware and software security.