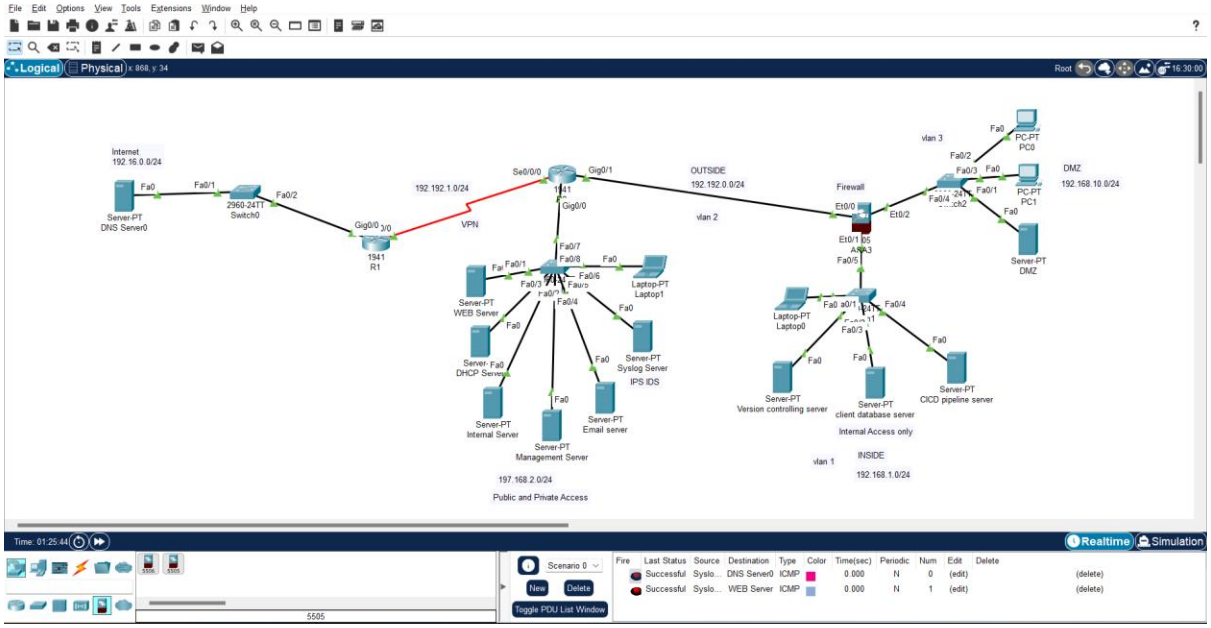
MITS5004 NETWORK DIAGRAM

////Table of Contents

Introduction

In the modern digital world, all business organizations generate data for all their business operations. As it deals with a vast amount of digital assets, computer security is essential for protecting individuals and organizations from cyber threats. As given in the case, Network Co., Inc. is one of the software development organizations that requires establishing a new office and connecting with the existing organization's network. In addition to that, the organization requires that both primary and secondary offices maintain their entire network infrastructure to keep their information safe. The organization is dealing with important information, valuable assets, and information details; safeguarding all information is possible by strengthening the organization's infrastructure. This report will present the strategic placement of security devices and provide a plan for Network Co., Inc.'s business expansion.

TASK1: Draw a Network Diagram



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Syslo...	DNS Server0	ICMP	🟥	0.000	N	0	(edit)	(delete)
●	Successful	Syslo...	WEB Server	ICMP	🟦	0.000	N	1	(edit)	(delete)

Figure 1 Network Diagram

The above-given diagram provides a detailed representation of the network diagram for Network Co., Inc. As given in the design, the internet is connected with firewalls before connecting to the routers as a secure model. Then the routers are directly accessed with primary and secondary internet service protocols [1]. After that, the router signal is captured over multiple switches for transmitting the data. Each department from both Network Co. Inc. will connect with the SE dev department, QA development, IT team, security, management dev, and new office buildings. For protection, several mechanisms are included in the design, such as a firewall and DMZ. Finally, connect with the servers for enhanced communication. Through the servers, both offices can perform access control, monitoring, directory management, and emails.

TASK2: Justifying Network Security

In the context of Network Co Inc, the network security plays a paramount that should focuses on managing evolving landscape of all technology threats. It is significant that could able to manage data breaches, ransomware attacks, industrial espionage, disruption of system, information theft and build customer reputation [2].

Manage Data Breaches

Through the secure network design, the Network Co inc can able to handle valuable and sensitive data. It will be possible by adopting proprietary software information and by accessing client databases. Otherwise the data breaches will affect the unauthorized access to information, financial loss and cause reputational damage and legal consequences [3]. In addition to that protecting customer data is crucial that will maintain trust and focuses on safeguarding personal and financial information.

Restrict Ransomware attacks

As the organization consists of several critical files [4]. There is a possibility that ransomware attacks might disrupts business operation. By having a robust network security infrastructure, users can able to detect and prevent from ransomware attack. In addition to that the effective security protocols will mitigate the risk of DDoS attacks and its uninterrupted services.

Industrial Espionage

This organization is one of the leading software leader, there are more possibility that most of the cybercriminal will attack their network to steal proprietary information and innovative ideas. So that the network security is essential for safeguarding intellectual property and to protect valuable information [4].

Information Theft:

The overall network design focuses on having effective network security. The confidentiality assurance is more important for both the office because that directly involves in protect confidential client data and business strategies.

The network diagram consists of two internet connections from two internet service providers to ensure data redundancy and continuity. This will be helpful in managing the connection failure and enhancing continuity [5]. Each building is connected to the internet through a router, which directs traffic to the respective internet service providers. Finally, switches are placed to facilitate network connections among various devices. All the firewalls are strategically placed to control the incoming and outgoing traffic. The limited use of firewalls is protected by various cost considerations. The servers focus on controlling the overall operation and enhancing the connection through access control servers and other servers.

TASK3: Firewalls Placement

In the process of designing overall network security architecture, Network Co Inc focuses on placing firewall. The main reason for placing the firewall is for effective protection, cost factor, analysis on flow of data to make maximum impact.

Firewall Type	Location	Reasoning
External Firewalls	Internet - Internal Network	First line of defense against external threats, filtering incoming traffic to allow only legitimate and safe data.
Perimeter Firewalls	Between Internet Connections	Extra layer of protection, controlling traffic between different internet connections and the internal network.
Internal Firewalls	Between Departments	Protects sensitive data by controlling traffic between different departments, preventing unauthorized access.
Departmental Firewalls	Between Specific Departments	Enhances security by isolating and protecting servers within each department from internal and external threats [6].
DMZ Firewalls	Entry and Exit Points of DMZ	Controls traffic entering and leaving the DMZ, safeguarding servers that require public access from

		potential threats.
BYOD and Remote Access	Entry Points for External Devices	Secures external devices accessing the network, ensuring compliance with security policies and protecting against threats introduced through external devices.

The placement of all the firewall helps all the management division by adopting overall critical function and to safeguard all the data by managing internal and external threats. In addition to that identify the DMZ control traffic by protecting servers and adoption on model with public access such as web servers [5]. In addition to that there were several security policies against potential threats for creating security zone on controlling overall data flows and minimize security breaches.

Overall Benefits

- The placement of firewall effectively secure overall network without overburdening in cost factor.
- The strategic placement creates security zone on offering protection to critical assets, control data flow and minimize data breaches [6].

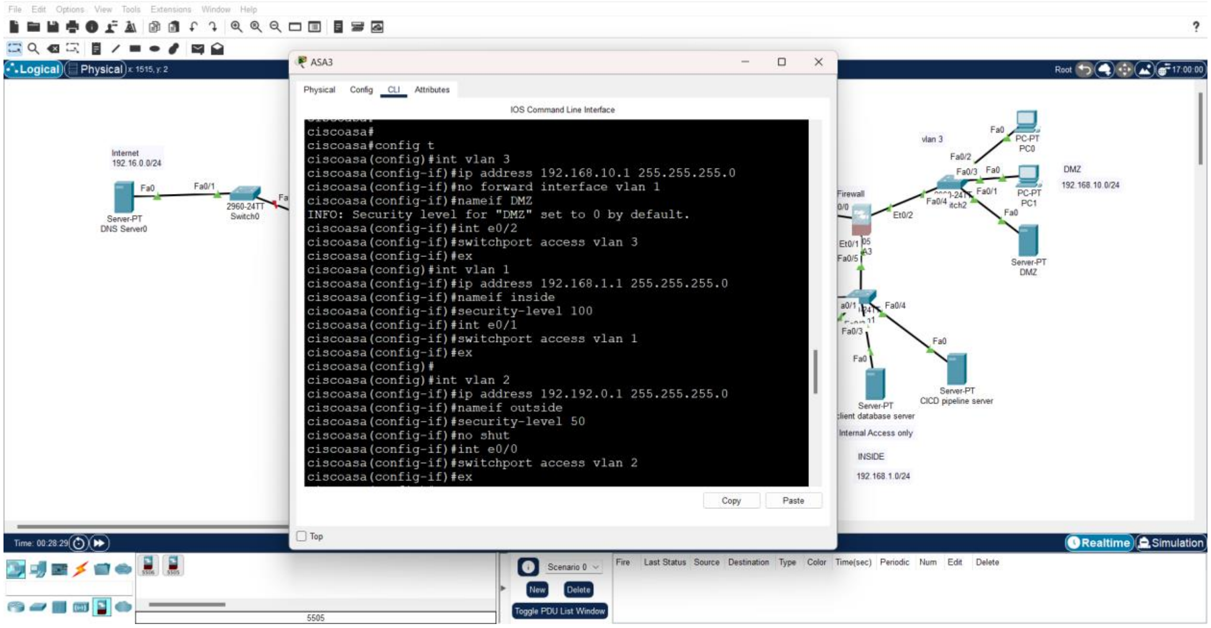
By implementing the placement, Network Co Inc can able to achieve a balance for cost effectiveness, robust network security and availability of its data and services.

TASK4: DMZ Configuration

Demilitarized Zone

It is a critical component of network architecture that is place in external and internal network. It is high designed for enhancing services and to access from internal network.

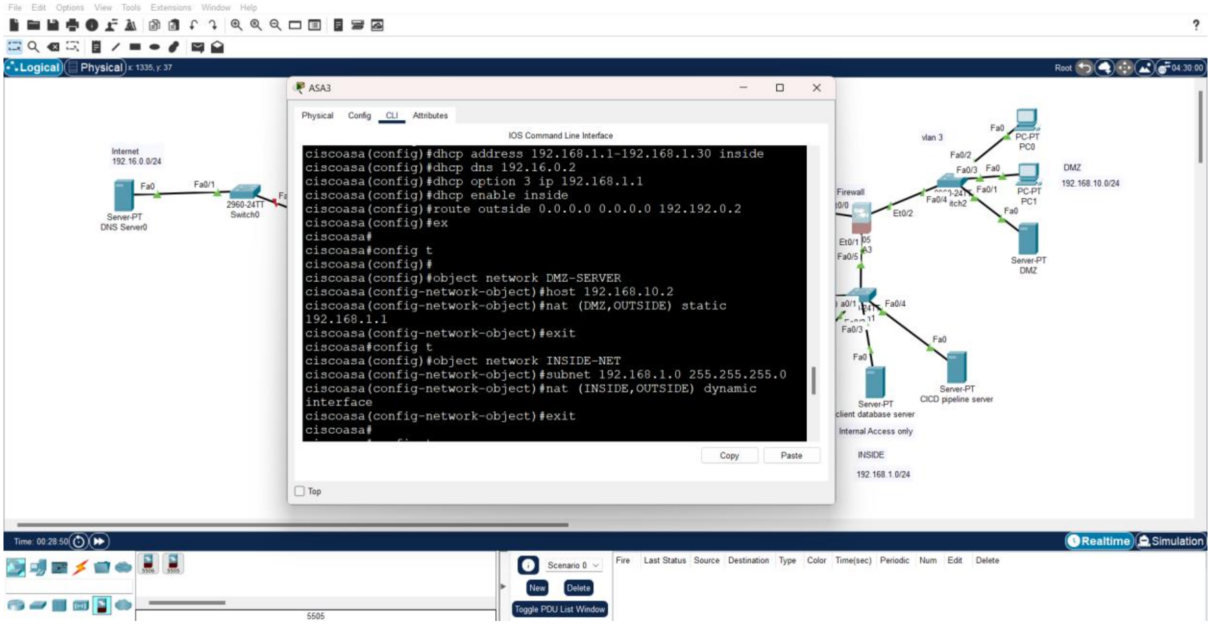
<u>DMZ Configuration</u>



```
ciscoasa#
ciscoasa#config t
ciscoasa(config)#int vlan 3
ciscoasa(config-if)#ip address 192.168.10.1 255.255.255.0
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)#int e0/2
ciscoasa(config-if)#switchport access vlan 3
ciscoasa(config-if)#ex
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#int e0/1
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#ex
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip address 192.192.0.1 255.255.255.0
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#no shut
ciscoasa(config-if)#int e0/0
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#ex
```

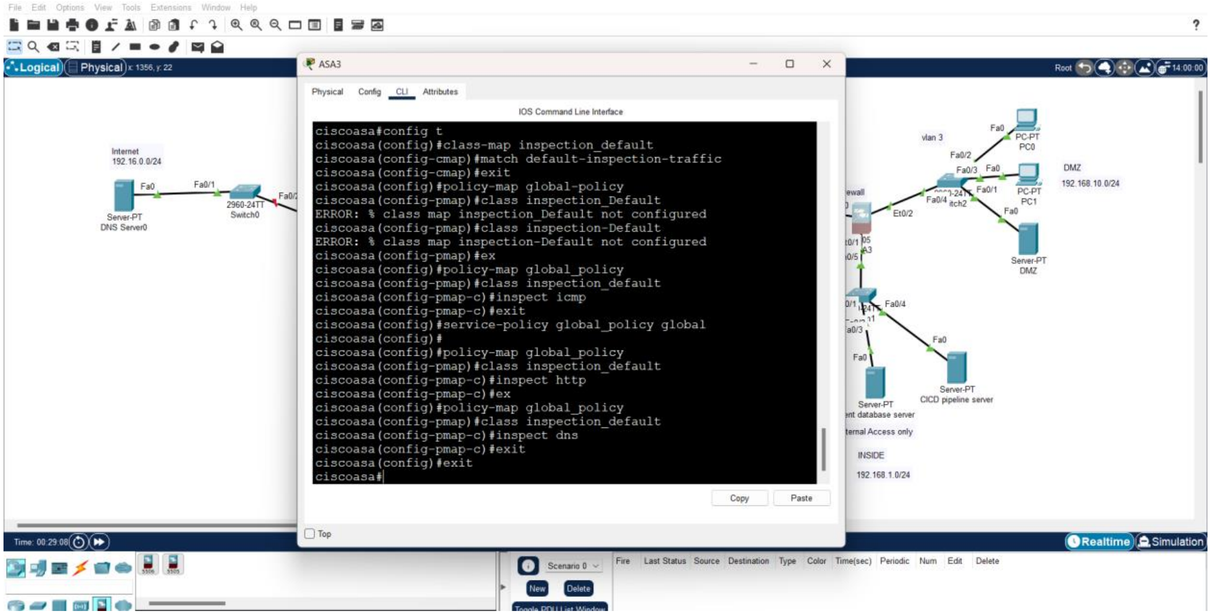
Figure 2 Figure for DMZ

The firewall is focusing on deploying firewall at entry and exit points.



```
ciscoasa(config)#dhcp address 192.168.1.1-192.168.1.30 inside
ciscoasa(config)#dhcp dns 192.16.0.2
ciscoasa(config)#dhcp option 3 ip 192.168.1.1
ciscoasa(config)#dhcp enable inside
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 192.192.0.2
ciscoasa(config)#ex
ciscoasa#
ciscoasa#config t
ciscoasa(config)#
ciscoasa(config)#object network DMZ-SERVER
ciscoasa(config-network-object)#host 192.168.10.2
ciscoasa(config-network-object)#nat (DMZ,OUTSIDE) static
192.168.1.1
ciscoasa(config-network-object)#exit
ciscoasa#config t
ciscoasa(config)#object network INSIDE-NET
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (INSIDE,OUTSIDE) dynamic
interface
ciscoasa(config-network-object)#exit
ciscoasa#
```

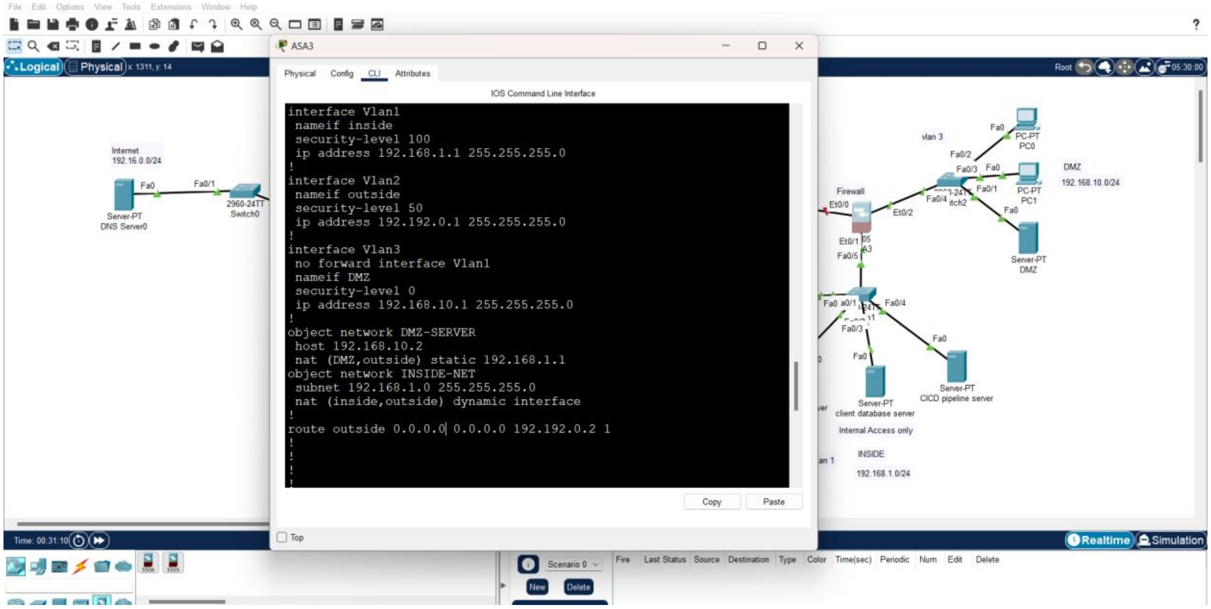
The configuration shows that this would allow only necessary traffics for web, email and DNS without blocking unauthorized access [7].



```
ciscoasa#config t
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global-policy
ciscoasa(config-pmap)#class inspection_Default
ERROR: % class map inspection_Default not configured
ciscoasa(config-pmap)#class inspection-Default
ERROR: % class map inspection-Default not configured
ciscoasa(config-pmap)#ex
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#service-policy global_policy global
ciscoasa(config)#
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect http
ciscoasa(config-pmap-c)#ex
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect dns
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#exit
ciscoasa#
```

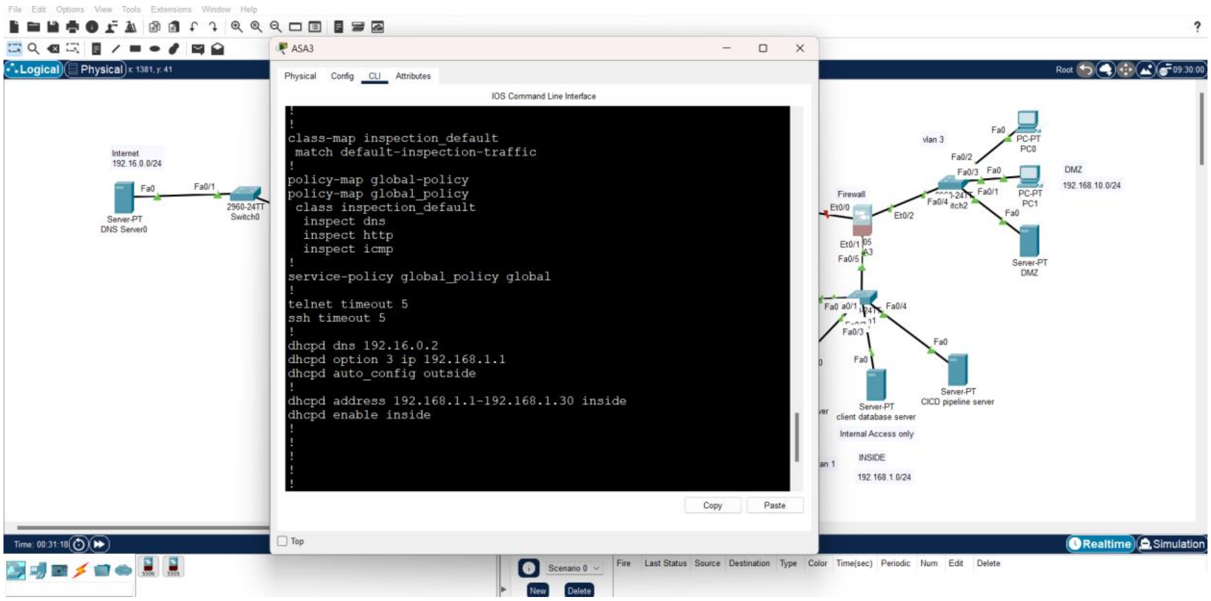
The Intrusion detection and prevention system is integrated with DMZ and improve their overall IPS devices and actively respond to prevent from overall security posture.

Show Run



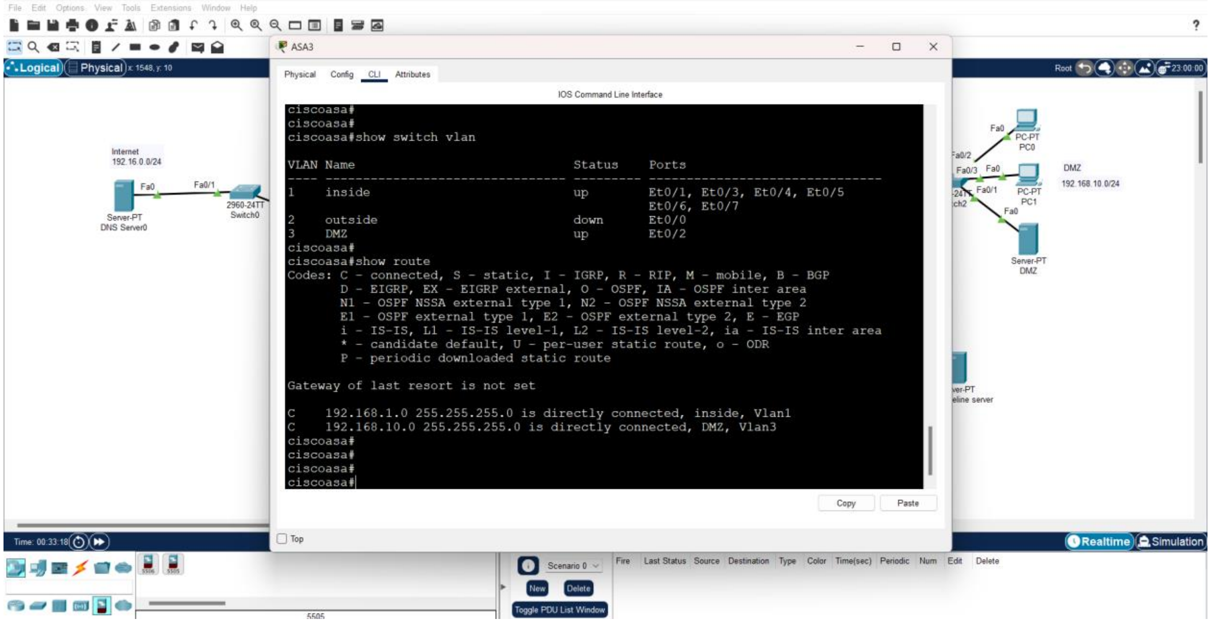
```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 50
 ip address 192.192.0.1 255.255.255.0
!
interface Vlan3
 no forward interface Vlan1
 nameif DMZ
 security-level 0
 ip address 192.168.10.1 255.255.255.0
!
object network DMZ-SERVER
 host 192.168.10.2
 nat (DMZ,outside) static 192.168.1.1
object network INSIDE-NET
 subnet 192.168.1.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 192.192.0.2 1
!
!
!
!
```

The traffic encryption is implemented to employ with security protocols such as HTTPS for web servers and to adopt with proper configuration to secure overall transmission.



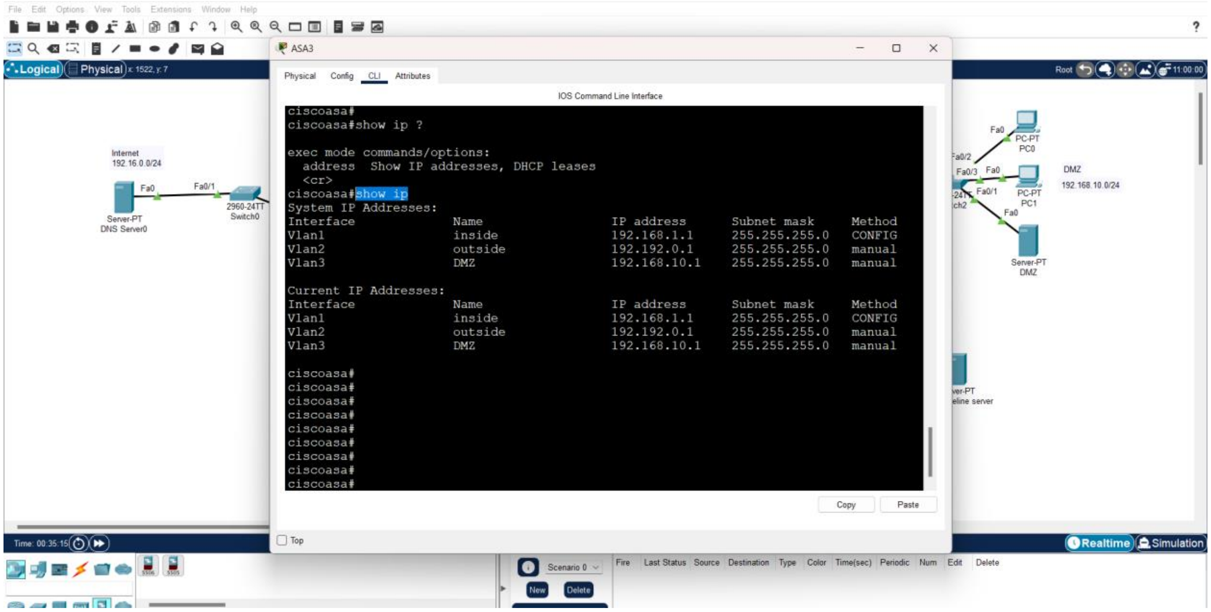
```
!
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map global-policy
policy-map global_policy
 class inspection_default
  inspect dns
  inspect http
  inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
dhcpd dns 192.16.0.2
dhcpd option 3 ip 192.168.1.1
dhcpd auto_config outside
!
dhcpd address 192.168.1.1-192.168.1.30 inside
dhcpd enable inside
!
!
!
!
!
```

This will provide entire protection to eaves dropping and data interception.



```
ciscoasa#
ciscoasa#
ciscoasa#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           up        Et0/1, Et0/3, Et0/4, Et0/5
                                                Et0/6, Et0/7
2    outside                          down      Et0/0
3    DMZ                              up        Et0/2
ciscoasa#
ciscoasa#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
C    192.168.10.0 255.255.255.0 is directly connected, DMZ, Vlan3
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
```

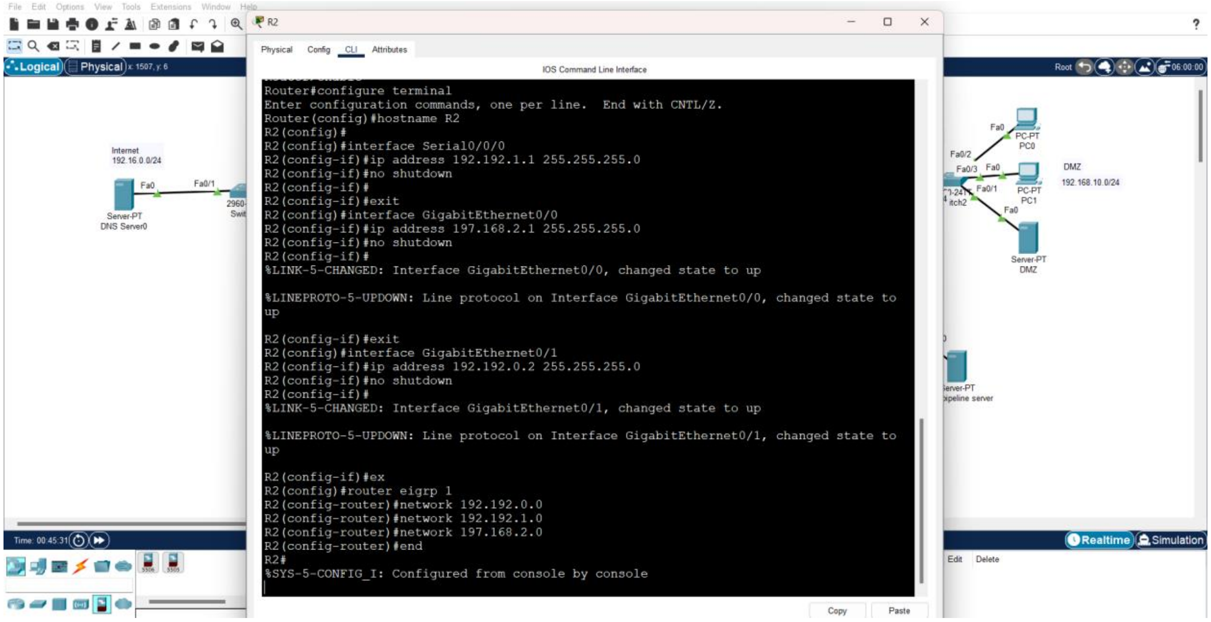
The above given image shows all the gateway information.



```
ciscoasa#
ciscoasa#show ip ?

exec mode commands/options:
  address  Show IP addresses, DHCP leases
  <cr>
ciscoasa#show ip
System IP Addresses:
Interface              Name                 IP address      Subnet mask     Method
Vlan1                  inside               192.168.1.1     255.255.255.0   CONFIG
Vlan2                  outside              192.192.0.1     255.255.255.0   manual
Vlan3                  DMZ                  192.168.10.1    255.255.255.0   manual

Current IP Addresses:
Interface              Name                 IP address      Subnet mask     Method
Vlan1                  inside               192.168.1.1     255.255.255.0   CONFIG
Vlan2                  outside              192.192.0.1     255.255.255.0   manual
Vlan3                  DMZ                  192.168.10.1    255.255.255.0   manual

ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
```

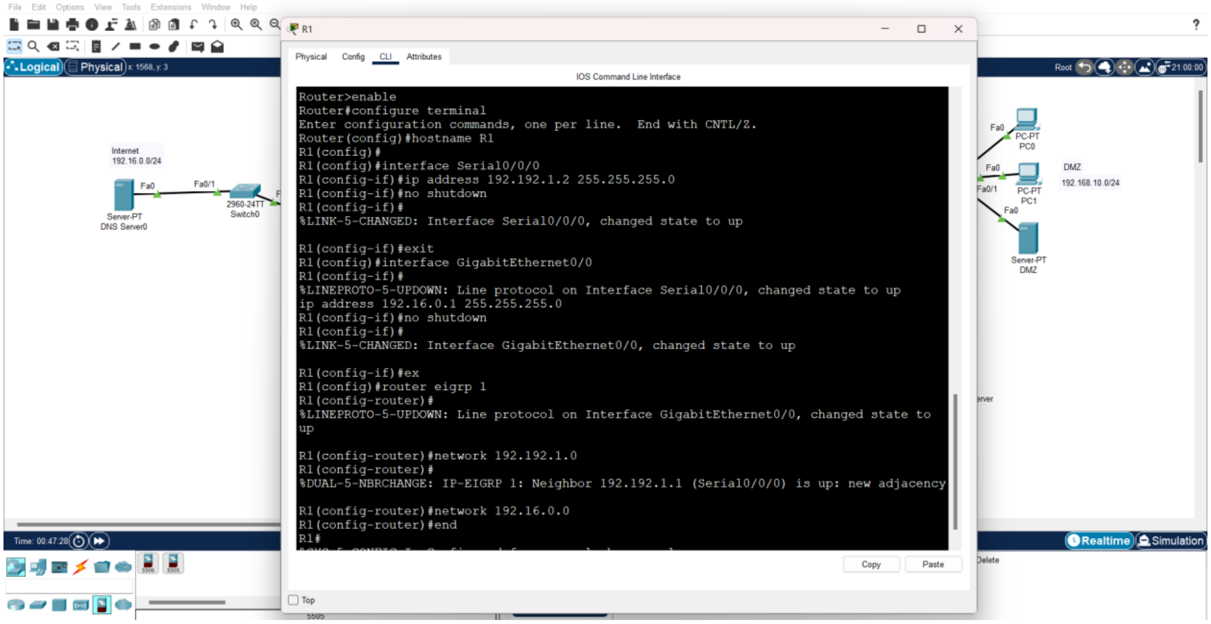
Finally, the logging and monitoring has been implemented for all the DMZ activities that will offer overall protection and by detecting all anomalies.

Router Configuration



```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 192.192.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
R2(config-if)#exit
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip address 197.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
up

R2(config-if)#exit
R2(config)#interface GigabitEthernet0/1
R2(config-if)#ip address 192.192.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
up

R2(config-if)#ex
R2(config)#router eigrp 1
R2(config-router)#network 192.192.0.0
R2(config-router)#network 192.192.1.0
R2(config-router)#network 197.168.2.0
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

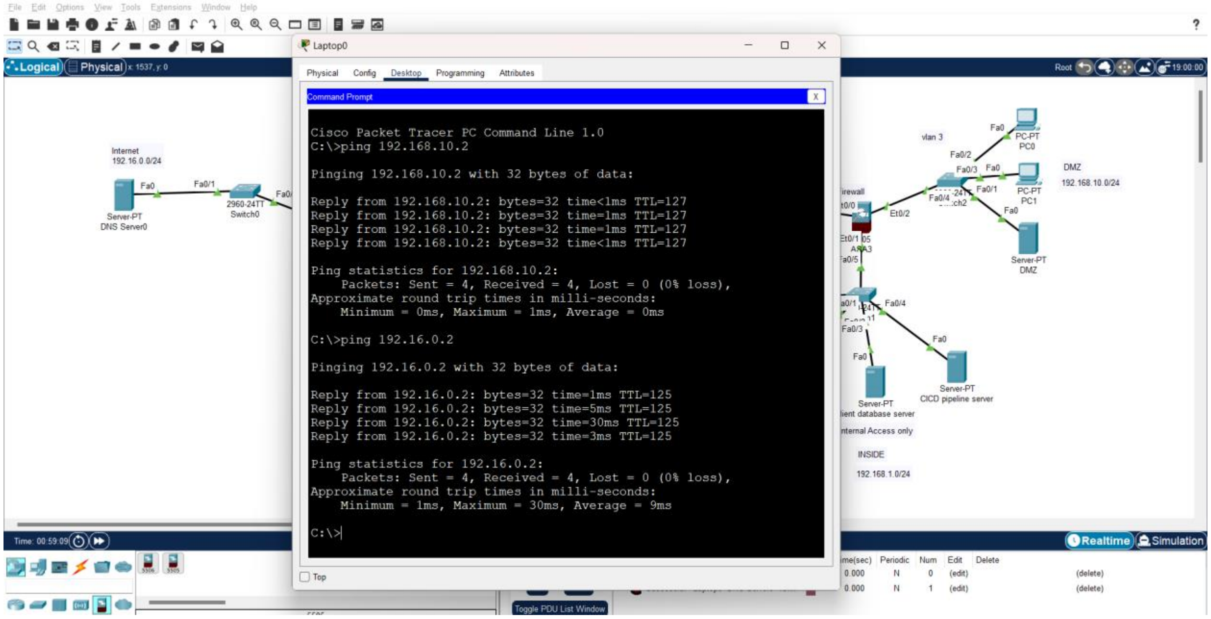
Connection for router is established in this network



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 192.192.1.2 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R1(config-if)#exit
R1(config)#interface GigabitEthernet0/0
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
ip address 192.16.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#ex
R1(config)#router eigrp 1
R1(config-router)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
up

R1(config-router)#network 192.192.1.0
R1(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.192.1.1 (Serial0/0/0) is up: new adjacency

R1(config-router)#network 192.16.0.0
R1(config-router)#end
R1#
```

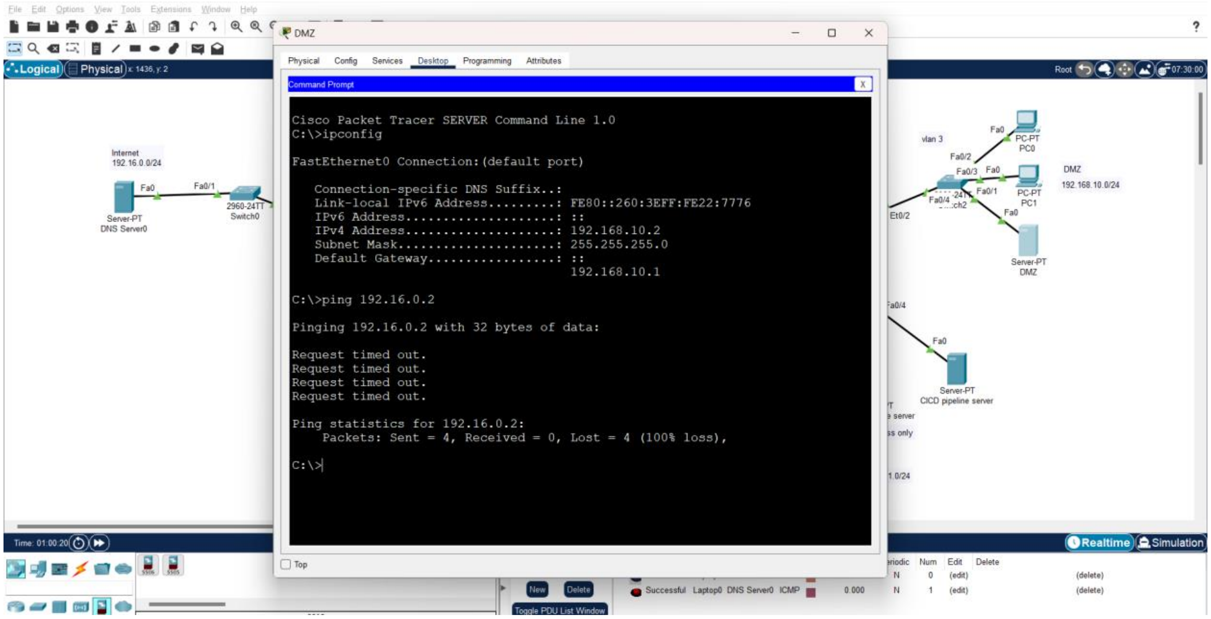
As given above, all the routers were placed.

Ping



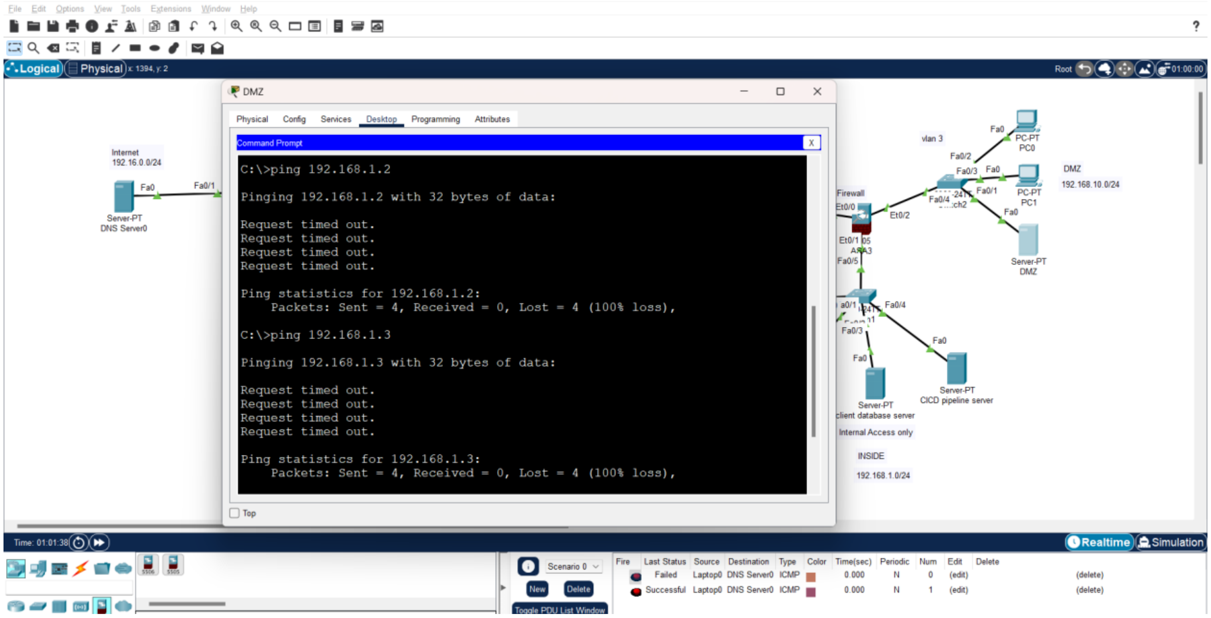
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.16.0.2

Pinging 192.16.0.2 with 32 bytes of data:

Reply from 192.16.0.2: bytes=32 time=1ms TTL=125
Reply from 192.16.0.2: bytes=32 time=5ms TTL=125
Reply from 192.16.0.2: bytes=32 time=30ms TTL=125
Reply from 192.16.0.2: bytes=32 time=3ms TTL=125

Ping statistics for 192.16.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 30ms, Average = 9ms

C:\>
```

Perform ping operation to enhance the connectivity and it shows that the connection has been established.



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:3EFF:FE22:7776
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.10.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.10.1

C:\>ping 192.16.0.2

Pinging 192.16.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.16.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

The packet send and received information were loaded without any delays.

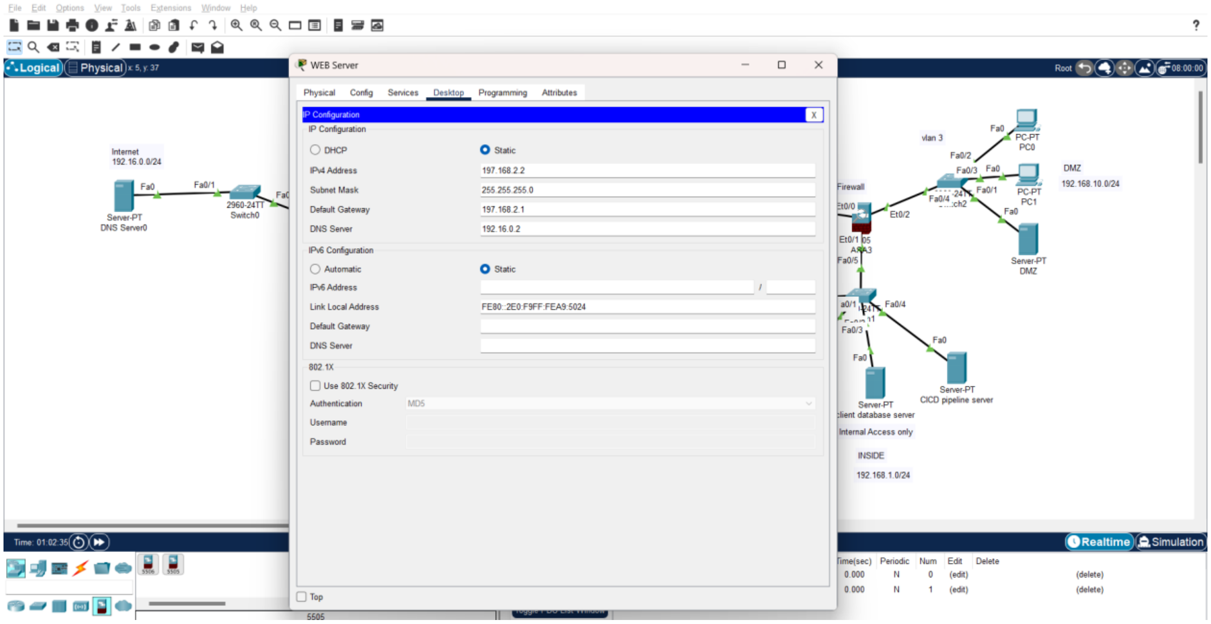


```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Failed	Laptop0	DNS Server0	ICMP	■	0.000	N	0	(edit)	(delete)
●	Successful	Laptop0	DNS Server0	ICMP	■	0.000	N	1	(edit)	(delete)

The packet loss details have been measured and managed with the timed out delay details entitled in it.

Web



WEB Server

IP Configuration

○ DHCP ● Static

IPv4 Address	197.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	197.168.2.1
DNS Server	192.16.0.2

IPv6 Configuration

○ Automatic ● Static

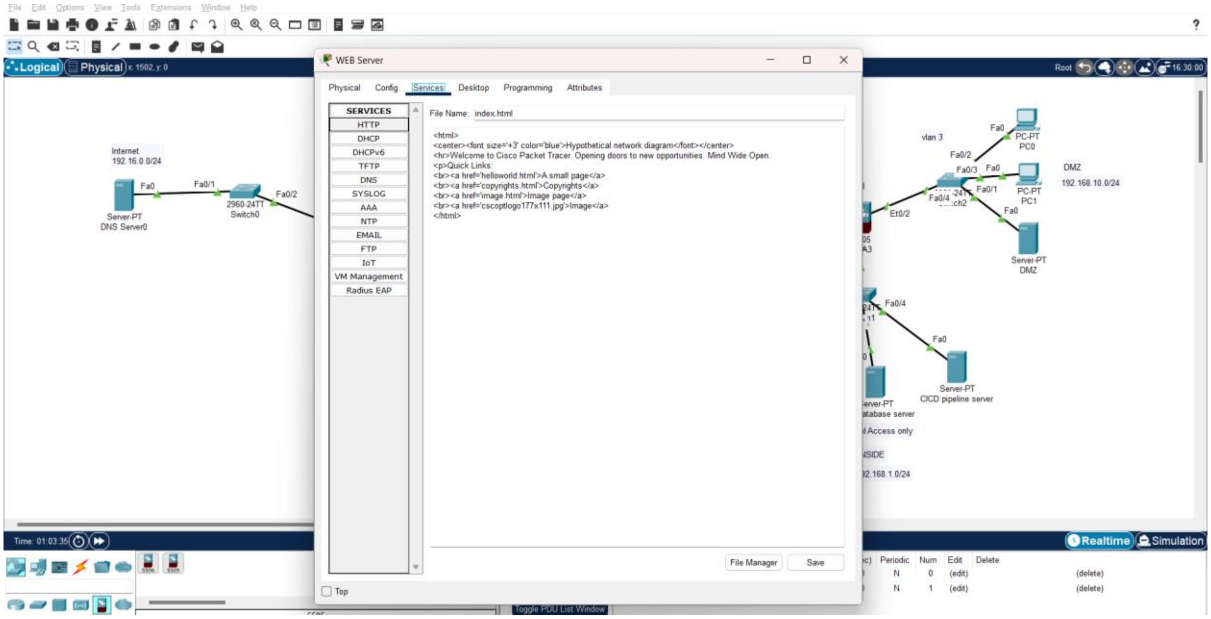
IPv6 Address	/
Link Local Address	FE80::2E0:F9FF:FEA9:5024
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

Choose the desktop in web application column and access to the static web details.

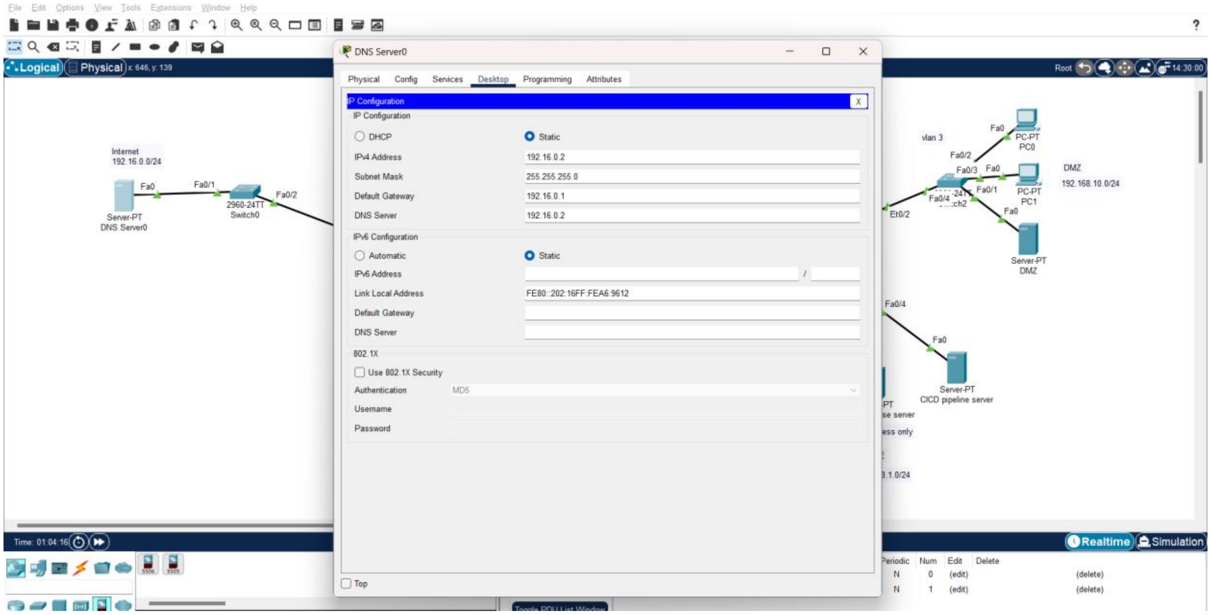


WEB Server

File Name: index.html

```
<html>
<center><font size='+3' color='blue'>Hypothetical network diagram</font></center>
<hr>Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

The HTTP connection were established and selected for loading overall information.



IP Configuration

○ DHCP ● Static

IPv4 Address	192.16.0.2
Subnet Mask	255.255.255.0
Default Gateway	192.16.0.1
DNS Server	192.16.0.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::202:16FF:FEA6:9612
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

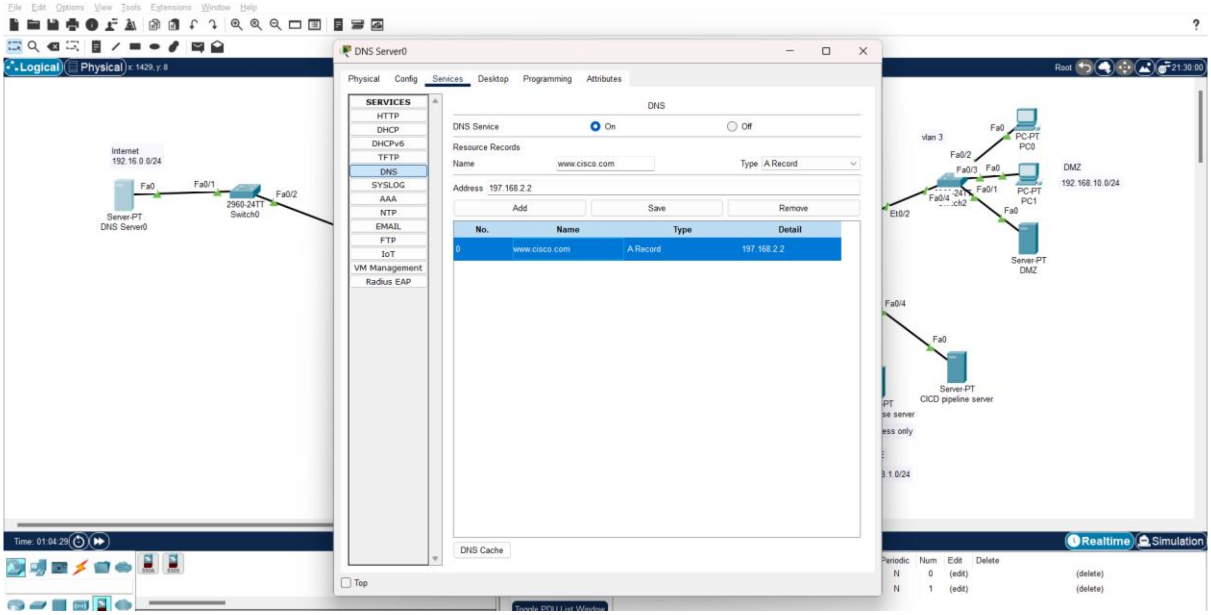
Authentication MD5

Username

Password

□ Top

The static information has been chosen by enabling link local address details.



DNS

DNS Service ● On ○ Off

Resource Records

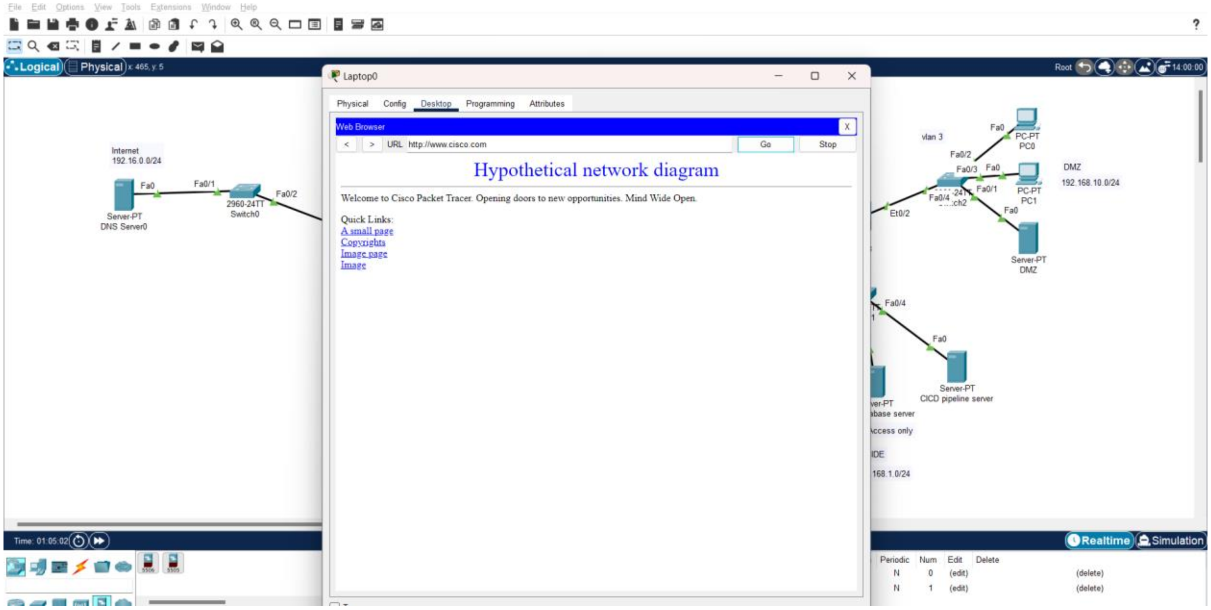
Name www.cisco.com Type A Record

Address 197.168.2.2

No.	Name	Type	Detail
0	www.cisco.com	A Record	197.168.2.2

□ Top

The service page is selected to enable DNS servers.



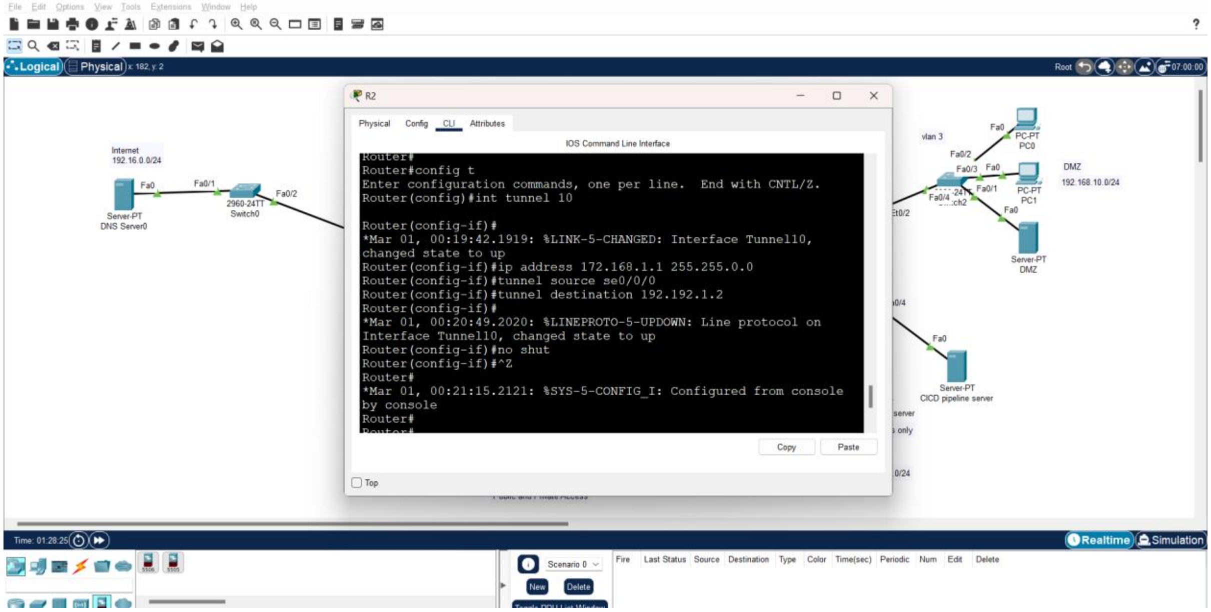
Hypothetical network diagram

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

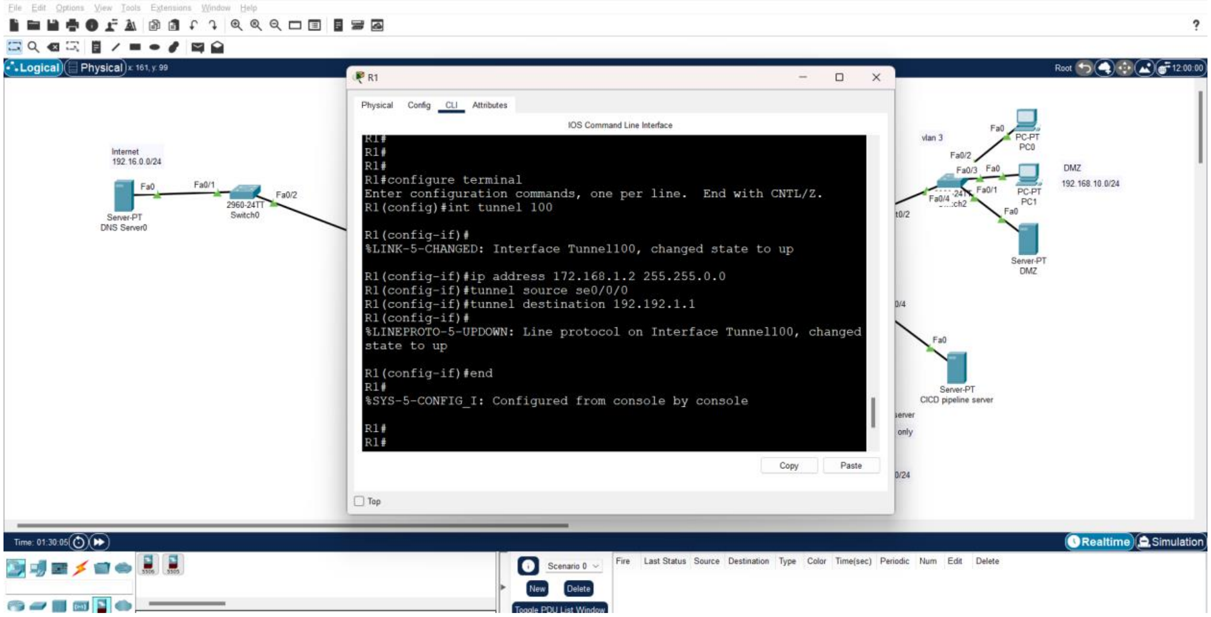
The webpage has been enabled for checking its entire services.

Vpn



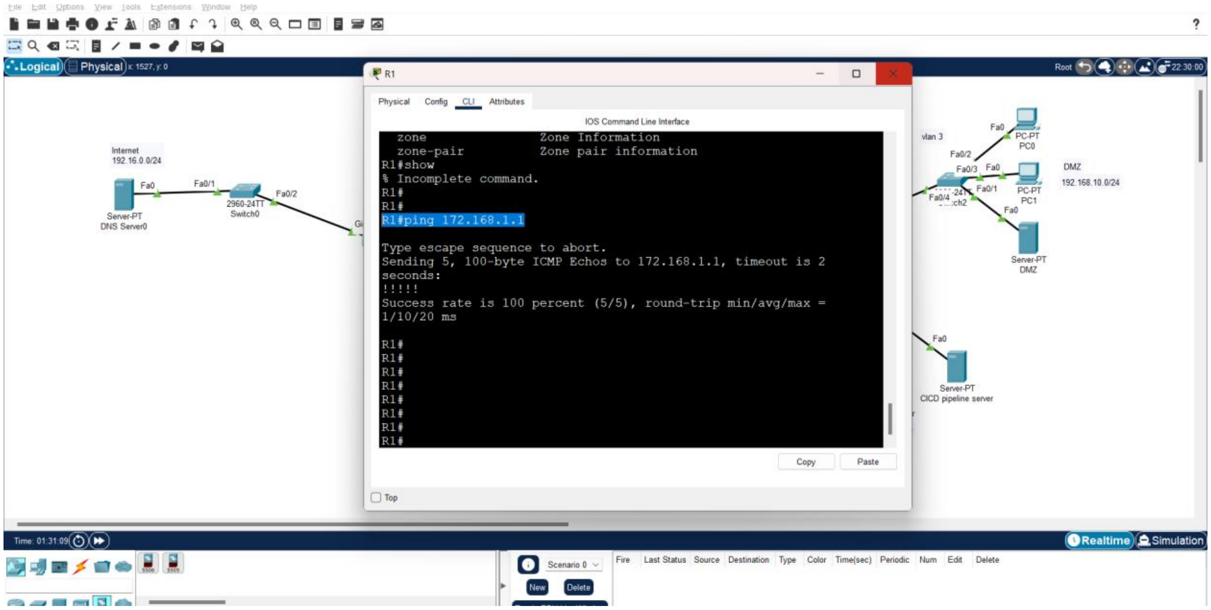
```
Router#
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int tunnel 10

Router(config-if)#
*Mar 01, 00:19:42.1919: %LINK-5-CHANGED: Interface Tunnel10,
changed state to up
Router(config-if)#ip address 172.168.1.1 255.255.0.0
Router(config-if)#tunnel source se0/0/0
Router(config-if)#tunnel destination 192.192.1.2
Router(config-if)#
*Mar 01, 00:20:49.2020: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel10, changed state to up
Router(config-if)#no shut
Router(config-if)#^Z
Router#
*Mar 01, 00:21:15.2121: %SYS-5-CONFIG_I: Configured from console
by console
Router#
Router#
```

The VPN is established and connected with the configuration status without affecting it entirely.



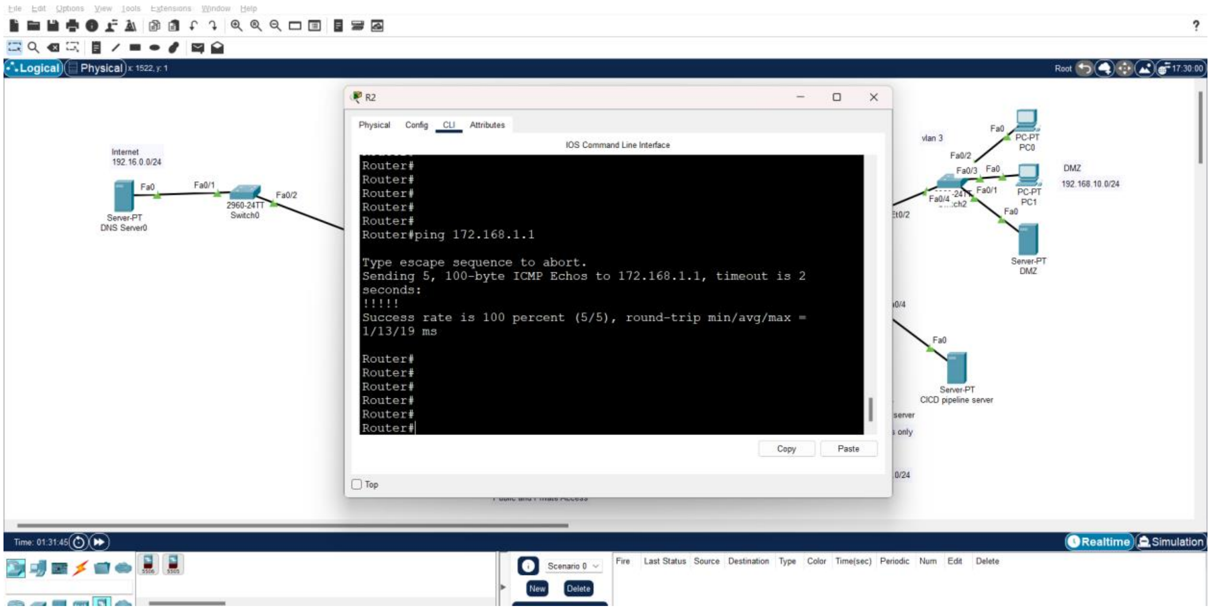
```
R1#
R1#
R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int tunnel 100

R1(config-if)#
%LINK-5-CHANGED: Interface Tunnel100, changed state to up

R1(config-if)#ip address 172.168.1.2 255.255.0.0
R1(config-if)#tunnel source se0/0/0
R1(config-if)#tunnel destination 192.192.1.1
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100, changed
state to up

R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#
```

The web server connectivity has provided and configuration successful on the same console.



```
  zone            Zone Information
  zone-pair       Zone pair information
R1#show
% Incomplete command.
R1#
R1#
R1#ping 172.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.168.1.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/10/20 ms

R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
```

The connectivity are enabled for successful pinging.



```
Router#
Router#
Router#
Router#
Router#
Router#ping 172.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.168.1.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/13/19 ms

Router#
Router#
Router#
Router#
Router#
Router#
```

In overall now the success rate has made without any errors.

Components in DMZ

- The purpose of the web server is to host public facing website and services.
- The mail server is placed to facilitate external communication through mail without having email infrastructure. This will helpful in preventing email borne threats that might impact on internal network [7].
- The DNS servers are used to resolve domain names for external users. This will helpful in safeguarding DNS related attacks for ensuring smooth external access.
- Security servers are used for providing security services such as authentication and access control. This will enhance overall network security for Network Co Inc by performing several security checks.

Table for configuration

Devices	interface	Ip address	Network	Subnet mask
R1	Se0/0/0	192.192.1.2	192.192.1.0/24	255.255.255.0
	Gig0/0	192.16.0.1	192.16.0.0/24	255.255.255.0
R2	Se0/0/0	192.192.1.1	192.192.1.0/24	255.255.255.0

	Gig0/0	197.168.2.2	197.168.2.0/24	255.255.255.0
	Gig0/1	192.192.0.1	192.192.0.0/24	255.255.255.0
ASA	Ethernet0/0	192.192.0.1	192.192.0.0/24	255.255.255.0
	Ethernet0/1	192.168.1.1	192.168.1.0/24	255.255.255.0
	Ethernet0/2	192.168.10.1	192.168.10.0/24	255.255.255.0

Vpn

Devices	Ip address	Network	Subnet mask
R1	172.168.0.1	172.168.0.0/16	255.255.0.0
R2	172.168.0.2	172.168.0.0/16	255.255.0.0

IPS IDS

Devices	Ip address	Network	Subnet mask
Syslog Server	197.168.2.6	197.168.2.0/24	255.255.255.0

TASK5: Additional Security Devices

The security devices incorporated with Network Co Inc for enhancing overall security posture of network.

Intrusion detection system

It is placed in critical data points within internal network between different departments and division. It is to be justified that IDS devices are adopted by monitoring overall network and system activities by detecting unusual behavior and potential security threats [8]. The placement of IDS devices requires comprehensive coverage and allows early detection.

Virtual Private Network Concentrator

The strategic position of VPN in this device is on internal network and accessed over external location. The advantages of VPN placement are to ensure secure and encrypted communication. This strategic placement provides secure access on maintaining control and visibility over remote connection.

Network Access Control System

The deployment of NAC devices acts as an entry point for overall internal network and this will comply with all security policies. It is to be justified that NAC devices supports to streamline endpoint management and to grant overall network access [9].

Intrusion Prevention System

The strategic position of IPS placement is placed between internal network and border between different department. The advantages were including detection and prevention from potential intrusion and proactively defend from threats to compromise network integrity. It will actively block overall malicious traffic against data threats.

TASK6: Security Policies Enhancement

Password Management Policy:

Multifactor Authentication: Enforce MFA for sensitive accounts.

Regular Password Changes: Mandate periodic password updates.

Password Complexity: Specify complex password requirements [10].

Data Classification and Handling Policy:

Data Sensitivity Levels: Classify data (public, internal, confidential).

Encryption Protocols: Enforce encryption for data in transit and at rest.

Remote Access Policy:

VPN Usage: Require VPNs for remote access.

Endpoint Security: Mandate updated antivirus and endpoint protection.

Logging and Monitoring: Implement comprehensive remote access logs.

Network Security Policy:

Firewall Rules: Clearly define and regularly review rules [11].

Intrusion Prevention Measures: Implement automatic threat detection and response.

Bring Your Own Device Policy:

Device Registration: Approve and register personal devices.

Mobile Device Management: Enforce MDM for mobile security.

Employee Training and Awareness Policy:

Regular Training Sessions: Conduct ongoing security training.

Incident Reporting: Clearly define the incident reporting process.

Security Audits: Schedule regular security audits and adapt policies accordingly.

Conclusion

Thus, the report has proposed Network Co. Inc. network security design and implemented robust protection methods for enhancing operational efficiency. The entire network design places all its essential components, integrated with supplementary security devices, etc., for managing all its diverse threats. Through effective security policies, organizations can adopt employee training, improve password management, and protect their data through a resilient framework. Overall, the design focuses on safeguarding all critical assets of the organization and fostering customer trust.

References

[1] M. Z. H. R. Z. C. P. Thapa, "Cybersecurity Research Datasets: Taxonomy and Empirical Analysis," *Tandy School of Computer Science,* pp. 29-89, 2020.

[2] J. Klein, S. Bhulai, M. Hoogendoorn, R. V. D. Mei and R. Hinfelaar, "Detecting Network Intrusion beyond 1999: Applying Machine Learning Techniques to a Partially Labeled Cybersecurity Dataset," *IEEE/WIC/ACM International Conference on Web Intelligence (WI),* vol. 11, pp. 1-9, 2018.

[3] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," *IEEE Access*, pp. 1-9, 2019.

[4] P. Ma, B. Jiang, Z. Lu, N. Li and Z. Jiang, "Cybersecurity named entity recognition using bidirectional long short-term memory with conditional random fields," *Tsinghua Science and Technology,* vol. 2, pp. 1-8, 2020.

[5] K. Maennel, "Learning Analytics Perspective: Evidencing Learning from Digital Datasets in Cybersecurity Exercises," *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* vol. 1, no. 1, pp. 456-478, 2020.

[6] A. H. Lashkari, A. F. A. Kadir, L. Taheri and A. A. Ghorbani, "Toward Developing a Systematic Approach to Generate Benchmark Android Malware Datasets and Classification," *International Carnahan Conference on Security Technology (ICCST),* vol. 2, no. 2, pp. 10-18, 2018.

[7] C. Beazley, K. Gadiya, R. K. U. Rakesh, D. Roden, B. Ye, B. Abraham, D. E. Brown and M. Veeraraghavan, "Exploratory Data Analysis of a Unified Host and Network Dataset," *Systems and Information Engineering Design Symposium (SIEDS),* vol. 1, no. 7, pp. 1-8, 2019.

[8] I. Ullah and Q. H. Mahmoud, "A Technique for Generating a Botnet Dataset for Anomalous Activity Detection in IoT Networks," *IEEE International Conference on Systems, Man, and Cybernetics (SMC),* vol. 1, no. 8, pp. 60-78, 2020.

[9] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima and B. Chen, "A Synthesized Dataset for Cybersecurity Study of IEC 61850 based Substation," *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm),* vol. 7, no. 10, pp. 1-7, 2018.

[10] F. Yi, B. Jiang, L. Wang and J. Wu, "Cybersecurity Named Entity Recognition Using Multi-Modal Ensemble Learning," *IEEE Access,* vol. 6, pp. 1-5, 2020.

[11] D. Gümüşbaş, T. Yıldırım, A. Genovese and F. Scotti, "A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems," *IEEE Systems Journal*, pp. 1-9, 2020.

[12] N. Vakakis, O. Nikolis, D. Ioannidis, K. Votis and D. Tzovaras, "Cybersecurity in SMEs: The Smart-Home/Office Use Case," *IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD),* vol. 9, pp. 1-9, 2019.

[13] P. Ma, B. Jiang, Z. Lu, N. Li and Z. Jiang, "Cybersecurity named entity recognition using bidirectional long short-term memory with conditional random fields," *Tsinghua Science and Technology,* vol. 1, pp. 1-7, 2021.

[14] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence based Network Intrusion Detection with Hyper-Parameter Optimization Tuning," *International Conference on Communication and Signal Processing (ICCSP),* pp. 1-8, 2019.

[15] A. Ju, " Self-Attention-Based Approach for Named Entity Recognition in Cybersecurity," *IEEE,* vol. 4, pp. 1-9, 2020.