

1. Executive Summary

Equinox IT Solutions LTD has been attacked in the past due to weak network security resulting in loss of data, information and reputation. As a network security engineer hired to make a robust network connectivity for the organization, using packet tracer and the best practices to solve the root cause of the breaches. Demonstrating a robust network security to remediate the issues through the connectivity. This report will detail the connections made in the organization in separate areas and how they are integrated in the network and how the routing is done from one area to another area. VLAN and Inter – VLAN is done to separate the accessibility of the networks in their areas. Discussing about the internal network, external network, DMZ network and public network their accessibility in the network to other networks, implementation of the network intrusion prevention system, site-to-site VPN, and the firewall configurations. In the research portion of this report, based on the previous demonstration the best practices and how implementation of VPN and Zero-trust framework are analyzed. This report's result will be to make sure that these breaches in Equinox IT Solutions LTD will not happen again and remediation plans must be applied and updated regularly.

2. Block A: Architecture and Communication

2.1. Configuring IP Connections and Device Hardening

To build the network for Equinox IT Solutions, packet tracer is used to connect the PCs and Servers in different areas to the routers and establish the connections. The entire network is built according to the assignment requirements. Then the end devices are placed in the assigned network areas that are Internal Site Network, External Site Network, DMZ Network and Public Network. Now the goal is to finish the basic configurations of the devices, starting with IP Configurations.

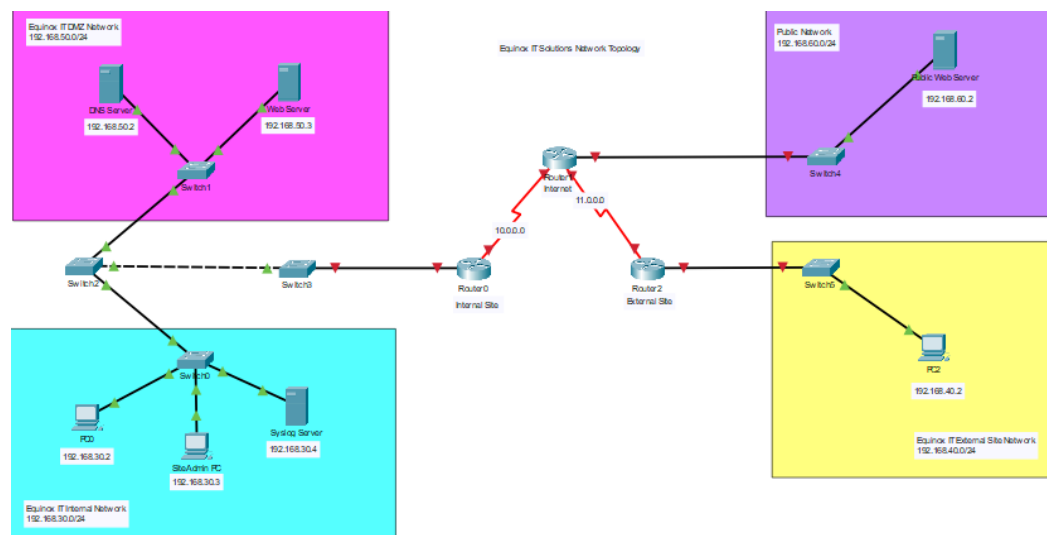
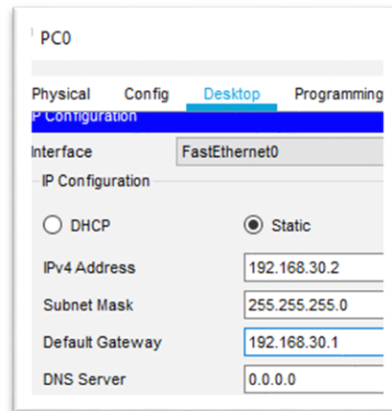


Figure 1: Equinox IT Solutions Network Topology

Above is the connected topology of the Network.

Static IP Configurations for the PCs

Static IP configurations of the devices in this demonstration is done in a simple Method that is through the config menu and then assigning the IP address, Subnet mask and default gateway to the device.

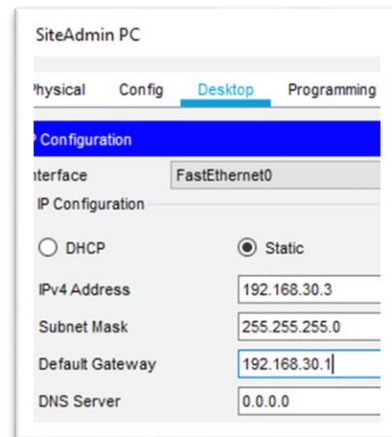


The screenshot shows the configuration window for PC0. The 'Desktop' tab is selected, and the 'Configuration' section is active. The 'Interface' is set to 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with: IPv4 Address: 192.168.30.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.30.1, and DNS Server: 0.0.0.0.

Field	Value
IPv4 Address	192.168.30.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.30.1
DNS Server	0.0.0.0

Figure 2: PC0 IP configuration

PC0 is configured to have IP address of 192.168.30.2 with a subnet mask of 255.255.255.0 and the default gateway as 192.168.30.1



The screenshot shows the configuration window for SiteAdmin PC. The 'Desktop' tab is selected, and the 'Configuration' section is active. The 'Interface' is set to 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with: IPv4 Address: 192.168.30.3, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.30.1, and DNS Server: 0.0.0.0.

Field	Value
IPv4 Address	192.168.30.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.30.1
DNS Server	0.0.0.0

Figure 3: Site admin PC Configuration

Site Admin PC is configured to have IP address of 192.168.30.3 with a subnet mask of 255.255.255.0 and the default gateway as 192.168.30.1

PC2

Physical Config **Desktop** Program

Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.40.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.40.1

DNS Server: 0.0.0.0

Figure 4: PC2 static IP configuration

PC2 is configured to have IP address of 192.168.40.2 with a subnet mask of 255.255.255.0 and the default gateway as 192.168.40.1

Dynamic IP Configuration

For a smaller set up of the network assigning the static IPs might be optimum but it is not the case for large networks. To remediate that dynamic IP configurations, the network administrator will help save time, reduce complications, and duplicate the IPs for access to the network. The commands used here can be used to assign dynamic IPs in router and the DHCP server as well.

Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with (
Switch(config)#ip dhcp excluded-address 192.168.30.1
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.30.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.30.1
Switch(dhcp-config)#dns-server 3.3.3.3
Switch(dhcp-config)#exit
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.30.6 255.255.255.0
Switch(config-if)#no shutdown
```

Figure 5: Switch0 DHCP Configuration

Switch0 is configured through CLI to assign dynamic IP addresses to the devices. An IP DHCP pool is created then the gateway IP '192.168.30.1' is

excluded. The network details are specified with network ID IP as '192.168.30.0' and the subnet mask as '255.255.255.0' and the dns-server as '3.3.3.3.' For system security some IPs are excluded for this pool which can be used for administrative or other purposes. Then vlan 1 is also assigned with an IP.

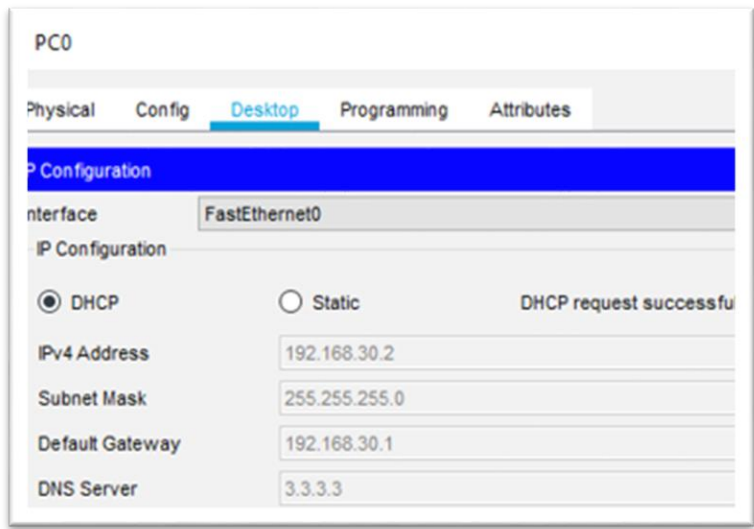


Figure 6: PC0 Dynamic IP

In the above figure, under the desktop tab the IP configurations are verified. By switching to the DHCP option, a request to the DHCP server is sent to obtain an IP address for the device. For PC0 the request is successful and the IP, Subnet mask, Default Gateway and DNS Server details can be verified.

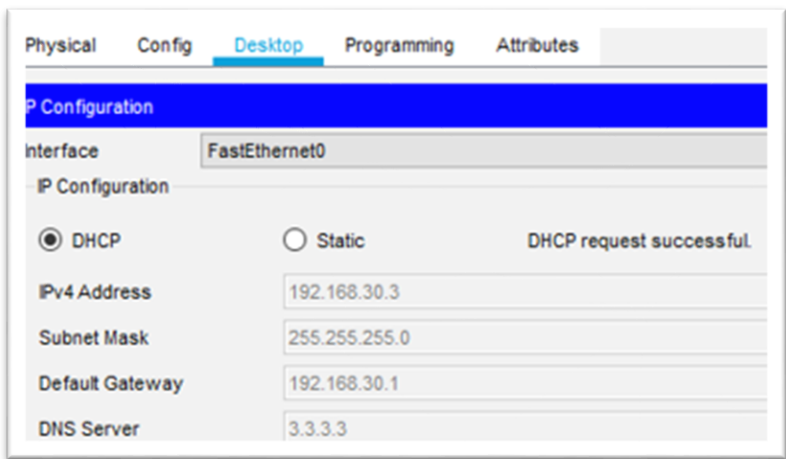


Figure 7: SiteAdmin PC

For SiteAdmin PC the request is successful and the IP, Subnet mask, Default Gateway and DNS Server details can be verified.

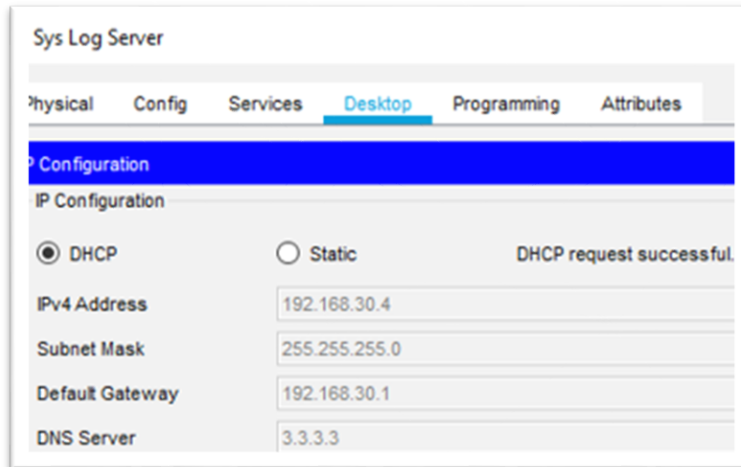


Figure 8: Syslog Server IP

For Syslog Server the request is successful and the IP, Subnet mask, Default Gateway, and DNS Server details can be verified.

```
Switch(config)#ip dhcp excluded-address 192.168.50.1
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.50.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.50.1
Switch(dhcp-config)#dns-server 5.5.5.5
Switch(dhcp-config)#exit
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.50.5 255.255.255.0
Switch(config-if)#no shutdown
```

Figure 9: Switch1 DHCP pool

Switch1 is configured through CLI to assign dynamic IP addresses to the devices. An IP DHCP pool is created then the gateway IP '192.168.50.1'.

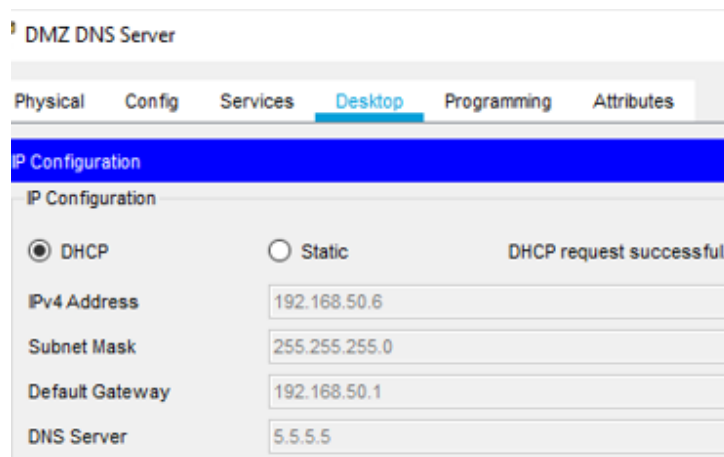


Figure 10: DNS Server

A request to the DHCP server is sent to obtain an IP address for the device. For the DNS Server, the request is successful, details can be verified.

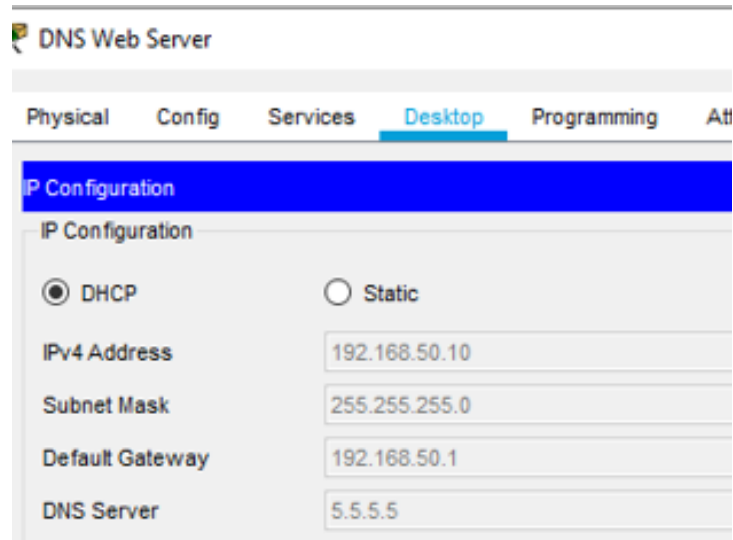


Figure 11: Web Server

In the above figure, under the desktop tab the IP configurations are verified. By switching to the DHCP option, a request to the DHCP server is sent to obtain an IP address for the device. For the Web Server, the request is successful and the IP, Subnet mask, Default Gateway and DNS Server details can be verified.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CN
Switch(config)#ip dhcp excluded-address 192.168.40.1
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.40.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.40.1
Switch(dhcp-config)#dns-server 4.4.4.4
Switch(dhcp-config)#exit
Switch(config)#int vlan1
Switch(config-if)#ip add 192.168.40.5 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan1
Switch(config-if)#no shutdown
```

Figure 12: Switch5 DHCP pool configuration

Switch5 is configured through CLI to assign dynamic IP addresses to the devices. An IP DHCP pool is created then the gateway IP '192.168.40.1' is excluded. The network details are specified with network ID IP as '192.168.40.0' and the subnet mask as '255.255.255.0' and the dns-server as '4.4.4.4.' For system security some IPs are excluded for this pool which can be used for administrative or other purposes.

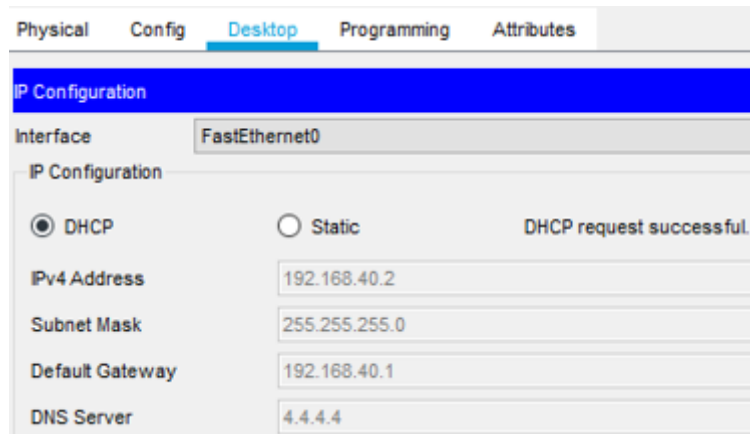


Figure 13: PC2 dynamic IP

In the above figure, under the desktop tab the IP configurations are verified. By switching to the DHCP option, a request to the DHCP server is sent to obtain an IP address for the device. For PC2 the request is successful and the details can be verified.

```
Switch4
-----
Physical  Config  CLI  Attributes

IOS Command Line Interface

Switch(config)#ip dhcp exclude-add 192.168.60.1
^
% Invalid input detected at '^' marker.

Switch(config)#ip dhcp excluded-address 192.168.60.1
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.60.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.60.1
Switch(dhcp-config)#dns-server 6.6.6.6
Switch(dhcp-config)#exit
Switch(config)#int vlan1
Switch(config-if)#ip add 192.168.60.5 255.255.255.0
Switch(config-if)#no shutdown
```

Figure 14: Switch4 DHCP pool configuration

Switch4 is configured through CLI to assign dynamic IP addresses to the devices. An IP DHCP pool is created then the gateway Ip '192.168.60.1' is excluded. The network details are specified with network ID IP as '192.168.60.0' and the subnet mask as '255.255.255.0' and the dns-server as '6.6.6.6.' For system security some IPs are excluded for this pool which can be used for administrative or other purposes.

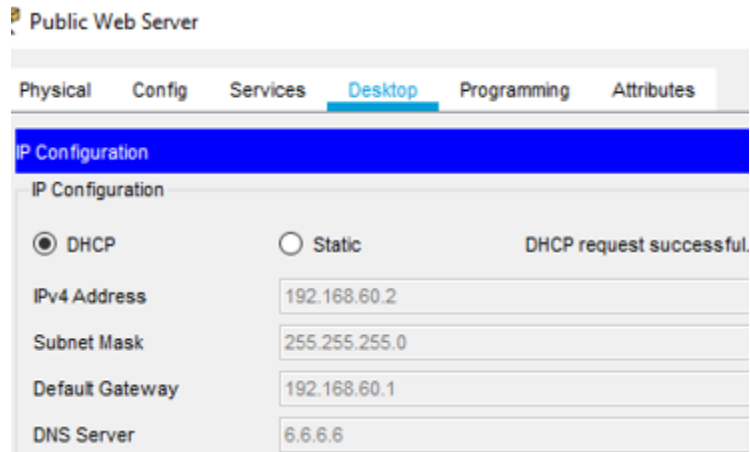


Figure 15: Public Web Server Dynamic IP

In the above figure, under the desktop tab the IP configurations are verified. By switching to the DHCP option, a request to the DHCP server is sent to obtain an IP address for the device. For the Public Web Server, the request is successful and the IP, Subnet mask, Default Gateway and DNS Server details can be verified.

2.2. Configuring servers- DNS, Web, Syslog and Public Servers

Web Server is configured to deliver webpages to any user who accesses the URL request over www, http is used for this task. Basic configurations of the Web Server are done and then HTML code is added to the HTTP option in the Services Tab of the server configuration. By typing the IP address of the Web Server, the configured webpage is verified

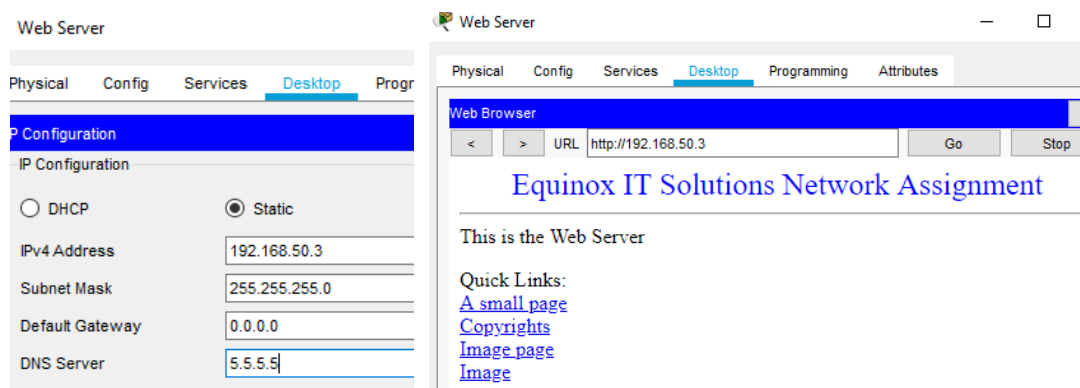


Figure 16: Web Server Configuration

DNS Server is configured for the users to access websites by a name rather than an IP address. Basic configurations of the DNS Server are done, then on the Services tab of the server configuration in the DNS services server 5.5.5.5 is added as the equinox it solutions.

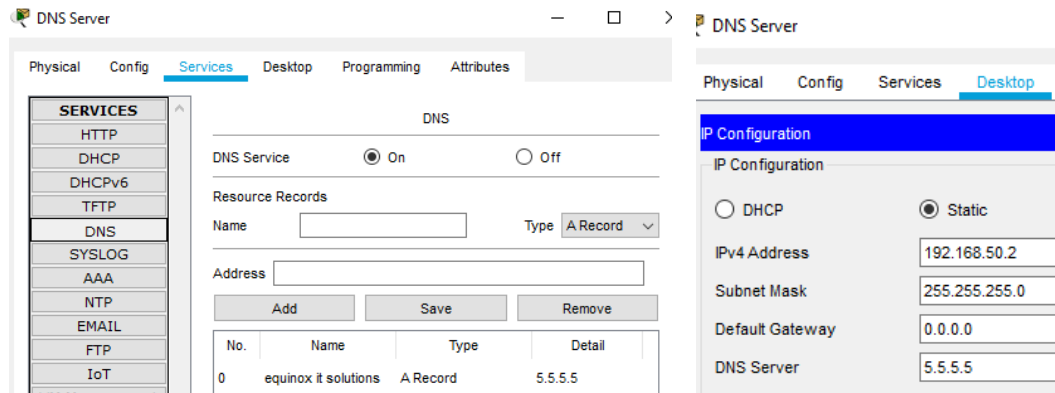


Figure 17: DNS Server

For the Syslog Server, the basic configurations of the server are completed. Then the SYSLOG services are turned on for when there is logging activity in the network.

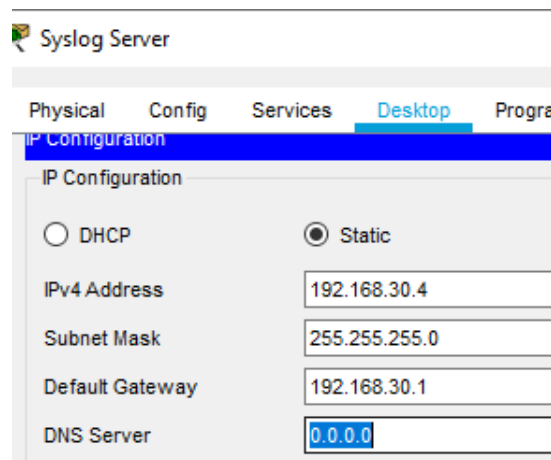


Figure 18: Syslog server

A Public Web Server can be configured like the Web Server configuration method. The difference being that this will be accessed by everyone thus having no confidential material. The webpage created can be accessed by typing in the IP '192.168.60.2.'

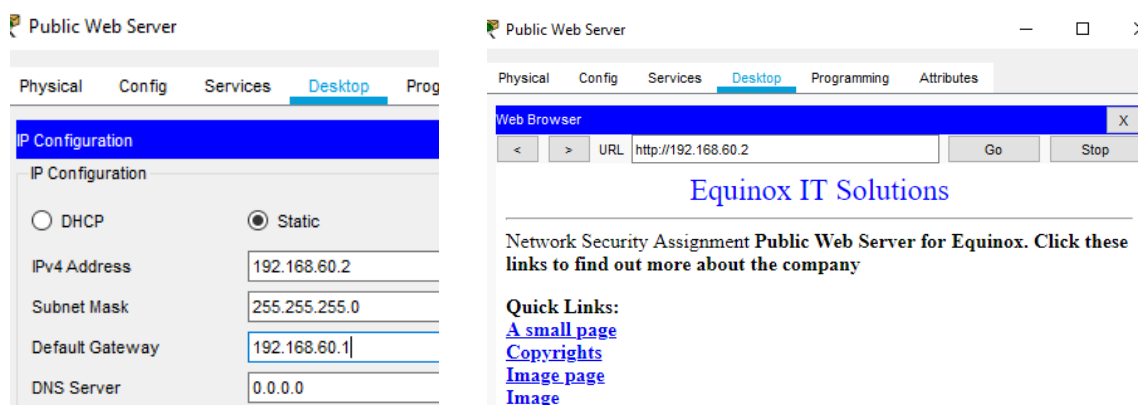


Figure 19: Public Web Server

The necessary configurations are done for the switches, PCs, and servers.

2.3. Dynamic Routing - OSPF Routing

OSPF routing is an internal routing protocol. Routers are first configured, and IPs are assigned. For router0, serial 0 interface is assigned with the IP address '10.0.0.1' and subnet mask '255.0.0.0' in the 10.0.0.0 network. In the same network, Router 1 is connected from serial 0 interface with the IP address '10.0.0.2' and subnet mask '255.0.0.0'. Similarly, in router2 serial 0 interface is assigned with the IP address '11.0.0.1' and subnet mask '255.0.0.0' in the 11.0.0.0 network while Router 1 is connected from serial 1 interface with the IP address '11.0.0.2' and subnet mask '255.0.0.0'.

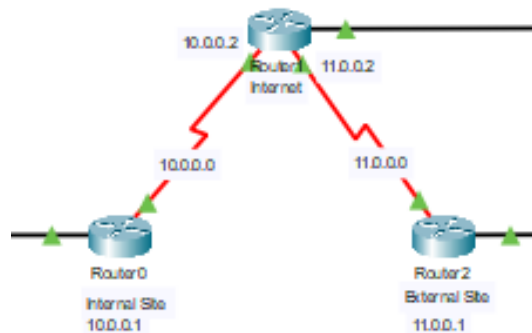
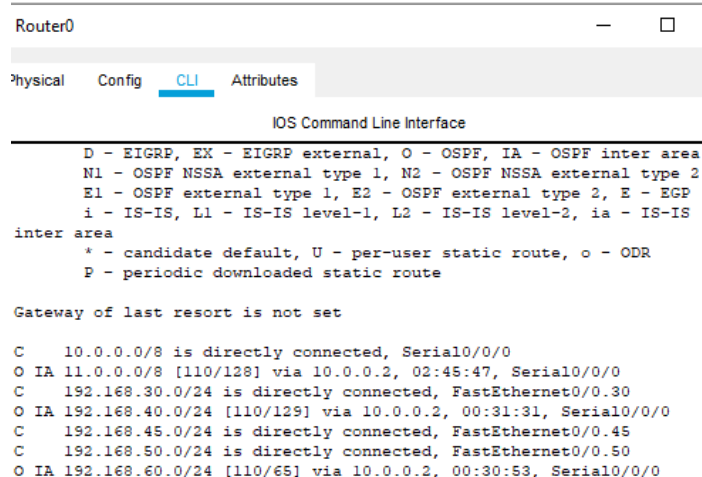


Figure 20: Configuration of the routers

Now that the connection is made, OSPF routing is configured for these three routers. For each router, connected links must be added to the OSPF area. It must be specified that they belong in the same area in each router configuration. For router0, the networks 192.168.30.0/24, 192.168.50.0/24 and 10.0.0.0/8 and the wildcard mask for the networks must be specified to the area 0. This is verified by the 'show run' command (C – connected connection and O - OSPF routing).



```

Router0
-----
Physical  Config  CLI  Attributes

IOS Command Line Interface

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

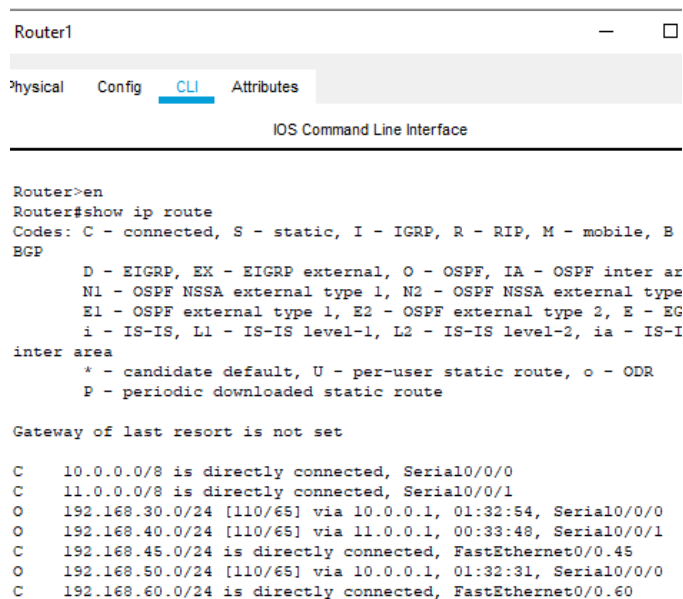
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0/0
O IA 11.0.0.0/8 [110/128] via 10.0.0.2, 02:45:47, Serial0/0/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0.30
O IA 192.168.40.0/24 [110/129] via 10.0.0.2, 00:31:31, Serial0/0/0
C    192.168.45.0/24 is directly connected, FastEthernet0/0.45
C    192.168.50.0/24 is directly connected, FastEthernet0/0.50
O IA 192.168.60.0/24 [110/65] via 10.0.0.2, 00:30:53, Serial0/0/0

```

Figure 21: OSPF Configuration routing for router 0

For router1, the networks 192.168.60.0/24, 10.0.0.0/8, and 11.0.0.0/8 and the wildcard mask for the networks must be specified to the area 0. This is verified by the 'show run' command.



```

Router1
-----
Physical  Config  CLI  Attributes

IOS Command Line Interface

Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
       BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter ar
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EG
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-I
       inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0/0
C    11.0.0.0/8 is directly connected, Serial0/0/1
O    192.168.30.0/24 [110/65] via 10.0.0.1, 01:32:54, Serial0/0/0
O    192.168.40.0/24 [110/65] via 11.0.0.1, 00:33:48, Serial0/0/1
C    192.168.45.0/24 is directly connected, FastEthernet0/0.45
O    192.168.50.0/24 [110/65] via 10.0.0.1, 01:32:31, Serial0/0/0
C    192.168.60.0/24 is directly connected, FastEthernet0/0.60

```

Figure 22: OSPF Configuration for router 1

For router0, the networks 192.168.40.0/24, and 11.0.0.0/8 and the wildcard mask for the networks must be specified to the area 0. This is verified by the 'show run' command

```

Router2
-----
Physical Config CLI Attributes
IOS Command Line Interface
Router#
03:41:26: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID,
from backbone area must be virtual-link but not found from 11.0.0.1,
Serial0/0/0
how ip 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

O IA 10.0.0.0/8 [110/128] via 11.0.0.2, 02:49:52, Serial0/0/0
C 11.0.0.0/8 is directly connected, Serial0/0/0
O IA 192.168.30.0/24 [110/129] via 11.0.0.2, 01:34:42, Serial0/0/0
C 192.168.40.0/24 is directly connected, FastEthernet0/0.40
C 192.168.45.0/24 is directly connected, FastEthernet0/0.45
O IA 192.168.50.0/24 [110/129] via 11.0.0.2, 01:34:19, Serial0/0/0
O IA 192.168.60.0/24 [110/65] via 11.0.0.2, 00:34:58, Serial0/0/0

```

Figure 23: OSPF Configuration routing for router 2

OSPF routing can be observed for each router since they are in the same area the routers are aware to send packets to those devices through the other router.

2.4. VLAN Trunking

VLAN Trunking is one of the best practices to isolate the network in the organization so that only authorized devices can gain access to information and are limited as per requirements and policies. The VLANs are created by assigning a number for the VLAN and a name. Additionally, a native VLAN 45 is created for trunking connections and default VLAN 1 is used for other purposes.

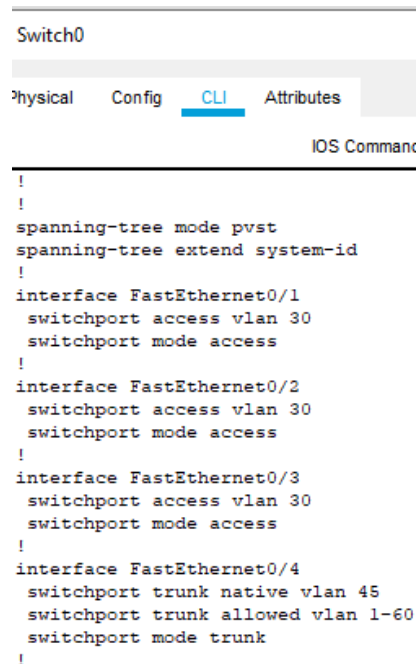
```

Switch(vlan)#vlan 60 name PublicNetwork
VLAN 60 modified:
      Name: PublicNetwork
Switch(vlan)#vlan 30 name InternalNetwork
VLAN 30 modified:
      Name: InternalNetwork
Switch(vlan)#vlan 40 name ExternalNetwork
VLAN 40 modified:
      Name: ExternalNetwork
Switch(vlan)#vlan 50 name DMZNetwork
VLAN 50 modified:
      Name: DMZNetwork
Switch(vlan)#

```

Figure 24: VLAN name

Switch0 is connected to PCs and server by an access point connection. These interfaces Fa0/1, Fa0/2 and Fa0/3 are configured to gain access to VLAN 30 through switchport. But for connecting switches trunk port is configured through which VLAN 1-60 can be allowed for transmitting traffic.



Switch0

Physical Config **CLI** Attributes

IOS Command

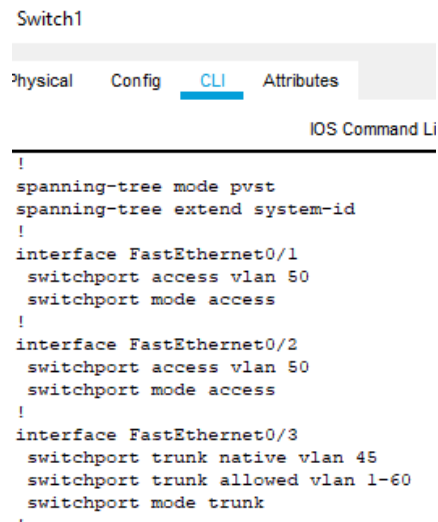
```

!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
!

```

Figure 25: Switch 0

Switch1 is connected to servers by an access point connection. These interfaces Fa0/1, and Fa0/2 are configured to gain access to VLAN 40 through switchport. Interface FA0/3 is made as trunk port.



Switch1

Physical Config **CLI** Attributes

IOS Command Li

```

!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
!

```

Figure 26: Switch 1

Switch2 is connected to three switches by a trunk point connection. These interfaces Fa0/1, Fa0/2 and Fa0/3 are configured to allow VLAN from 1-60 and have the native VLAN as 45.

Switch2

Physical Config CLI Attributes

IOS Command

```

!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/3
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
 switchport nonegotiate

```

Figure 27: Switch 2

Switch3 is connected to Switch0 and router0 by a trunk point connection. These interfaces Fa0/1, and Fa0/2 are configured to allow traffic from VLAN 1-60.

Switch3

Physical Config CLI Attributes

IOS Command

```

!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
!
interface FastEthernet0/3
!

```

Figure 28: Switch 3

Switch4 is connected to PC and router1 by an access point and a trunk point connection. Fa0/1 connection is made by the access point and assigned VLAN number, and Fa0/2 is configured to allow traffic from VLAN 1-60.

Switch4

Physical Config CLI Attributes

IOS Command

```

!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/2
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
 switchport nonegotiate

```

Figure 29: Switch 4

Switch5 is connected to PC2 and router2 by an access point and a trunk point connection. Fa0/1 connection is made by the access point to VLAN 40 and assigned VLAN number, and Fa0/2 is configured to allow traffic from VLAN 1-60.

Switch5

Physical Config CLI Attributes

IOS Command

```

!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/2
 switchport trunk native vlan 45
 switchport trunk allowed vlan 1-60
 switchport mode trunk
 switchport nonegotiate

```

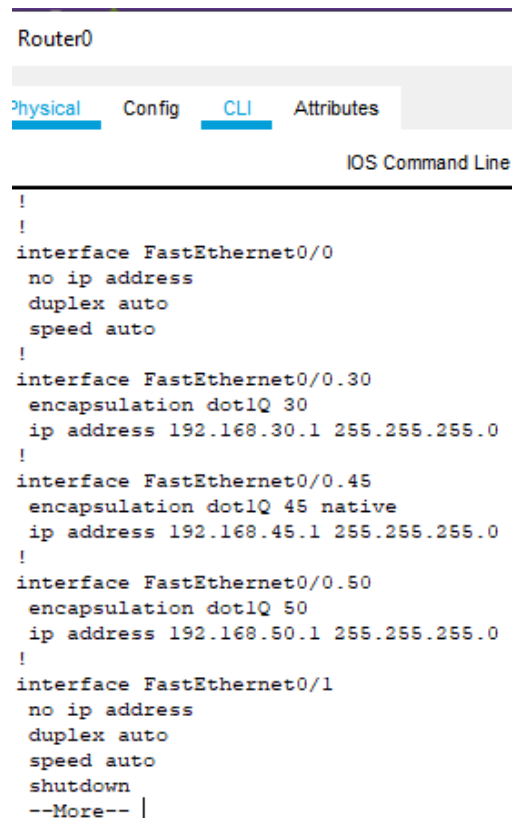
Figure 30: Switch 5

Successfully the VLANs are created, assigned, and connected by either an access connection or trunk connection.

2.5. Inter-VLAN routing using 802.1Q encapsulation

802.1Q encapsulation is used for inter-VLAN routing by creating sub interfaces for the networks with different IPs connected by the same interface in the router.

Configuration the sub interfaces Fa0/0.30 and Fa0/0.50 for the networks 192.168.30.0/24 and 192.168.50.0/24.

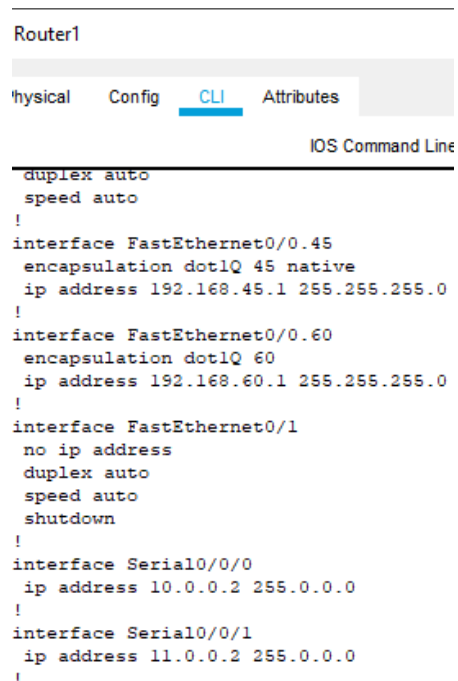


The screenshot shows the CLI of Router0. The 'CLI' tab is selected. The configuration includes:

```
Router0
!
!
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet0/0.30
  encapsulation dot1Q 30
  ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet0/0.45
  encapsulation dot1Q 45 native
  ip address 192.168.45.1 255.255.255.0
!
interface FastEthernet0/0.50
  encapsulation dot1Q 50
  ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
--More-- |
```

Figure 31: router0 Inter - VLAN

Configuring the sub interfaces Fa0/0.60 for the network 192.168.60.0/24.



The screenshot shows the CLI of Router1. The 'CLI' tab is selected. The configuration includes:

```
Router1
!
!
duplex auto
speed auto
!
interface FastEthernet0/0.45
  encapsulation dot1Q 45 native
  ip address 192.168.45.1 255.255.255.0
!
interface FastEthernet0/0.60
  encapsulation dot1Q 60
  ip address 192.168.60.1 255.255.255.0
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface Serial0/0/0
  ip address 10.0.0.2 255.0.0.0
!
interface Serial0/0/1
  ip address 11.0.0.2 255.0.0.0
!
```


Figure 32: Router1

Configuring the sub interfaces Fa0/0.40 for the network 192.168.40.0/24.

Router2

Physical Config CLI Attributes

IOS Command Line

```
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
!
interface FastEthernet0/0.45
encapsulation dot1Q 45 native
ip address 192.168.45.1 255.255.255.0
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 11.0.0.1 255.0.0.0
clock rate 2000000
!
```

Figure 33: Router2

Efficient connections of 802.1Q encapsulation for Inter – VLAN routing to the routers have been made.

Running Simple ICMP packets to ping the devices throughout the network to verify all the connections in different areas.

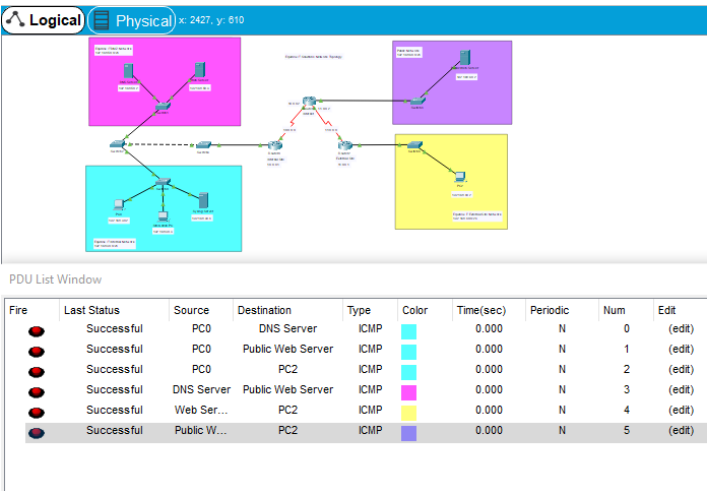


Figure 34: Successful Connection of the entire network

3. Block B: Secure Operations and Service Delivery

3.1. Implement ACL on Routing device

Standard Access Lists are created as this is a small network. Access Lists are configured as a method to either permit access or deny access for certain IPs or the entire network. The configuration is based on certain assumptions about the network. 192.168.30.0/24 Network is the internal network of the organization therefore the network can access all the devices, but no other network can access the Internal network. 192.168.40.0/24 Network is the external network of the organization often used by guests therefore the network has limited access, only Public Network is permitted to use. 192.168.50.0/24 Network is the DMZ network of the organization often used by employees therefore the network cannot access the internal network (SiteAdmin PC), only Public Network and External Network is permitted to use. 192.168.60.0/24 Network is the public network of the organization often used by guests therefore the network has no limited access, in case a hacker can get into the network then they may escalate the privileges and gain the administrative access for the network.

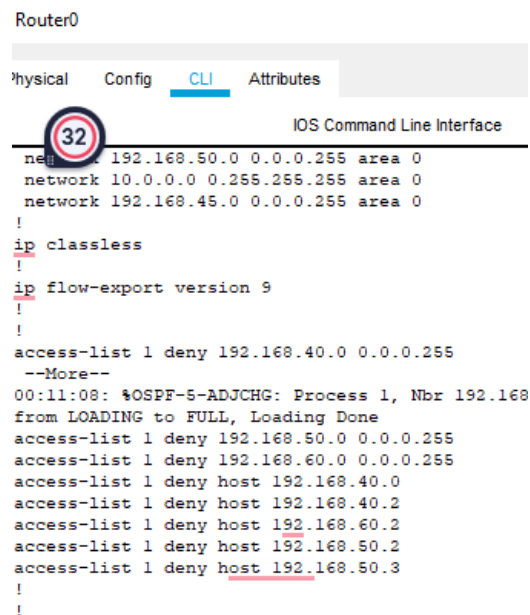
The image is a screenshot of a network router's command-line interface (CLI). At the top, it says 'Router0'. Below that, there are tabs for 'Physical', 'Config', 'CLI' (which is selected and highlighted in blue), and 'Attributes'. A red circle with the number '32' is overlaid on the 'CLI' tab. The main area shows the 'IOS Command Line Interface' with a list of configuration commands. The commands include: 'network 192.168.50.0 0.0.0.255 area 0', 'network 10.0.0.0 0.255.255.255 area 0', 'network 192.168.45.0 0.0.0.255 area 0', '!', 'ip classless', '!', 'ip flow-export version 9', '!', 'access-list 1 deny 192.168.40.0 0.0.0.255', '--More--', '00:11:08: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.0 from LOADING to FULL, Loading Done', 'access-list 1 deny 192.168.50.0 0.0.0.255', 'access-list 1 deny 192.168.60.0 0.0.0.255', 'access-list 1 deny host 192.168.40.0', 'access-list 1 deny host 192.168.40.2', 'access-list 1 deny host 192.168.60.2', 'access-list 1 deny host 192.168.50.2', 'access-list 1 deny host 192.168.50.3', '!', and '!'.

Figure 35: Access List configuration on Router0

```

Router2
Physical Config CLI Attributes
21 IOS Command Line Interface
log-adjacency-changes
network 192.168.40.0 0.0.0.255 area 1
network 11.0.0.0 0.0.0.255 area 1
!
router ospf 1
log-adjacency-changes
network 192.168.40.0 0.0.0.255 area 0
network 11.0.0.0 0.255.255.255 area 0
network 192.168.45.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 2 deny 192.168.60.0 0.0.0.255
access-list 2 permit any
!

```

Figure 36: Access List configuration on Router 2

Verification of the Access List configuration. Internal Network Access to the other networks.

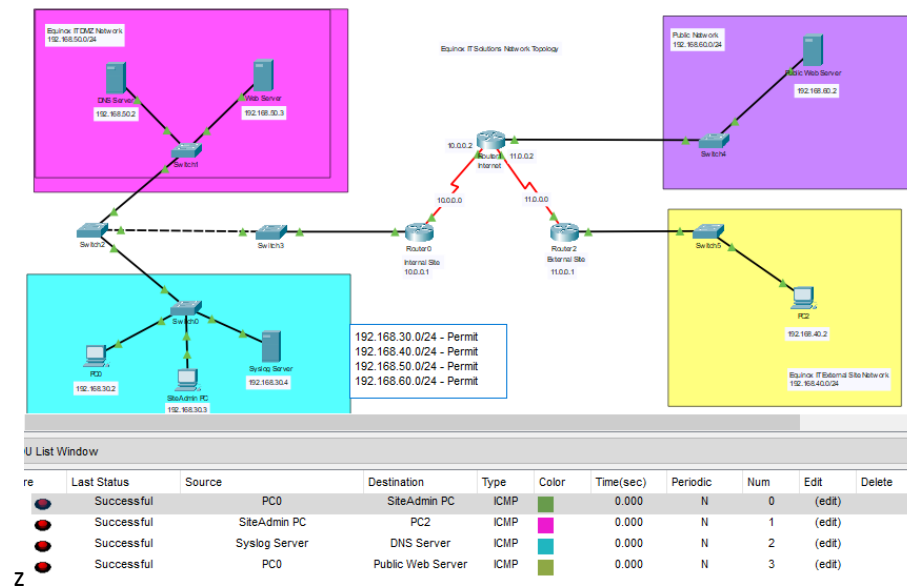


Figure 37: Devices in 192.168.30.0 Network

External Network Access to the other networks. As verified this network connects to itself and public Network

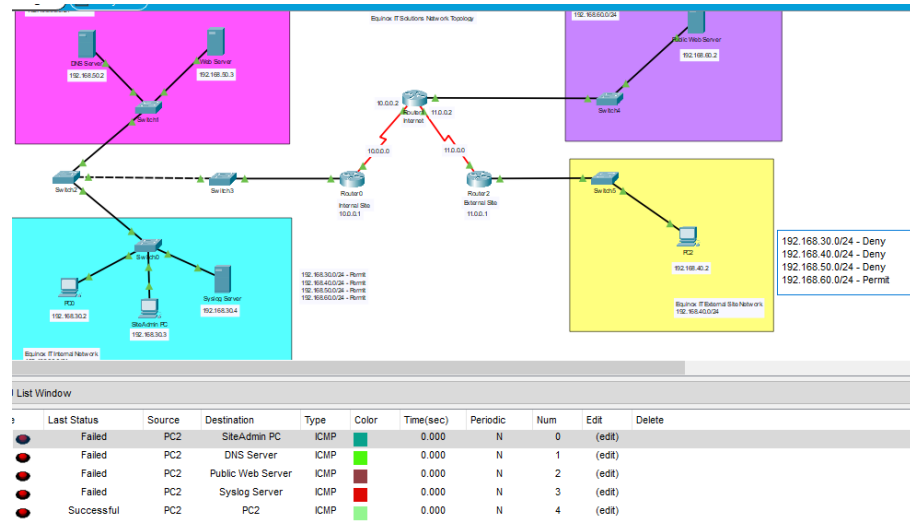


Figure 38: Devices in 192.168.40.0 Network

Verification of the Access List configuration. DMZ Network Access to the other networks excluding the internal network.

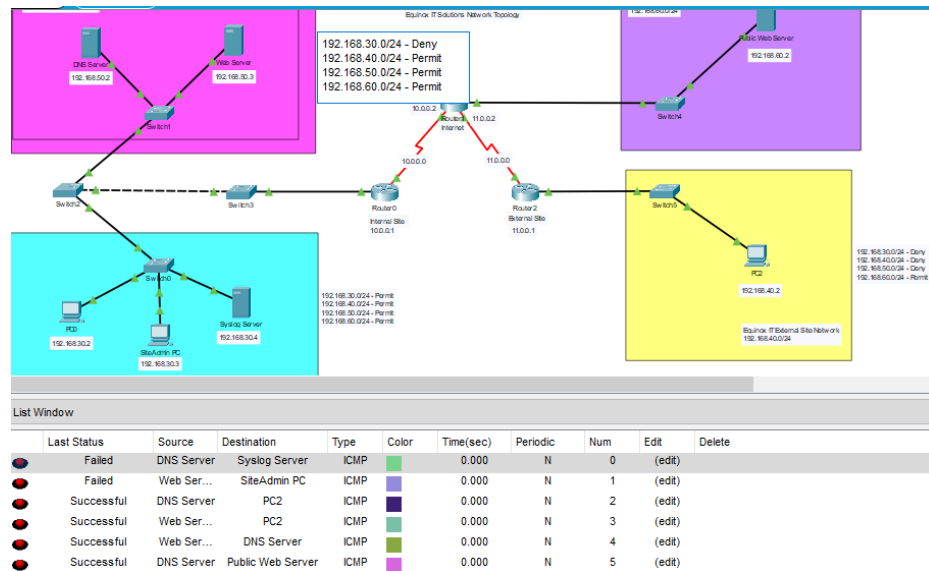


Figure 39: Devices in 192.168.50.0 Network

Verification of the Access List configuration. Public Network is denied having any connection to the other networks.

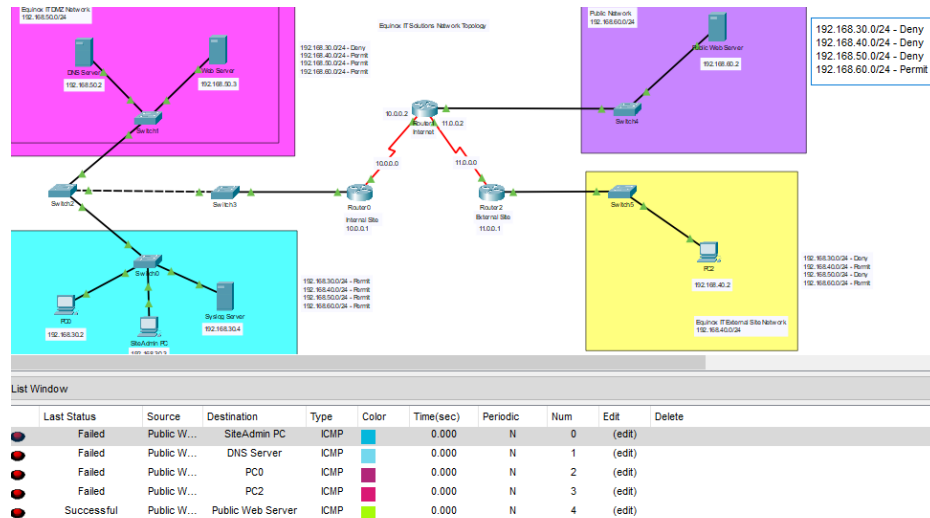


Figure 40: Devices in 192.168.60.0 Network

Access Lists are successfully implemented as per a few probable scenarios in this network.

3.2. Implement Site-To-Site IPsec VPN (Virtual Private Network)

Activating the license of the router for security. Creating ACL for both the routers and enabling the isakmp policy and configuring the options for the policy. Then crypto ipsec is configured with aes-256 and sha encryption then the crypto map is created. Once the map is ready it is applied to the interface of the serial connection. Once the commands are configured on both router0 and router2 then the Site-to-Site VPN is established.

```
Router0
physical Config CLI Attributes
IOS Command Line Interface

interface: Serial0/0/0
Crypto map tag: IPSEC-MAP, local addr 10.0.0.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.30.0/255.255.0.0/0)
remote ident (addr/mask/prot/port):
(192.168.40.0/255.255.0.0/0)
current_peer 11.0.0.1 port 500
ISAKMP: flags=[origin_is_acl,]
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.0.0.1, remote crypto endpt.: 11.0.0.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x66BF745 (1723919845)

inbound esp sas:
spi: 0xB961239C (3110151068)
```

Figure 41: Router0 – Crypto map

In the above figure, there crypto map can be identified, and other options are displayed but the main focus is the number of packets that are encrypted and decrypted from router0 to router2.

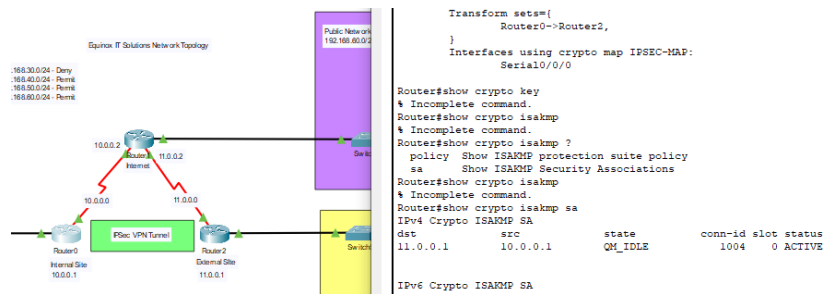


Figure 42: Router 0 – crypto ipsec

The show options for router 0 is crypto ipsec and crypto isakmp.

```

Router2
----- [
Physical Config CLI Attributes
IOS Command Line Interface

interface: Serial0/0/0
Crypto map tag: IPSEC-MAP, local addr 11.0.0.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.40.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.30.0/255.255.255.0/0/0)
current_peer 10.0.0.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 11.0.0.1, remote crypto endpt.:10.0.0.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0xB961239C(3110151068)

inbound esp sas:
spi: 0x66BF6745(1723819845)

```

Figure 43: Router 2 – show crypto map

The crypto map created on router2 includes the encrypted and decrypted files.

```

Router2
----- [
Physical Config CLI Attributes
IOS Command Line Interface

Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
10.0.0.1 11.0.0.1 QM_IDLE 1037 0 ACTIVE

IPv6 Crypto ISAKMP SA

Router#show crypto map
Crypto Map IPSEC-MAP 10 ipsec-isakmp
Peer = 10.0.0.1
Extended IP access list 100
access-list 100 permit ip 192.168.40.0 0.0.0.255
192.168.30.0 0.0.0.255
access-list 100 permit ip 192.168.40.0 0.0.0.255
192.168.50.0 0.0.0.255
Current peer: 10.0.0.1
Security association lifetime: 4608000 kilobytes/86400
seconds
PFS (Y/N): Y
Transform sets={
  Router2->Router0,
}

```

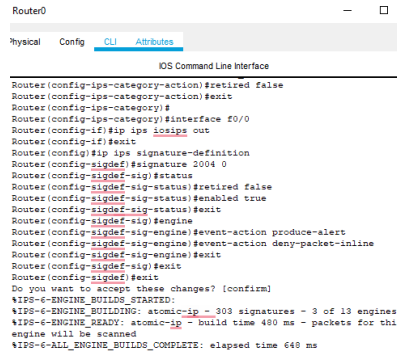
Figure 44: Router2 - Crypto ISAKMP and Crypto map

The above shows the isakmp and crypto map.

The Site-to-Site IPsec VPN is created and configured successfully, and it is verified in the above figures.

3.3. Network IOS IPS implementation and testing

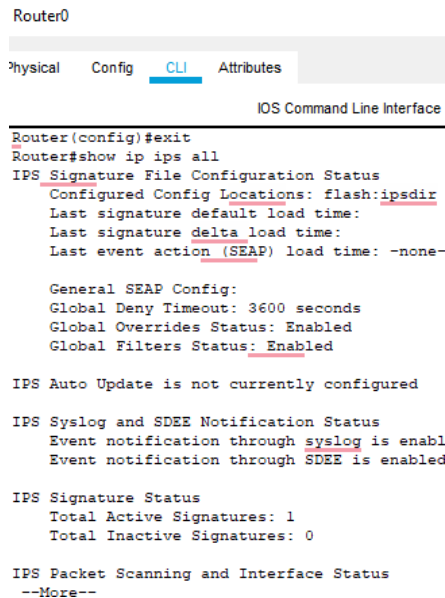
Intrusion Prevention System is used to scan the traffic and. First to enable the IOS IPS on the router0 to config the IPs and assign to a location that is safe and the name is changed to iOS ips and further the signatures are changed from default settings by 'retired false' command. This iOS ips is assigned to the interface. Then the logging is enabled so the traffic is logged on to the SYSLOG server. The signature and sub-signal idea are altered for notifying any alerts.



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#
Router(config-ips-category)#interface Z0/0
Router(config-if)#ip ips iosips out
Router(config-if)#exit
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig-engine)#
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef-sig)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILD_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this
engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 640 ms
```

Figure 45: IOS IPS Configurations

The IPS status and configurations are verified in the below figure.



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#exit
Router#show ip ips all
IPS Signature File Configuration Status
  Configured Config Locations: flash:ipsdir
  Last signature default load time:
  Last signature delta load time:
  Last event action (SEAP) load time: -none-

General SEAP Config:
  Global Deny Timeout: 3600 seconds
  Global Overrides Status: Enabled
  Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
  Event notification through syslog is enabl
  Event notification through SDEE is enabled

IPS Signature Status
  Total Active Signatures: 1
  Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
--More--
```

Figure 46: Logging of the activity from IPS is verified on the SYSLOG Server in the below figure.

Syslog			
Service			
	Time	Hostname	Message
9	03.01.1993 12:05:55.466 AM	192.168.30.1	00:05:55: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.60.1 on Serial0/0/...
10	03.01.1993 12:06:04.390 AM	192.168.30.1	%IPS-6-ENGINE_BUILDS_STARTED: 00:06:04 UTC Mar 01 1993
22	03.01.1993 12:07:17.694 AM	192.168.30.1	%SYS-5-CONFIG-I: Configured from console by console
23	03.01.1993 12:07:17.694 AM	192.168.30.1	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.30.4 port 514 started - CLI initiated
24	03.01.1993 12:07:25.547 AM	192.168.30.1	00:07:25: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.60.1 on Serial0/0/...

Figure 47: The IOS IPS was successfully created, and it is verified by the SYSLOG Server.

3.4. Firewall configurations

Firewall is created to

The Web server firewall services are used to configure the Firewall actions. Except the internal network 192.168.30.0/24, the other networks are not permitted access to the DMZ Network.

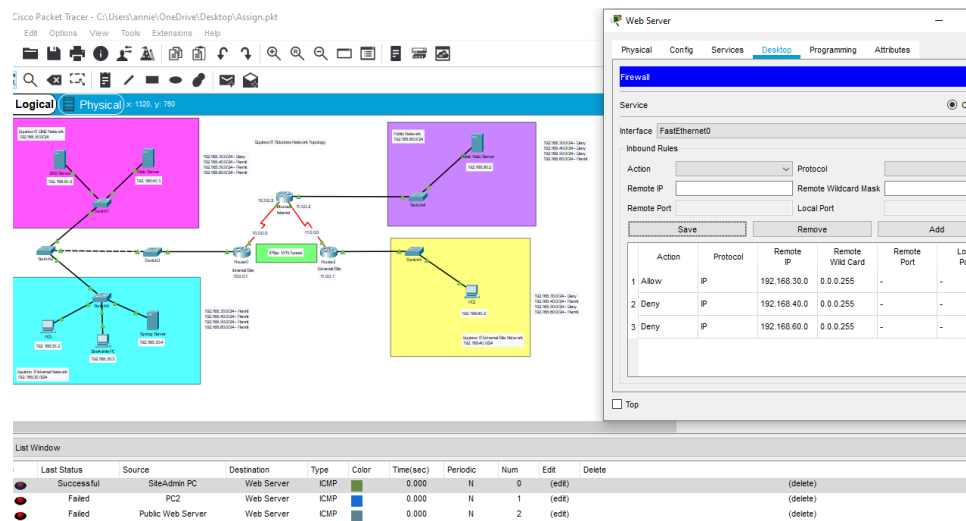


Figure 48: Firewall Configuration on the Web Server

The webpage of the server is accessed on the networks. In the network 192.168.30.0/24 the SiteAdmin PC can access the webpage with the IP '192.168.50.3' whereas the PC2 from the External Network cannot access this webpage showing 'Request Timeout' error.

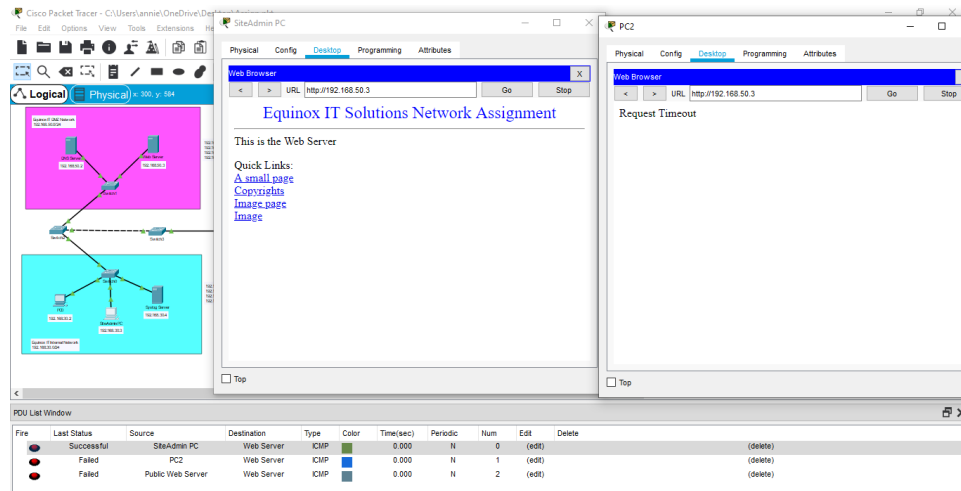


Figure 49: Verification of the Firewall

Successful configuration of the firewall in the webserver and above the verification is displayed.

4. Research & Development

4.1. Zero Trust Network Security Framework

A network security framework known as "Zero Trust" mandates that everyone within or beyond the organization's network, must first be verified, approved, and continually checked for security configuration and posture before connectivity to applications or information is provided or maintained. The zero-trust framework that is followed by organizations is NIST 800-207. These are the most complete, vendor-neutral standards available for governmental agencies and for any company only for governmental agencies, as well as any organization, these are the most complete, distributor standards available. For something like a cloud-first, work-from-home strategy that most businesses must use, NIST standards guarantee compliance and security against contemporary assaults.

The organization would be at hazardous threats from fraudulent employees as well as genuine qualifications stolen by threat hackers, enabling unauthorized & affected transactions direct connections when in the network, under the standard method, which implicitly trusted users and end devices inside that organization's boundary. Businesses must safeguard an infrastructure deployment methodology that is: Uncontrolled endpoints, multiple identities, many cloud-applications, and software-as-a-service applications.

The steps for putting into practice a developed Zero-Security framework are as follows:

- i. Planning: Tailor the policy and best practices according to the laws, regulations and standards.
- ii. Remediation: Detect and stop threats as they breach and prepare laws to fortify the business plan.

- iii. Upgrade: Research further accordingly to improve the standards and user experience for the customers and employees.

According to the case study above of the implementation of a network configuration of Equinox IT Solutions. Only authorized end devices in that area network can access the organization's networks. In the access list configurations, the internal network could access the entire network, but no other network could access the internal network in the organization. External networks and any user connected to them could only access the public Network but not the DMZ Network and Internal Network. Implementing a zero-trust model and limiting access only to authorized users connected to the authorized and highly secured network. DMZ Network could connect to all networks except the internal network of the organization. Then there is the public network, which cannot access any other network. In case there is an intrusion in the public network then it is isolated in the network and cannot access any confidential information that is harmful to the organization. Through injections or privilege escalation, it is possible that a hacker can gain access which is the best reason not to provide access to any other network as the employees sometimes don't follow the rules and best practices to protect their credentials.

4.2. Overview of VPN reliability

Through a wireless site, such as the Internet, a virtual private network (VPN) creates a link to a private network. Most people think of it as a type of tunneling. VPNs come in a variety of forms. Two protocols are frequently connected using VPNs. However, web server VPNs are what the users want to examine. A very common method for giving outside devices access to a organization's network is client-access VPNs. In this regard, IPSec VPNs and SSL VPNs are now the two most widely used technologies.

In the case study of Part A and B. The site-to-site VPN joins several different networks, including an organization's network and internal office network, in contrast to a wireless monitoring VPN, which links end devices or employees to a company's internal network. Site-to-site VPNs are a popular choice among businesses because they enable private internet protocol label switching (MPLS) circuits to be replaced by internet connections for private traffic. Organizations with several branches in various regions that require continuous access to, and usage of the organization's network commonly employ site-to-site VPNs. A corporation may safely link Equinox's network with its remote offices using a site-to-site VPN so that they can interact and share resources as one network.

However, being widely used, wireless access VPN and site-to-site VPN each have vulnerabilities, principally as a result of the security monitoring model's limits in terms of offering all-encompassing safety. The growing use of cloud-based infrastructure and apps, such as those for cybersecurity, combined with a growth in the number of remote workers makes boundary-based cybersecurity solutions challenging to use and more ineffective when used alone. To guarantee that devices connected to the company's network from outside of the

organizational perimeter - and the data traveling between the devices and the network - remain safe, organizations must go beyond VPN features.

The foundation of Internet Protocol Security (IPSec) VPN technology is the establishment of an authorized connection linking systems or individuals. Through tunneling, encryption, and authentication, it achieves these objectives, but it also gives businesses the option of choosing the precise security measures that are best for them. At the network layer, this group of standards provides security for IP communications. The initial purpose of IPSec VPN technology was to safeguard data transmission over the Internet between trustworthy, internal networks. Later, IPSec solutions were expanded to safeguard information sent between mobile employees getting remote access to an organization's internal network more effectively than traditional dial-in techniques. An IT department must install and maintain unique VPN clients on each PC from which a user wants to access in order to use an IPSec VPN.

The first of the VPN gateways transmit a request to the next gateway to set up an IPSec connection in order to enable VPN connections. The two VPN gateways establish an IPSec connection and communicate with one another. When domains over one system need to interact with domains on the other system, the routing on each system is set up such that the traffic flow is immediately diverted through the IPSec connection, safeguarding it as necessary. The connections between the two networks can be supported by a single IPSec connection that creates a tunnel between the gateways, or numerous IPSec connections can each protect a distinct class or kind of data. The VPN tunnel is protected by encryption algorithms against online attackers and data theft. The encryption techniques to be used are selectable by the administrator. Although RC4 is quicker, it has less robustness. Although AES256 is slower, it has almost perfect strength. The following HMAC (Hash-based Message Authentication Code) - 160-bit hashing algorithms are also used by VPN. They are all held to global standards.

5. Conclusion and Future Work

The main focus of this report has been to create a robust network system as a network security engineer for equinox IT Solutions LTD. Based on the figures and demonstrations, a successful network system was established for the organization. Configurations like OSPF routing, VLAN, and inter-VLAN were completed on the routers. Furthermore the services like access lists, site-to-site VPN, firewall, and network Intrusion prevention system were established.

Research work was done on Zero-trust security framework in the network and based on the previous findings and assumption this was implemented. The confidentiality, integrated and availability are the key principles that must be upheld while implementing the Zero-trust security framework.

VPNs are discussed in the research portion. A general discussion of VPNs are done along with its types and determining that IPsec VPN is best for the organizations. IPSec

VPN implementation for the organizations are discussed for the general requirements of the business and also for remote connection for the employees to the organization's network in a work from home situation. Therefore it is important to use best practices and remediate risks while implementing a network security system for an organization.

References:

Simmons, C. (2001). Microsoft ISA Configuration and Administration. Wiley.

Naganand Doraswamy and Harkins, D. (2002). IPSec. Upper Saddle River, N.J. ; London: Prentice Hall Ptr.

Deal, R.A. and Cisco Systems, Inc (2006). The complete Cisco VPN configuration guide. Indianapolis, Ind.: Cisco Press.

Hooper, H. (2012). CCNP security VPN : 642-647 official cert guide. Indianapolis, In: Cisco Press.

Snader, J.C. (2006). VPNs illustrated : tunnels, VPNs, and IPsec. Upper Saddle River, Nj Addison-Wesley C.

Lammle, T. (2007). CCNA: Cisco Certified Network Associate study guide ; [exam 640-802]. Indianapolis, Ind. Wiley.