Network Topology Proposal for Tech Zolutions Inc

Student ID: 5662142

Table of Contents

1. Introduction

This report was created on behalf of the company Tech Zolutions Inc. Specifically, the company has recently moved to a new office building with 150 employees. The office is divided into five departments, development, sales, HR, IT, and Finance. It also has a conference room accessible to all departments and a server room. This report details how a secure network was designed and implemented for this company.

The designed network separates the departments and services into network segments. The network is secured with Zone-Policy Firewalls, passwords, encryptions, and AAA authentications. A VPN connection was established to secure site-to-site communication with the company's remote branch office. The final topology was created and simulated using Cisco Packet Tracer.

2. Network design

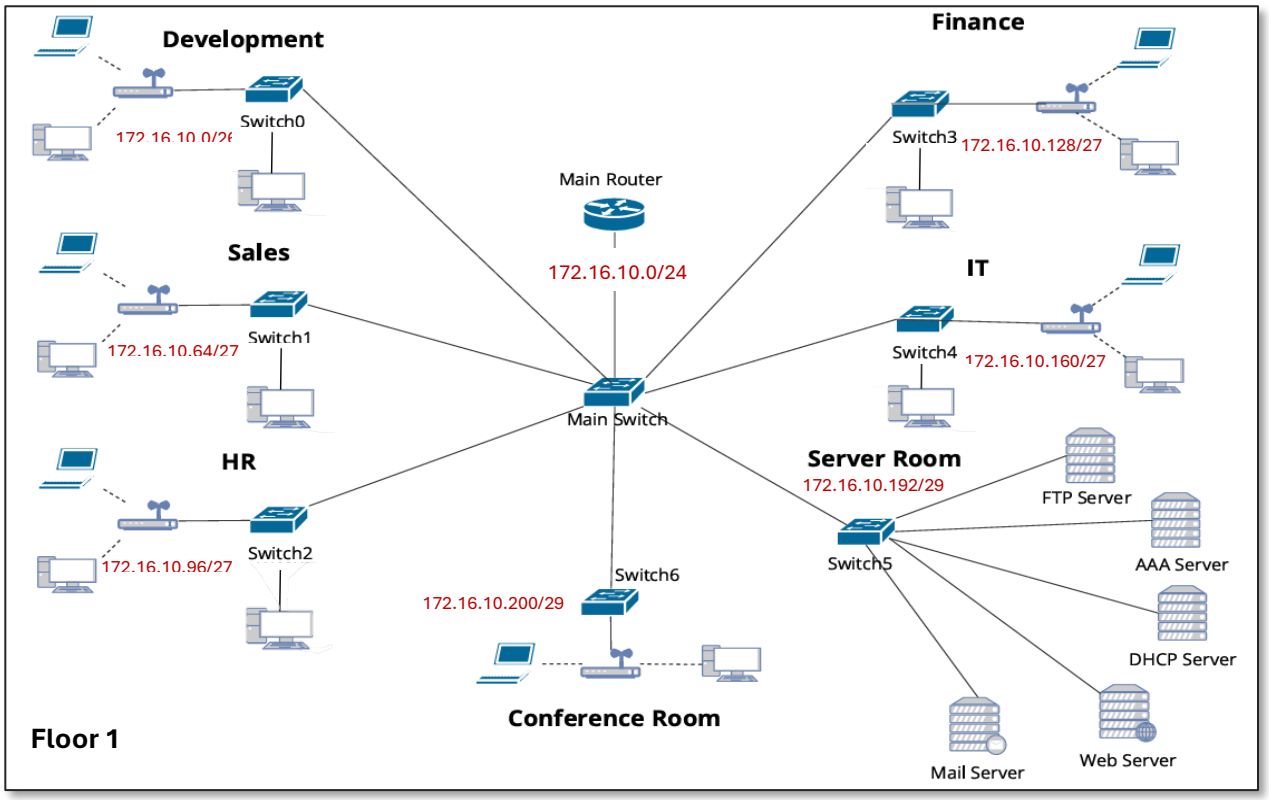

Figure 1. Initial Network Design for Tech Zolutions Inc.

The initial network topology consists of the five departments, a conference room and a server room on the first floor of the office. All these divisions are connected by a main router that handles inter-network routing. Each department has a wireless network which devices can connect to. Departments and the conference room can host several devices, such as laptops or PCs. To allow video conferencing, the conference room contains a laptop and PC.

The server room contains the company's servers. The FTP server simulates the company's file system. The DHCP server assigns IP addresses dynamically. The web server hosts the company's website, while the email server hosts the company's domain (tech.com).

3. implementation

3.1 Network Design and Configuration

3.1.1 subnetting

Justification

The office's network was divided into 8 subnets: one for each department, one for the server room, one for the conference room, and another for the demilitarized zone (discussed later). The network was grouped as such to separate the departments since each has distinct network requirements. It also ensures data security, especially for the server room.

Configuration

The company has the assigned base address 172.16.10.0/24. This IP range was divided across the 8 subnets to accommodate each subnet's required number of hosts.

Each subnet was allocated the minimum number of IP addresses needed to accommodate its required number of hosts (employees) (Table 1). This approach leaves the maximum number of addresses available for future subnet expansions. The first usable IP address in each subnet was allocated to the default gateway. To assign the address ranges, the largest remaining subnet was assigned first, up until all were allocated.

Subnet Name	Requested Host Addresses	Network Address	Default Gateway	Usable Ip Address Range	Broadast Address	Subnet Mask
Development	50	172.16.10.0/26	172.16.10.1	172.16.10.1-172.16.10.62	172.16.10.63	255.255.255.192
Sales	30	172.16.10.64/27	172.16.10.65	172.16.10.65-172.16.10.94	172.16.10.95	255.255.255.224
HR	25	172.16.10.96/27	172.16.10.97	172.16.10.97-172.16.10.126	172.16.10.127	255.255.255.224
Finance	25	172.16.10.128/27	172.16.10.129	172.16.10.129-172.16.10.158	172.16.10.159	255.255.255.224
IT	20	172.16.10.160/27	172.16.10.161	172.16.10.161-172.16.10.190	172.16.10.191	255.255.255.224
Server Room	3	172.16.10.192/29	172.16.10.193	172.16.10.193-172.16.10.198	172.16.10.199	255.255.255.248
Conference Room	3 (implicit)	172.16.10.200/29	172.16.10.201	172.16.10.201-172.16.10.206	172.16.10.207	255.255.255.248
DMZ	2	172.16.10.208/29	172.16.10.209	172.16.10.209-172.16.10.214	172.16.10.215	255.255.255.248

Table 1. Subnetting of the internal network.

All devices in the network were assigned IP addresses statically through the **ip configuration** window. For example, the first end device in the development department was assigned the IP address 172.16.10.2, with a default gateway of 172.16.10.1 (Figure 2).

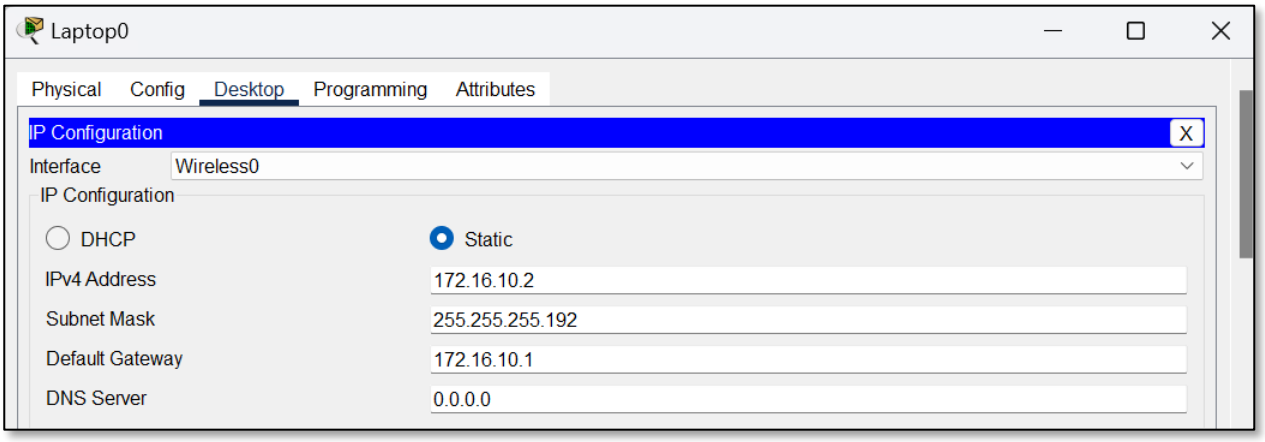

Figure 2. Statically assigning IP address to Laptop0.

Verification

The assignment of the IP addresses was verified by hovering over each device in the packet tracer file.

```
Device Name: Laptop0
Device Model: Laptop-PT

Port         Link   IP Address          IPv6 Address                            MAC Address
Wireless0    Up     172.16.10.2/26      <not set>                               0010.1138.5180
Bluetooth    Down   <not set>           <not set>                               00E0.B009.B25E

Gateway: 172.16.10.1
DNS Server: 8.8.8.8
```

Figure 3. Result of hovering over Laptop0.

3.1.2 VLANs

Justification

Each subnet (Table 1) was assigned a VLAN to segment the network. The VLANs were implemented with a main switch connected to the main router using Router-on-a-stick (ROAS). The main switch is connected to each local switch, which in turn serves a subnet/VLAN. To enhance network security, VLAN 99 was designated as the native VLAN, replacing the default VLAN 1.

Since each subnet has its own VLAN, the connected devices in the same VLAN can communicate with each other but must pass through the router to communicate with other VLANs. For example, VLAN 10's devices can communicate with each other, but must pass through the router (inter-VLAN routing) to communicate with VLAN 20. This logically separates network traffic between subnets and ensures ACLs can restrict unauthorized

access. The separation also makes the network more scalable if future network expansions or restructurings are made. This design reduces traffic load since each local switch only transmits the traffic of its local VLAN.

Configuration

Configuring the VLANs included configuring the local department switches, the main switch, then the main router.

Subnet/VLAN Name	VLAN	Network Address	Switch - Devices	Switch - Main Switch Int.	Main Switch - Switch Int.	Default Gateway	Default Gateway Int.
Development	10	172.16.10.0/26	Fa0/1 Fa0/2	Fa0/4	Fa0/2	172.16.10.1	G0/0.10
Sales	20	172.16.10.64/27	Fa0/2 Fa0/3	Fa0/1	Fa0/3	172.16.10.65	G0/0.20
HR	30	172.16.10.96/27	Fa0/2 Fa0/3	Fa0/1	Fa0/4	172.16.10.97	G0/0.30
Finance	40	172.16.10.128/27	Fa0/1 Fa0/2	Fa0/4	Fa0/5	172.16.10.129	G0/0.40
IT	50	172.16.10.160/27	Fa0/1 Fa0/2	Fa0/4	Fa0/6	172.16.10.161	G0/0.50
Server Room	60	172.16.10.192/29	Fa0/1 Fa0/2 Fa0/3	Fa0/4	Fa0/7	172.16.10.193	G0/0.60
Conf. Room	70	172.16.10.200/29	Fa0/2 Fa0/4	Fa0/1	Fa0/8	172.16.10.201	G0/0.70
Native	99	N/A	N/A	N/A	N/A	N/A	N/A

Table 2. Assigned VLANs of each subnet and their respective connected interfaces.

Local Switches Configuration

On each subnet's local switch, the corresponding VLAN was created (Figure 4). VLAN 99 was also configured as the native VLAN. For example, the Development department was assigned VLAN 10 (labelled Development) (Table 2). All interfaces on the local switch connecting to end devices were set to access mode and assigned respective VLANs. For example, any laptops, pcs, or access points connected to the development's switch were set on VLAN 10. The interface connecting each local switch to the main switch was set to trunk mode, enabling traffic exchange between different VLANs. VLAN 99 was allocated as the native VLAN for trunk links.

```
Dev(config)#vlan 99
Dev(config-vlan)#name Native
Dev(config-vlan)#exit
Dev(config)#vlan 10
Dev(config-vlan)#name Development
Dev(config-vlan)#exit
Dev(config)#interface Fa0/1
Dev(config-if)#switchport mode access
Dev(config-if)#switchport access vlan 10
Dev(config-if)#interface Fa0/2
Dev(config-if)#switchport mode access
Dev(config-if)#switchport access vlan 10
Dev(config)#interface Fa0/4
Dev(config-if)#switchport mode trunk
Dev(config-if)#switchport trunk allowed vlan 10
Dev(config-if)#switchport trunk native vlan 99
```

Figure 4. Configuring VLANs on development's subnet switch

Main Switch Configuration

On the main switch, all the VLANs were created and named respectively, ranging from VLAN 10 to 70 (Figure 5). The native VLAN 99 was also created. The interface on the main switch connecting to the main router was trunked to enable traffic from several VLANs.

```
MainSwitch(config)#vlan 99
MainSwitch(config-vlan)#name Native
MainSwitch(config-vlan)#vlan 10
MainSwitch(config-vlan)#name Development
MainSwitch(config-vlan)#vlan 20
MainSwitch(config-vlan)#name Sales
MainSwitch(config-vlan)#vlan 30
MainSwitch(config-vlan)#name HR
MainSwitch(config-vlan)#vlan 40
MainSwitch(config-vlan)#name Finance
MainSwitch(config-vlan)#vlan 50
MainSwitch(config-vlan)#name IT
MainSwitch(config-vlan)#vlan 60
MainSwitch(config-vlan)#name Server
MainSwitch(config-vlan)#vlan 70
MainSwitch(config-vlan)#name Conference
```

Figure 5. Creating VLANs on main switch.

Trunk mode was enabled on every interface connecting the main switch to a local switch (Figure 6). Only the VLAN specific to that subnet was allowed. For example, only VLAN 10 was allowed on the trunk link between the main switch and development switch (Figure 6). Although multiple VLANs could be allowed on the trunk link, it was limited to the subnet-specific VLAN to control and secure traffic. The native VLAN 99 was set up.

```
MainSwitch(config-if)#interface Fa0/2
MainSwitch(config-if)#switchport mode trunk
MainSwitch(config-if)#switchport trunk allowed vlan 10
MainSwitch(config-if)#switchport trunk native vlan 99
```

Figure 6. Setting the interface connecting main switch to development's local switch to trunk mode.

The connection from the main switch to the main router was also set to trunk mode (Figure 7). On it, VLANs 10 to 70 were allowed, enabling traffic from all the created VLANs to reach the router. Again, the native VLAN 99 was set up.

```
MainSwitch(config)#interface fa0/1
MainSwitch(config-if)#switchport mode trunk
MainSwitch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70
MainSwitch(config-if)#switchport trunk native vlan 99
```

Figure 7. Setting the interface connecting main switch to main router to trunk mode.

Main Router Configuration

To enable Inter-VLAN routing, ROAS was used. The main router is connected to the main switch on the interface Gig0/0. Each VLAN created was assigned to a sub-interface on Gig0/0. For example, VLAN 10 was assigned to the interface Gig0/0.10 (Figure 8). The sub-interface Gig0/0.99 was reserved for VLAN 99. Each sub-interface's default gateway was set as the first usable address of the subnet.

```
MainRouter(config)#interface GigabitEthernet0/0.99
MainRouter(config-subif)#encapsulation dot1Q 99 native
MainRouter(config-subif)#interface GigabitEthernet0/0.10
MainRouter(config-subif)#encapsulation dot1Q 10
MainRouter(config-subif)#ip address 172.16.10.1 255.255.255.192
MainRouter(config-subif)#interface GigabitEthernet0/0.20
MainRouter(config-subif)#encapsulation dot1Q 20
MainRouter(config-subif)#ip address 172.16.10.65 255.255.255.224
```

Figure 8. Configuring router-on-a-stick on the main router.

Verification

Local Switch Verification

The commands **show vlan brief** and **show interfaces trunk** verify the correct interfaces were set up on the VLANs and trunk mode. All end devices (on interfaces Fa0/1-3) are connected on VLAN 10, native VLAN is set to 99, and only VLAN 10 is allowed on trunk port Fa0/4.

```
Dev#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Development                      active    Fa0/1, Fa0/2, Fa0/3
99   Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Dev#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/4       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/4       10
```

Figure 9. Verifying VLANs and trunks on the development's local switch.

Main Switch Verification

The main switch's VLANs are correctly set up (Figure 10). The trunk ports between local switches and the main switch allow only the local VLAN. The interface Fa0/1 (connecting main switch to router) correctly allows VLANs 10-70 to be routed (Figure 11).

```
MainSwitch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Development                      active
20   Sales                            active
30   HR                               active
40   Finance                          active
50   IT                               active
60   Server                           active
70   Conference                       active
99   Native                           active
```

Figure 10. Verifying VLANs on the main switch.

```
MainSwitch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99
Fa0/4       on           802.1q         trunking      99
Fa0/5       on           802.1q         trunking      99
Fa0/6       on           802.1q         trunking      99
Fa0/7       on           802.1q         trunking      99
Fa0/8       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,30,40,50,60,70
Fa0/2       10
Fa0/3       20
Fa0/4       30
Fa0/5       40
Fa0/6       50
Fa0/7       60
Fa0/8       70
```

Figure 11. Verifying trunk connections on main switch.

Main Router Verification

Router-on-a-stick is correctly set up since each VLAN's sub-interface appears in the **show run** command (Figure 12).

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.1 255.255.255.192
 ip helper-address 172.16.10.196
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.10.65 255.255.255.224
 ip helper-address 172.16.10.196
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.10.97 255.255.255.224
 ip helper-address 172.16.10.196
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.10.129 255.255.255.224
 ip helper-address 172.16.10.196
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 172.16.10.161 255.255.255.224
 ip helper-address 172.16.10.196
!
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 172.16.10.193 255.255.255.248
 ip access-group AAA-ACL out
!
interface GigabitEthernet0/0.70
 encapsulation dot1Q 70
 ip address 172.16.10.201 255.255.255.248
 ip helper-address 172.16.10.196
!
interface GigabitEthernet0/0.99
 encapsulation dot1Q 99 native
 no ip address
```

*Figure 10. Results of the **show run** command on main router.*

Testing connection

Because of VLANs and ROAS, different VLANs can ping other VLANs within the network. For example, Laptop6 in VLAN 10 (172.16.10.2) can successfully ping VLAN 20 (172.16.10.66) and VLAN 50 (172.16.10.162) (Figure 13).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.66

Pinging 172.16.10.66 with 32 bytes of data:

Reply from 172.16.10.66: bytes=32 time=8ms TTL=127
Reply from 172.16.10.66: bytes=32 time=4ms TTL=127
Reply from 172.16.10.66: bytes=32 time=12ms TTL=127
Reply from 172.16.10.66: bytes=32 time=10ms TTL=127

Ping statistics for 172.16.10.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 12ms, Average = 8ms

C:\>ping 172.16.10.162

Pinging 172.16.10.162 with 32 bytes of data:

Reply from 172.16.10.162: bytes=32 time<1ms TTL=127
Reply from 172.16.10.162: bytes=32 time<1ms TTL=127
Reply from 172.16.10.162: bytes=32 time=10ms TTL=127
Reply from 172.16.10.162: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.162:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Figure 11. Successful Inter-VLAN routing between VLAN 10, 20, and 50

3.1.3 Servers Configuration

Four servers were set up in the server room: FTP, DHCP, Web, and Email Server. The FTP server simulates the company's file server, containing shared files and databases. The web server hosts the company's website and internal web applications. The DHCP assigns IP addresses to devices, while the email server handles email communications within the company. Table 3 summarizes users created on the aforementioned servers.

SERVER NAME	IP ADDRESS	USERNAME	PASSWORD
FTP	172.16.10.194	ftp_user	123
		ftp2	123
EMAIL	172.16.10.195	user1@tech.com	123
		user2@tech.com	123
AAA	172.16.10.198	it1	123
DHCP	172.16.10.196	N/A	N/A
WEB	172.16.10.197	N/A	N/A

Table 3. Server Room credentials.

FTP Server

On the FTP server, only the FTP service was enabled. Two users were created with all permissions enabled (Figure 14).

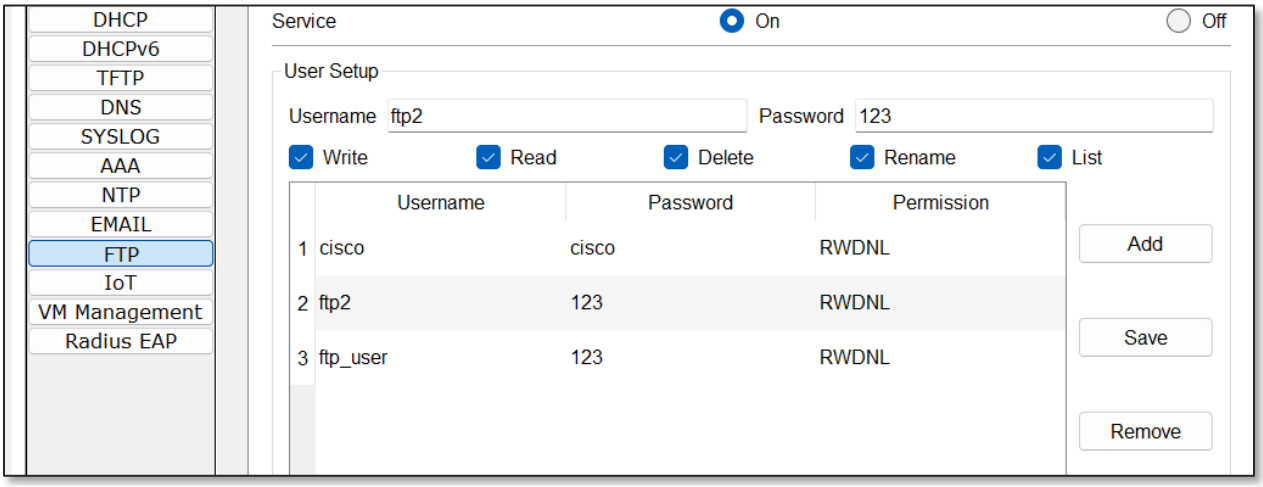

Figure 12. Setting up the FTP server.

To verify functionality, Laptop5 (conference room) accesses the FTP server and sends a file, which appears in the FTP server. Other devices in the internal network had the same successful result.

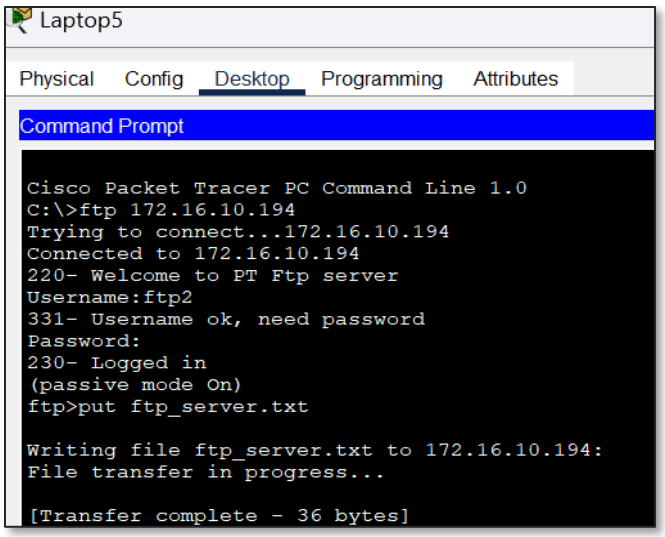

Figure 15. Laptop5 (VLAN 70) connecting and transferring to FTP Server (VLAN 60).

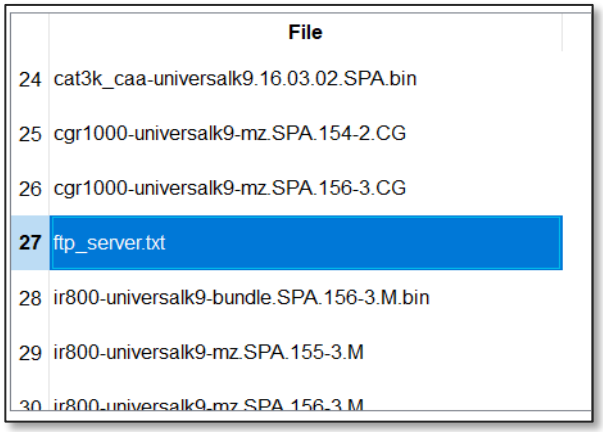

Figure 13. FTP server (VLAN 60) receiving transferred file from Laptop5 (VLAN 70).

Email Server

On the email server, only SMTP and POP3 services were enabled. Two users were created on the service, with the domain name set to **tech.com** (Figure 17).

To verify functionality, an email was sent from user1 on Laptop5 (Conference Room) to user2 on Laptop2 (HR). The email was successfully received (Figure 19).

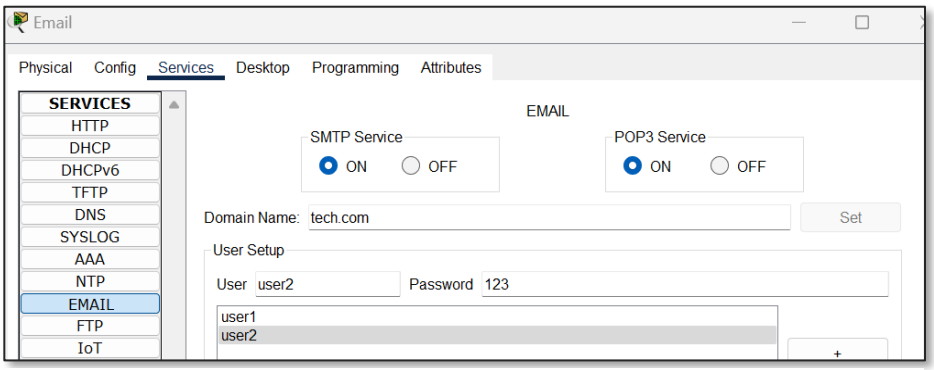

Figure 15. Setting up the Email Server.

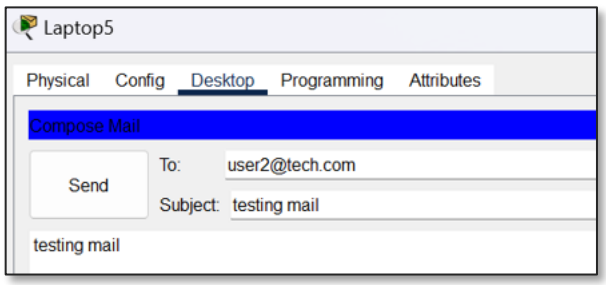

Figure 18. user1 sending an email to user2.

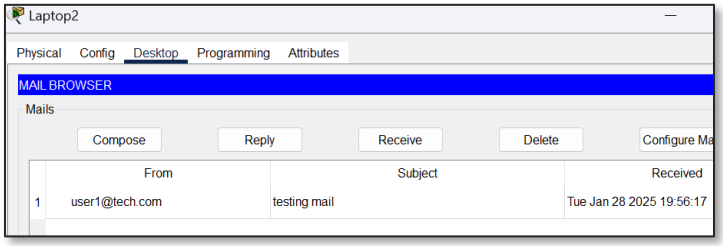

Figure 14. user2 receiving email from user1.

Web Server

To set up the Web server, only HTTP/HTTPS services were enabled. The content of the **index.html** (FIGURE 20) was overwritten to ensure it was the correct file being served. To verify functionality, an HTTP request from Laptop6 (VLAN 10) accesses the web server by requesting the server's IP address (172.16.10.197) on the web browser (Figure 21).

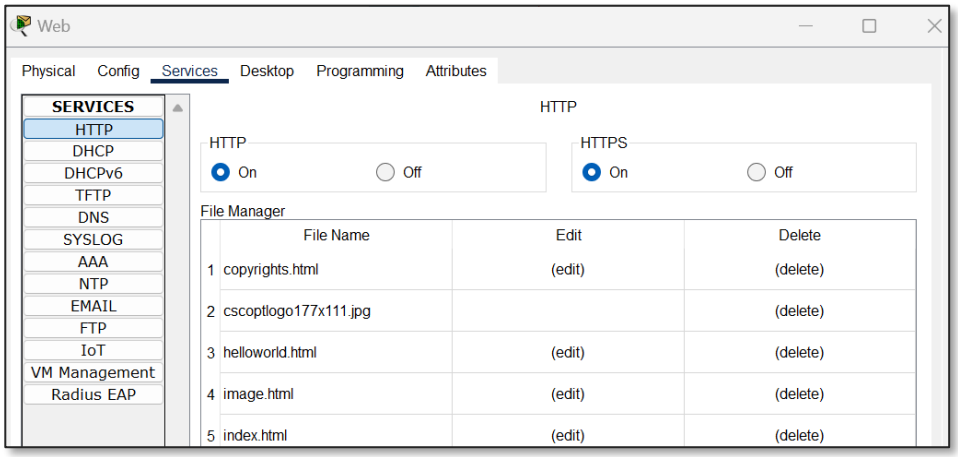

Figure 17. Setting up the Web Server.

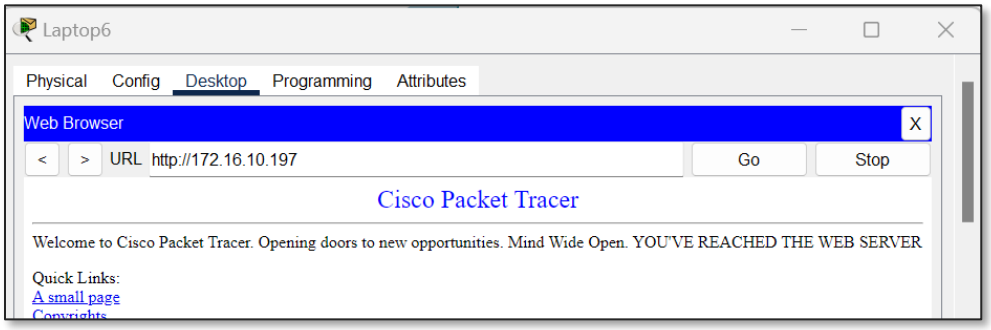

Figure 17. Laptop6 accesses the Web Server.

DHCP Server

On the DHCP server, DHCP service was enabled. A separate pool was created for each VLAN to assign the subnets (Figure 22). For example, VLAN 10 was given the default gateway 172.16.10.1 and a start address of 172.16.10.2. This allowed the DHCP server to dynamically assign IP addresses.

Currently, the router blocks broadcasts, so end devices cannot make DHCP broadcasts to reach the DHCP server. A DHCP helper address was set on the main router's sub-interfaces; this allows request forwarding from any VLAN to the DHCP server. Figure 23 demonstrates setting the helper address on the main router for VLAN 10.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan70	172.16.10.201	8.8.8.8	172.16.10.202	255.255.255....	6	0.0.0.0	0.0.0.0
vlan10	172.16.10.1	8.8.8.8	172.16.10.2	255.255.255....	62	0.0.0.0	0.0.0.0
vlan20	172.16.10.65	8.8.8.8	172.16.10.66	255.255.255....	30	0.0.0.0	0.0.0.0
vlan30	172.16.10.97	8.8.8.8	172.16.10.98	255.255.255....	30	0.0.0.0	0.0.0.0
vlan40	172.16.10.129	8.8.8.8	172.16.10.130	255.255.255....	30	0.0.0.0	0.0.0.0
vlan50	172.16.10.161	8.8.8.8	172.16.10.162	255.255.255....	30	0.0.0.0	0.0.0.0

Figure 19. Setting up the DHCP server.

```
MainRouter(config)#interface GigabitEthernet0/0.10
MainRouter(config-subif)#ip helper-address 172.16.10.196
```

Figure 18. Setting the DHCP helper address.

To verify the DHCP functionality, end devices were set to DHCP in **IP configuration**. Laptop0 was allocated the first available IP address in VLAN 10 (Figure 24).

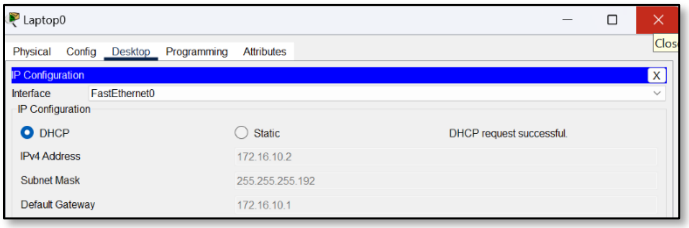

Figure 20. Verifying DHCP Server.

3.1.4 Wireless connections

To set up wireless connections, an access point (AP) was placed in each subnet, excluding the server room (VLAN 60). This allowed employees to operate on a wireless network within their VLANs. All end devices connecting wirelessly were set up with WPC300N/ WMP300N wireless adaptors to enable wireless AP connection.

On port 1 of each AP, the port was switched on, and the WPA2-PSK authentication was enabled with a passkey (Table 4). This ensures only authorized devices can connect wirelessly.

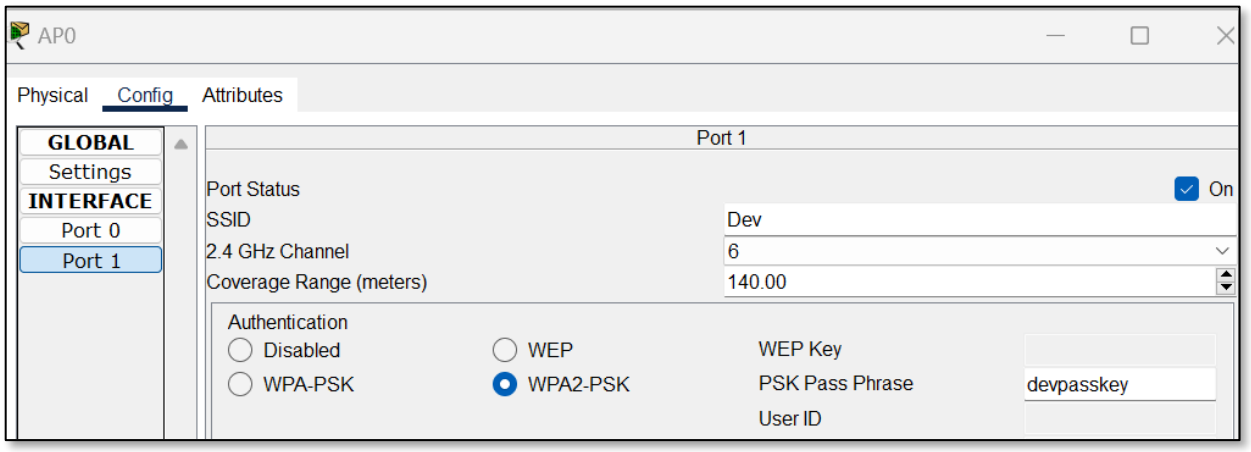

Figure 21. Setting up development's access point.

AP NAME	ASSIGNED VLAN	PASSWORD	CONNECTED DEVICES
AP0	Development	devpasskey	Laptop0 – PC0
AP1	Sales	salespasskey	Laptop1 – PC1
AP2	HR	hrpasskey	Laptop2 – PC2
AP3	Finance	finpasskey	Laptop3 – PC3
AP4	IT	itpasskey	Laptop4 – PC4
AP5	Conf. Room	confpasskey	Laptop5 – PC5

Table 4. Wireless APs configuration.

To verify functionality, Laptop0 in the Development department connects to AP0 (Figures 26-27).

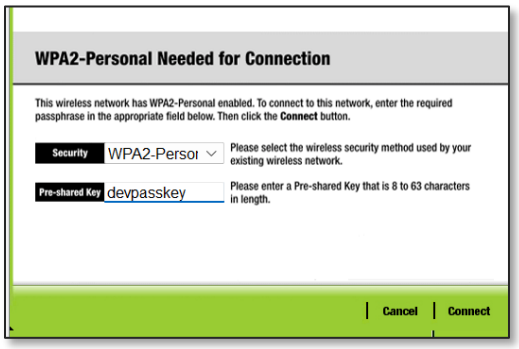

Figure 26. Laptop0 (Development) connecting to AP0.

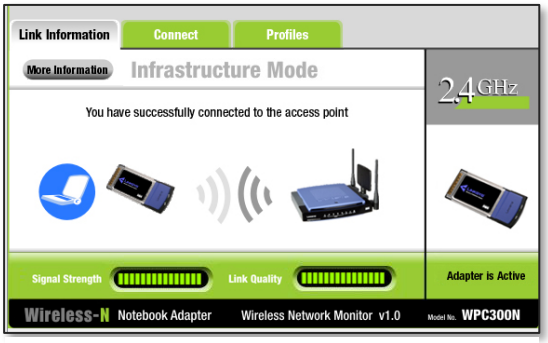

Figure 27. Laptop0 (Development) connected to AP0.

3.2 Security and Zones of Trust

3.2.1 Password Configuration

Passwords were configured on all switches and routers within the network (Table 5). The passwords were set on the console line and privileged mode access, ensuring two-step security and permitting only authorized access. The **password-encryption service** was enabled to encrypt passwords. Figure 28 demonstrates setting password for development. The passwords were simplified for ease of temporary usage.

```
Dev#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Dev(config)#line console 0
Dev(config-line)#password dev123
Dev(config-line)#login
Dev(config-line)#enable password dev123
Dev(config)#exit
Dev#
%SYS-5-CONFIG_I: Configured from console by console

Dev#show running-config | section password
service password-encryption
enable password 7 08254958584B56
 password 7 08254958584B56
```

Figure 28. Setting encrypted passwords on Development's local switch.

Device Name	Device Type	Console Password	Privileged Mode Password
Dev	Switch-2960	dev123	dev123
Sales	Switch-2960	sales123	sales123
HR	Switch-2960	hr123	hr123
Finance	Switch-2960	fin123	fin123
IT	Switch-2960	it123	it123
Server Room	Switch-2960	ser123	ser123
Conf. Room	Switch-2960	conf123	conf123
DMZ	Switch-2960	dmz123	dmz123
Main Switch	Switch-2960	main123	main123
Main Router	Router-2911	main123	main123
Zone Router	Router-2911	zone123	zone123
Remote Router	Router-2911	rem123	rem123
Remote	Switch-2960	rem123	rem123
External (ISP)	Router-2911	isp123	isp123
External	Switch-2960	ext123	ext123

Table 5. Password configuration of all switches and routers.

3.2.2 Zones Design

The network was divided into three zones: internal, demilitarized (DMZ), and external (Figure 29). This design enhances security by controlling traffic flow; the zones ensure the internal network is isolated from external networks while still allowing authorized access to internal services.

The DMZ hosts the mail and web server. External networks can freely access the DMZ, allowing external devices access to public-side services; these include the company's website and email server. The external zone would only require access to these two servers, so internal processes are protected. The DMZ was assigned the next available subnet from the internal network (172.16.10.208/29). This ensured the DMZ was not part of internal VLANs.

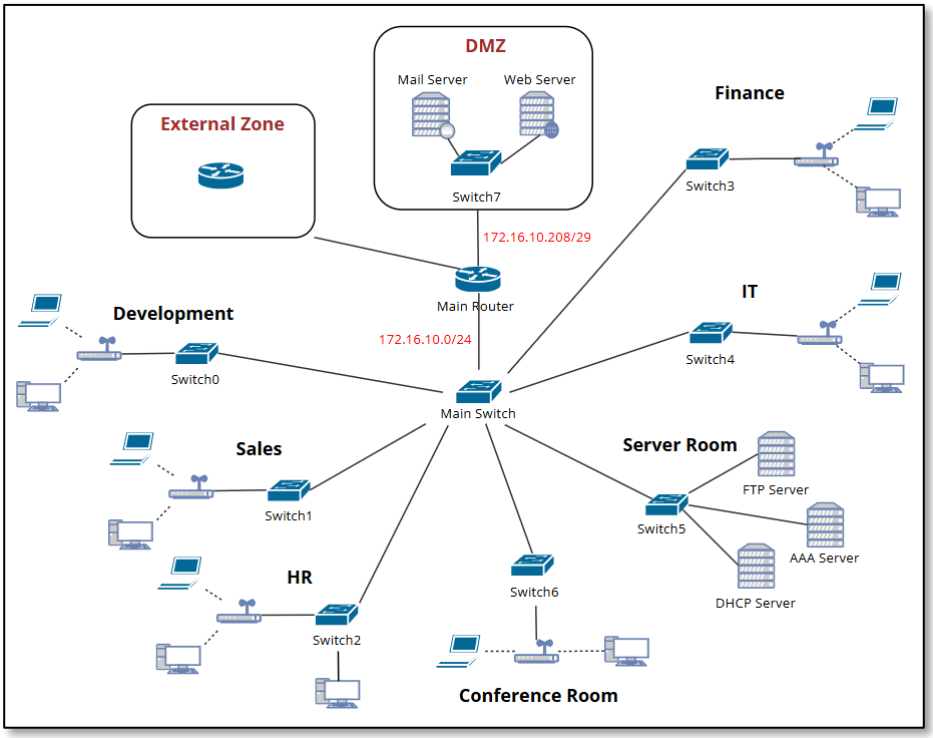

Figure 29. Dividing network into zones of trust (Internal, DMZ, External)

Policies

The policies, summarized in Table 6, were created with internal zone security and the company's requirements in mind.

Inner Zone Policies

Any established connections from the DMZ must be accepted to ensure the web and email servers can reply to initiated connections. Any established connections from the outer zone must be accepted to allow responses to internally initiated requests. For example, employees requesting a website from the internet require a response.

DMZ Policies

The DMZ contains email and web servers. Therefore, external requests for the company's website must be accepted. Similarly, external mail users must be able to send emails to the company's mail server. Both servers must be able to receive responses to initiated external connections.

The DMZ must also accept internal users accessing its web server or resolving domain names using DNS. This grants employees access to the company's website. Additionally, the internal users must send/retrieve emails, so they require access to the email server. The IT department must communicate freely with the DMZ since the department requires access to all network devices and servers.

Outer Zone Policies

Internal users must access external web services to access the internet. They must also be able to use DNS. Any established connections must be allowed access, but any requests from the server room must be denied. This mitigates the risk of critical data leakages.

To allow emails to be sent from the email server, the DMZ must be able to send emails to the external zone. The DMZ must also be able to use DNS and receive responses to initiated connections.

Source Zone	Destination Zone	Protocol Allowed	Source	Destination
Outer	Inner	TCP	Remote Branch	FTP server
		TCP (established)	Any	Any
Inner	Outer	TCP (established)	Any	Any
		TCP	Any (excluding server room)	Any
		HTTP, HTTPS, DNS	Any	Any
Inner	DMZ	HTTP, HTTPs, DNS	Any	Web Server
		SMTP (25), POP3 (110), POP3S (995), IMAP (143), IMAPS (993)	Any	Email Server
		TCP (established)	Any	Any
		IP	IT department	Any
DMZ	Inner	IP	Any	Remote Branch
		TCP (established)	Any	Any
Outer	DMZ	HTTP, HTTPs, DNS	Any	Web Server
		SMTP	Any	Email Server
		POP3, POP3S, IMAP, IMAPS	Remote Branch	Email Server
		TCP (established)	Any	Any
DMZ	Outer	SMTP (25, 465, 587), DNS	Email Server	Any
		TCP (established)	Any	Any

Table 6. Summary of ZPFs.

3.2.3 ZPFs Implementation

Zone Router - Main Router Configuration

To implement the zones, an additional router (called Zone Router) was added on top of the main router. This was necessary because the main router was configured with sub-interfaces for inter-VLAN routing, so zone-based firewall segmentation cannot be directly applied to it. The zone router's interfaces are summarized in Table 7; the outer zone was assigned a random IP address. To connect the routers, a new subnet (172.16.10.216/29) was created. The main router's interface was allocated the IP address 172.16.10.217, and the zone router's interface the address 172.16.10.218. The interfaces of the zone router link the outer zone, inner zone, and DMZ.

Zone	Source Router	Source Interface	Source Interface IP/Default Gateway
Outer	Zone Router	Gig0/0	198.51.100.1/24
DMZ	Zone Router	Gig0/1	172.16.10.209/29
Inner	Zone Router	Gig0/2	172.16.10.218/29

Table 7. Zone router's interfaces.

Static routing was used to forward packets from the main router to the zone router and vice versa. The zone router forwards packets from the external zone (198.51.100.0/24) and the DMZ (172.16.10.208/29) to the main router (172.16.10.217) (Figures 31-33) and vice versa.

```
MainRouter(config)#ip route 172.16.10.208 255.255.255.248 172.16.10.218
MainRouter(config)#ip route 198.51.100.0 255.255.255.192 172.16.10.218
```

Figure 30. Setting static routes from main router (172.16.10.217) to zones router (172.16.10.218).

```
L       172.16.10.201/32 is directly connected, GigabitEthernet0/0.70
S       172.16.10.208/29 [1/0] via 172.16.10.218
C       172.16.10.216/29 is directly connected, GigabitEthernet0/1
L       172.16.10.217/32 is directly connected, GigabitEthernet0/1
     175.16.0.0/24 is subnetted, 1 subnets
S       175.16.10.0/24 [1/0] via 172.16.10.218
S    198.51.100.0/24 [1/0] via 172.16.10.218
```

*Figure 31. results of **show ip route** command on main router (172.16.10.217).*

```
ZonesRouter(config)#ip route 172.16.10.0 255.255.255.192 172.16.10.217
```

Figure 32. Setting static routes from zones router (172.16.10.218) to main router (172.16.10.217).

```
     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
S       172.16.10.0/24 [1/0] via 172.16.10.217
C       172.16.10.208/29 is directly connected, GigabitEthernet0/1
L       172.16.10.209/32 is directly connected, GigabitEthernet0/1
C       172.16.10.216/29 is directly connected, GigabitEthernet0/2
L       172.16.10.218/32 is directly connected, GigabitEthernet0/2
     198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       198.51.100.0/24 is directly connected, GigabitEthernet0/0
L       198.51.100.1/32 is directly connected, GigabitEthernet0/0
```

*Figure 33. Results of **show ip route** command on zone router (172.16.10.218).*

Zone Router Configuration

The zone router was configured with the **securityk9** technology package to allow for zoning (Figure 35). The version c2900 was used since that is the zone router's version (Figure 34). The router's configuration was saved, then the router was reloaded.

```
ZonesRouter#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTW
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
```

*Figure 34. Results of **show version** command on zone router.*

```
ZonesRouter(config)#license boot module c2900 technology-package securityk9
```

*Figure 35. Configuring **k9security** technology package.*

Zone Members Creation

To create the ZPFs, the zone members were first created and assigned to their respective interfaces (Table 7). This was verified using the **show zone security** command (Figure 37).

ACLs Creation

Six access control lists (ACLs) were created, one for each pair of zones (Figure 38). They were configured based on the restrictions discussed in Table 6. In addition to SMTP, POP3, POP3S (995), IMAP (143) and IMAPs (993) were used when retrieving emails should be configured. Also, SMTP (587) and SMTPS (465) were used when sending emails should be configured. Their creation was verified using the **show ip access-list** command (Figure 38).

```
ZonesRouter#show ip access-lists
Extended IP access list IN-TO-OUT-ACL
    10 permit tcp any any established
    20 deny tcp 172.16.10.192 0.0.0.7 any
    30 permit tcp any any eq www
    40 permit tcp any any eq 443
    50 permit udp any any eq domain
    60 permit tcp any any eq domain
Extended IP access list OUT-TO-IN-ACL
    10 permit tcp 175.16.10.0 0.0.0.255 host 172.16.10.194
    20 permit tcp any any established
Extended IP access list DMZ-TO-IN-ACL
    10 permit ip any 172.16.10.160 0.0.0.31
    20 permit tcp any any established
Extended IP access list IN-TO-DMZ-ACL
    10 permit tcp any host 172.16.10.210 eq www
    20 permit tcp any host 172.16.10.210 eq 443
    30 permit tcp any host 172.16.10.210 eq domain
    40 permit udp any host 172.16.10.210 eq domain
    50 permit tcp any host 172.16.10.211 eq smtp
    60 permit tcp any host 172.16.10.211 eq pop3
    70 permit tcp any host 172.16.10.211 eq 995
    80 permit tcp any host 172.16.10.211 eq 143
    90 permit tcp any host 172.16.10.211 eq 993
    100 permit tcp any any established
    110 permit ip 172.16.10.160 0.0.0.31 any
Extended IP access list OUT-TO-DMZ-ACL
    10 permit tcp any host 172.16.10.210 eq www
    20 permit tcp any host 172.16.10.210 eq 443
    30 permit tcp any host 172.16.10.211 eq smtp
    40 permit tcp 175.16.10.0 0.0.0.255 host 172.16.10.211 eq pop3
    50 permit tcp 175.16.10.0 0.0.0.255 host 172.16.10.211 eq 995
    60 permit tcp 175.16.10.0 0.0.0.255 host 172.16.10.211 eq 143
    70 permit tcp 175.16.10.0 0.0.0.255 host 172.16.10.211 eq 993
    80 permit tcp any any established
Extended IP access list DMZ-TO-OUT-ACL
    10 permit tcp host 172.16.10.211 any eq smtp
    20 permit tcp host 172.16.10.211 any eq 465
    30 permit tcp host 172.16.10.211 any eq 587
    40 permit udp host 172.16.10.211 any eq domain
    50 permit tcp host 172.16.10.211 any eq domain
    60 permit tcp any any established
```

*Figure 38. Configuring ACLs on zone router/ Result of **show ip access-list** command.*

Class Maps Creation

Six class maps of type inspect were created; each was allocated its respective ACL. For example, the IN-TO-OUT-CMAP was allocated the access-group IN-TO-OUT-ACL. The same command was repeated to assign the remaining five class maps. The type was set to **inspect** to specify that selected traffic must be inspected, and the **match-all** command was used to ensure all the conditions are met to allow traffic to pass.

```
ZonesRouter(config)#class-map type inspect match-all IN-TO-OUT-CMAP
ZonesRouter(config-cmap)#match access-group name IN-TO-OUT-ACL
```

Figure 39. Creating the inner to outer zone class map.

Policy Maps Creation

Six policy maps were created, allocating each a class map. For example, the policy map IN-TO-OUT-PMAP was allocated the class map IN-TO-OUT-CMAP (Figure 40). Its type was set to **inspect** for incoming traffic. Since no protocol was specified, the policy map inspects all protocols.

```
ZonesRouter(config-cmap)#policy-map type inspect IN-TO-OUT-PMAP
ZonesRouter(config-pmap)#class type inspect IN-TO-OUT-CMAP
ZonesRouter(config-pmap-c)#inspect
```

Figure 40. Creating the inner to outer zone policy map.

Zone Pair Creation

Six zone pairs were created, matched to their policy maps. For example, the IN-TO-OUT zone pair had source set to IN-ZONE and destination to OUT-ZONE (Figure 41).

```
ZonesRouter(config)#zone-pair security IN-TO-OUT source IN-ZONE destination OUT-ZONE
ZonesRouter(config-sec-zone-pair)#service-policy type inspect IN-TO-OUT-PMAP
```

Figure 41. Creating the zone pair for the inner to outer zone pair.

ZPF verification

The command **show policy-map type inspect zone-pair sessions** was used to check if any sessions were activated when a network request was made.

In-Out Zone Pair

The requests that must be accepted are:

- Internal devices making an HTTP/HTTPs request to an external device

This was verified by sending an HTTP request from Laptop1 (inner zone: 172.16.10.66/27) to Laptop12 (outer zone: 198.51.100.2/24). The connection was successfully detected by the IN-TO-

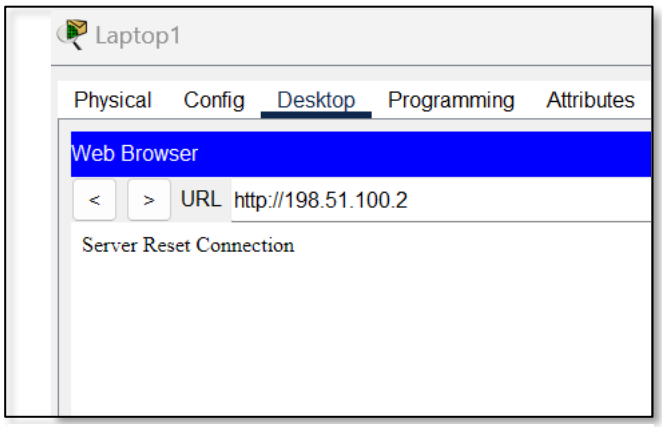

Figure 42. Inner zone (laptop1) making an HTTP request to external zone (laptop12).

```
ZonesRouter#show policy-map type inspect zone-pair sessions

policy exists on zp IN-TO-OUT
 Zone-pair: IN-TO-OUT

  Service-policy inspect : IN-TO-OUT-PMAP

    Class-map: IN-TO-OUT-CMAP (match-all)
      Match: access-group name IN-TO-OUT-ACL
      Inspect

        Number of Half-open Sessions = 1
        Half-open Sessions
         Session 1823245712
(172.16.10.66:1028)=>(198.51.100.2:80) tcp SIS_OPENING
          Created 00:00:01, Last heard  00:00:00
          Bytes sent (initiator:responder) [128:0]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

*Figure 43. In-to-out connection detected using the **show policy-map** command.*

OUT-PMAP (Figure 43). The same HTTP request to Laptop12 from DMZ devices was correctly denied.

The requests that must be denied are:

- Server Room devices making any request to an external device

This was verified by sending an HTTP request from the DHCP server (server room: 172.16.10.196) to Laptop12 (outer zone: 198.51.100.2). The request timed out on the web browser (Figure 44) and was not detected by the IN-TO-OUT-PMAP (Figure 45), confirming the request failed.

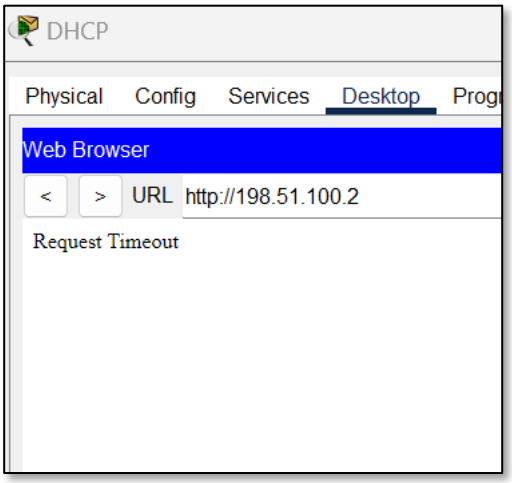

Figure 44. Server Room (DHCP server) making an HTTP request to external zone (laptop12).

```
policy exists on zp IN-TO-OUT
 Zone-pair: IN-TO-OUT

  Service-policy inspect : IN-TO-OUT-PMAP

    Class-map: IN-TO-OUT-CMAP (match-all)
      Match: access-group name IN-TO-OUT-ACL
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

*Figure 45. In-to-out connection undetected using the **show policy-map** command.*

Out-In Zone Pair

The requests that must be accepted are:

- Established connections initiated by the internal network

This was already verified in the section *"In-Out Zone Pair"* since the internal HTTP request to Laptop12 received a response (Figure 42).

The requests that must be denied are:

- Any connections that are initiated by the external network

This was verified by sending an HTTP request from the external network to the internal. Specifically, Laptop12 (external: 198.51.100.2/24) could not send an HTTP request to PC0 (inner zone: 172.16.10.3/26).

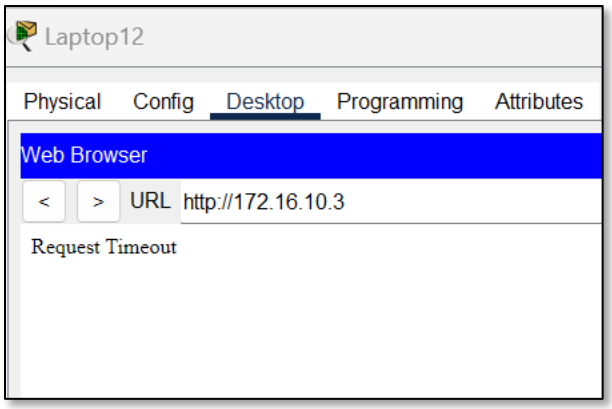

Figure 46. external zone (laptop12) making an HTTP request to Inner Zone (PC0).

```
policy exists on zp OUT-TO-IN
 Zone-pair: OUT-TO-IN

  Service-policy inspect : OUT-TO-IN-PMAP

    Class-map: OUT-TO-IN-CMAP (match-all)
      Match: access-group name OUT-TO-IN-ACL
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

*Figure 47. out-to-in connection undetected using the **show policy-map** command.*

In-DMZ Zone Pair

The requests that must be accepted are:

- Internal devices making HTTP/HTTPs requests to the web server

This was verified by sending an HTTP request to the web browser (Figure 48) and to the email browser (Figure 49) from Laptop1 (inner zone: 172.16.10.67/27). Only the request to the web browser succeeded, verifying functionality.

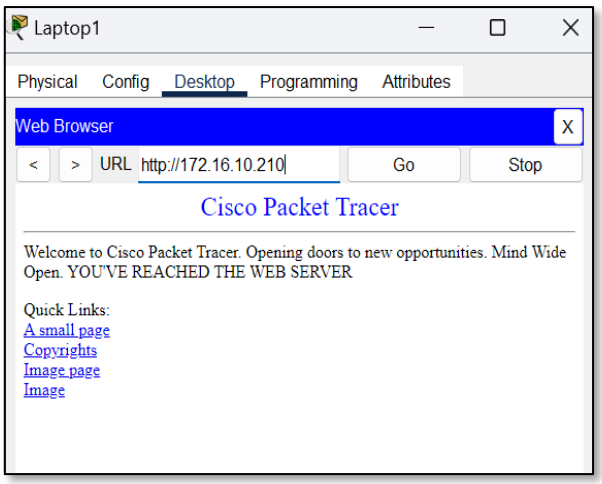

Figure 48. Successful HTTP request from inner zone to web server.

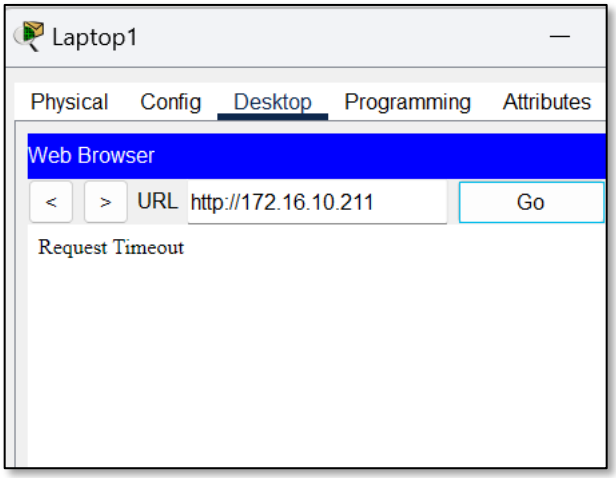

Figure 49. Failed HTTP request from inner zone to email server.

- Internal devices sending/receiving emails on the company's mail server

This was verified by sending an email from **user1** on Laptop6 to **user2** on Laptop0. Figure 51 show the email was successfully received on Laptop0.

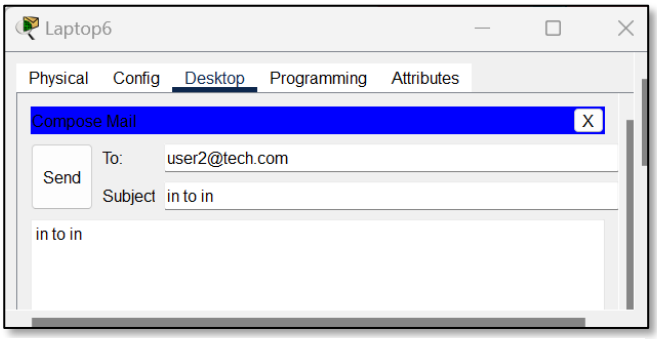

Figure 50. Successful sent email from Laptop6 (user1) to Laptop0 (user2).

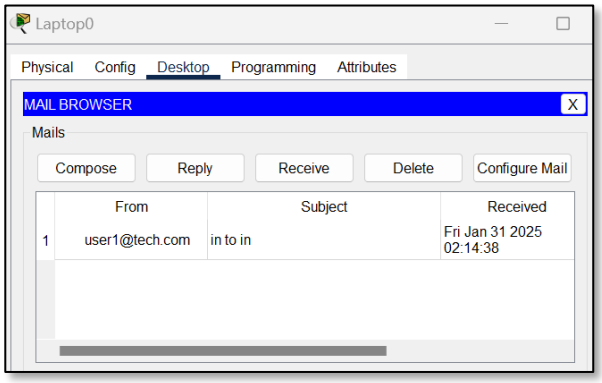

Figure 51. Successful receipt of email from Laptop6 (user1) to Laptop0 (user2).

- IT department accessing servers on the DMZ

This was verified by pinging the email server from a device in the IT department and another in the HR department. Only the IT department could ping the email server, verifying the connection (Figures 52-53).

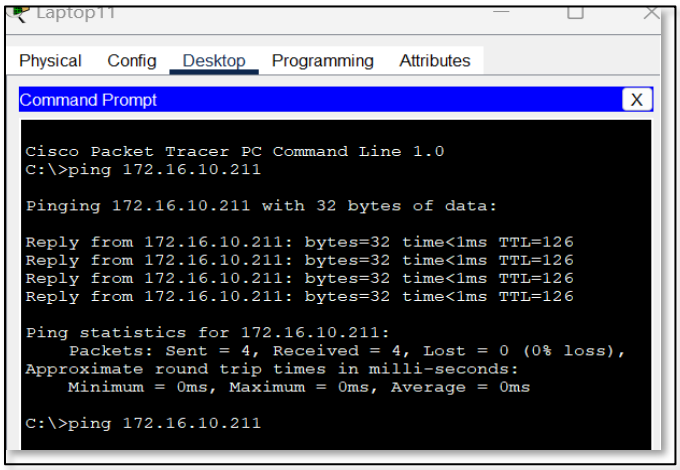

Figure 52. Successful ping to Email Server from IT department (Laptop11).

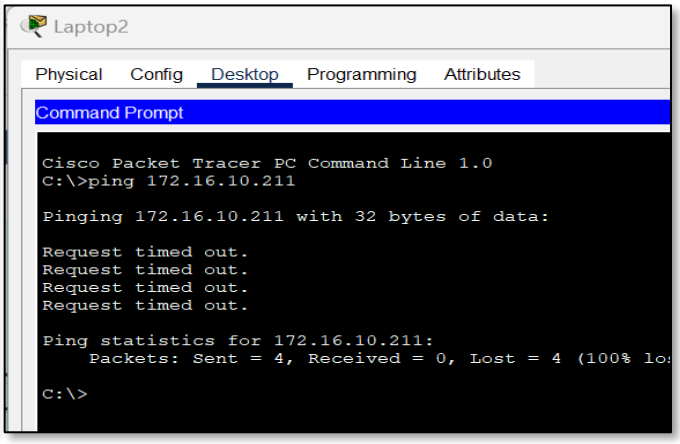

Figure 53. Failed ping to Email Server from HR department (Laptop2).

DMZ-In Zone Pair

The requests that must be accepted are:

- Established connections initiated by the internal network

This has already been verified since requests from the Internal network to the DMZ were successful (section "*In-DMZ Zone Pair*").

- Requests from DMZ to IT department only

This was verified by pinging the IT department from the DMZ. The ping was initiated from the email server to the department's Laptop11. Another ping was made to the Sales department's Laptop1. Only the IT's ping was successful which verifies the connection.

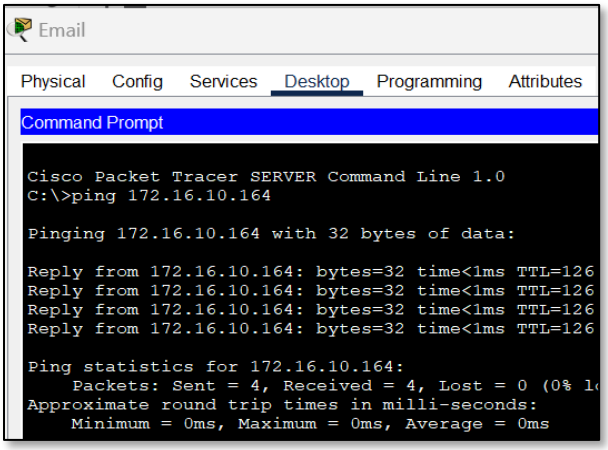

Figure 54. Successful ping from email server to laptop11 (IT).

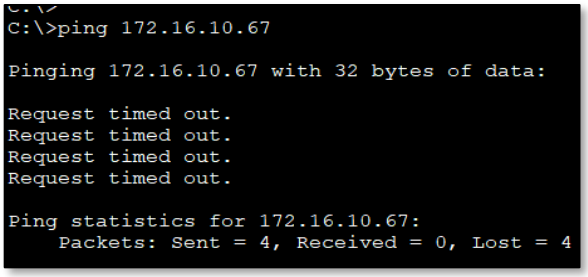

Figure 55. Failed ping from email server to laptop1 (Sales).

- Sending Emails from external mail servers to the mail server

This was verified by sending an email from the external network (Laptop12) to the email **user1@tech.com**, which exists on the company's mail server. The email was successfully sent, verifying the connection (Figure 58).

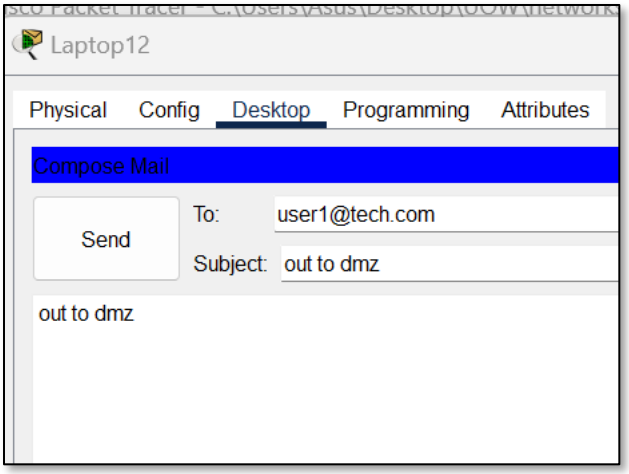

Figure 57. Email sent from External network (Laptop12).

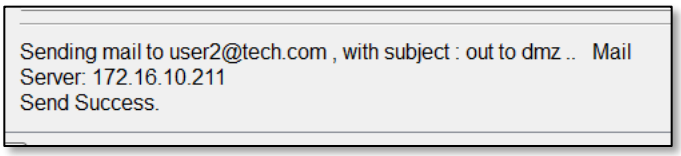

Figure 58. Email successfully sent to the email server in the DMZ.

The requests that must be denied are:

- Retrieving emails from the internal mail server on an external network

This was verified by retrieving emails from the internal mail server on the external network (Laptop12). The connection timed out, confirming the request was dropped (Figure 59).

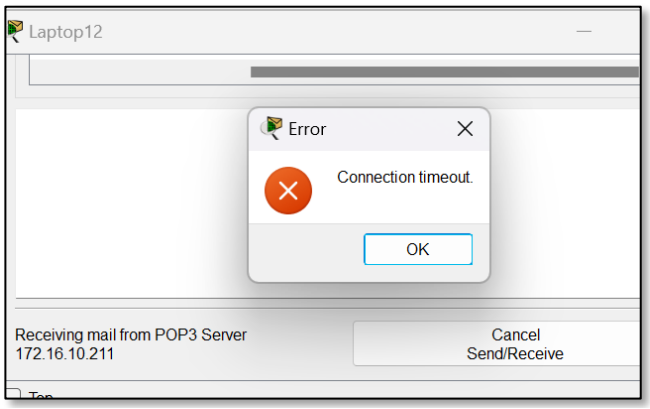

Figure 59. Connection timeout when retrieving emails on the external network (Laptop12).

DMZ-Out Zone Pair

The requests that must be accepted are:

- Sending emails from the internal mail server to an external mail server

This was verified in several steps. An external mail server (198.51.100.3 - out.com) and DNS server (198.51.100.4) were created on the external network (Figure 60). The DNS server of internal and external mail servers was set to 198.51.100.4.

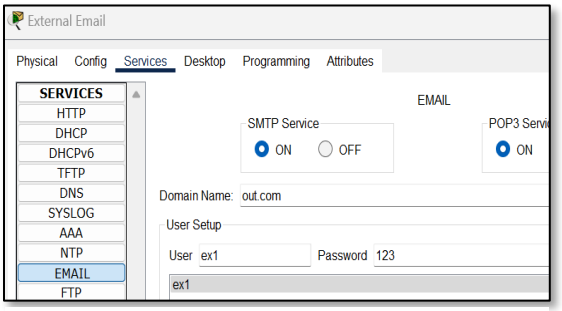

Figure 60. Setting up the external mail server.

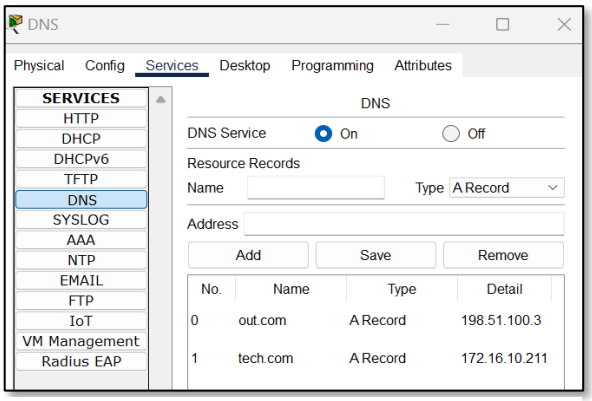

Figure 61. Setting up the DNS server (with both email servers inputted).

An email was sent from user1@tech.com from the DMZ and received by ex1@out.com on the external network (Figure).

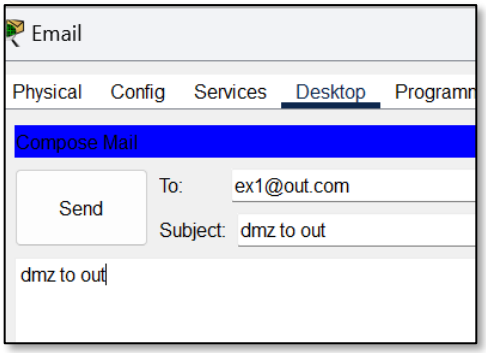

Figure 62. Sending email from user1@tech.com to ex1@out.com.

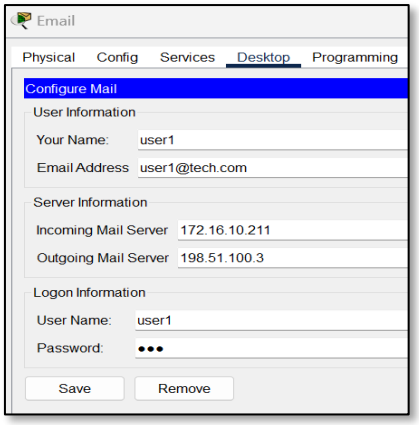

Figure 63. Setting the outgoing mail server address to the external email server.

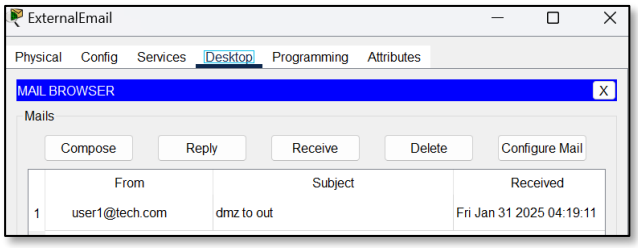

Figure 64. Successful receipt of email from user1@tech.com to ex1@out.com.

3.2.3 Inter-Subnet Access

According to the company's requirements, all employees, irrespective of department, require mostly full access to the network. Specifically, different departments must be able to communicate with each other, and all departments must access the FTP, Email, Web and DHCP servers to work efficiently. For example, the sales department needs access to the FTP server to access customer databases, while the finance department requires access to the financial database. All employees must also be able to communicate with the external network to allow internet usage. The only restriction is on the AAA server; only IT should access it for any required maintenance, increasing the server's security. This restriction was completed by adding an ACL on the main router. The ACL (Figure 65) restricts access to the host IP address 172.16.10.195 (AAA server's IP address) to only the IT department.

```
MainRouter>en
MainRouter#show ip access-list
Extended IP access list AAA-ACL
    10 permit ip 172.16.10.160 0.0.0.31 host 172.16.10.195
    20 deny ip any host 172.16.10.195
    30 permit ip any any
```

Figure 65. Creating AAA-ACL on the main router.

To verify this, a ping was initiated from Laptop11 (IT) and Laptop1 (Sales) to the AAA Server. Only the IT's ping was successful, indicating the restriction was applied (Figure 66-67).

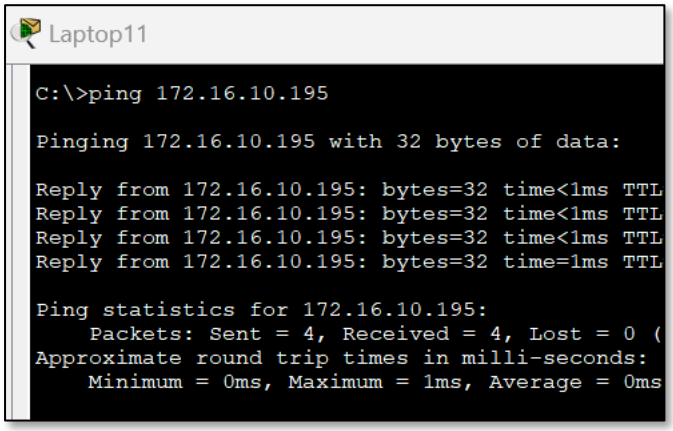

Figure 66. Pinging the AAA server from IT.

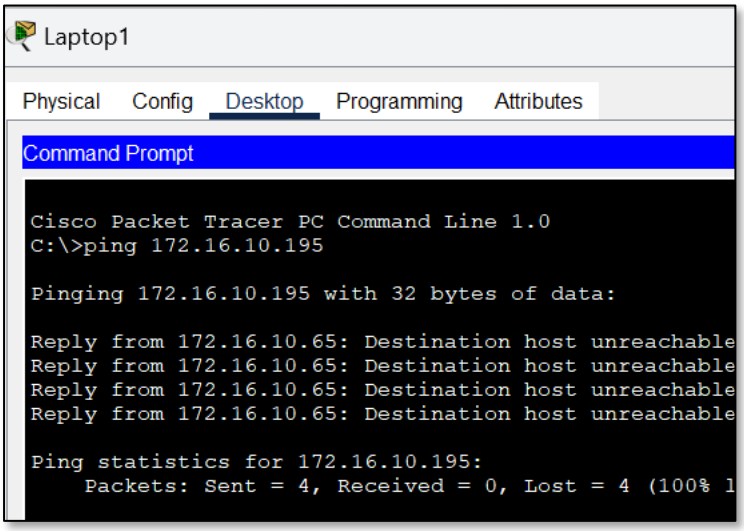

Figure 67. Pinging AAA server from Sales.

3.3 Advanced Security Configuration

3.3.1 Creating Remote branch

The company's internal network is connected to a remote branch office with 10 employees. This was simulated using an external router with two interfaces (Figure 68). The first connects to the remote branch and the second to the external network. The branch was assigned the random network address 175.16.10.0/24.

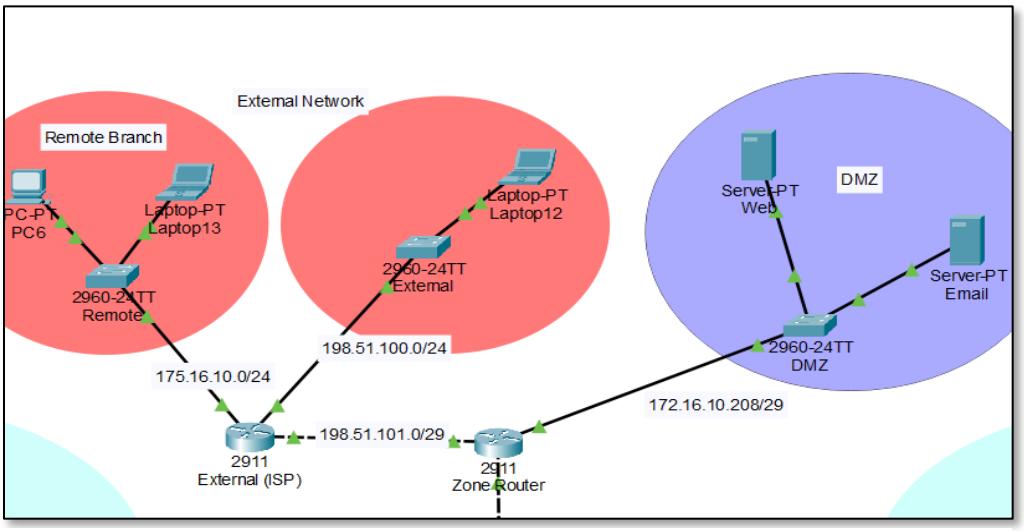

Figure 68. Initial Remote branch network design.

3.3.2 ACLs for Remote branch Access

Currently, the remote branch is handled as external traffic by the ZPFs. Unlike external traffic, the remote branch must access the FTP server (172.16.10.194) and receive emails from the internal mail server. These conditions were added to the previously configured ACLs (Figure 38).

Access to the email server was verified by sending/receiving emails from the internal email server on the remote branch (Figure 69-70).

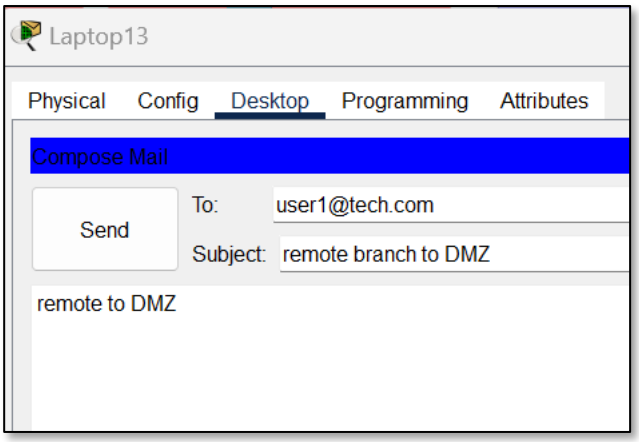

Figure 69. Sending an email from user2@tech.com to user1@tech.com on remote branch.

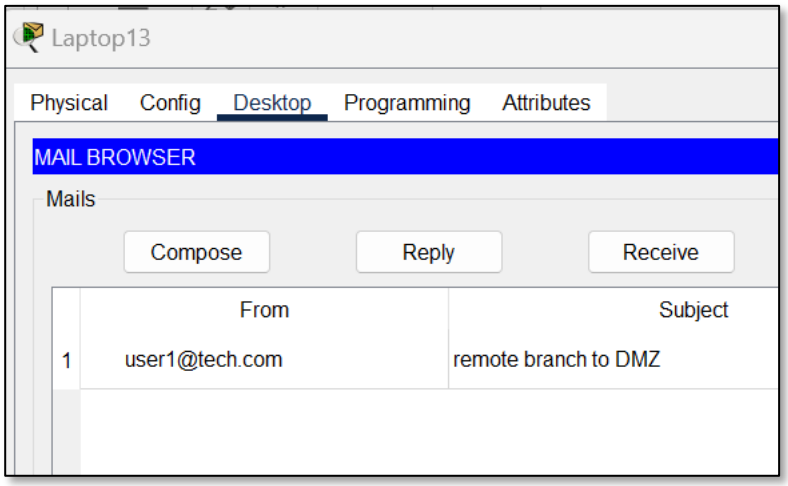

Figure 70. Successfully receiving the email on user1@tech.com on remote branch.

Access to the FTP server was verified by successfully establishing an FTP connection from the remote branch (Figure 71).

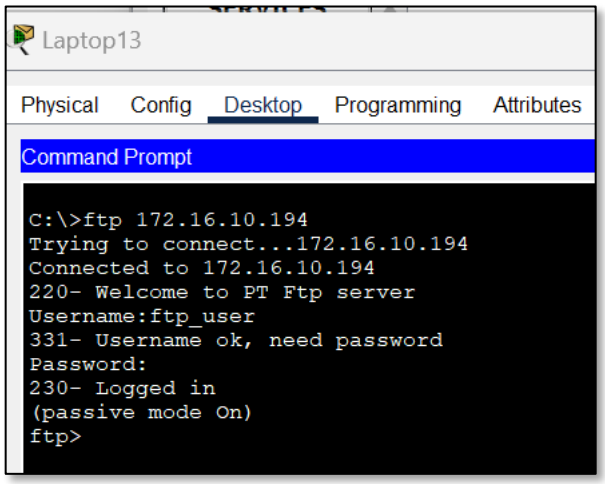

Figure 71. Remote branch (laptop13) successfully accessing internal FTP Server.

3.3.3 Configuring the VPN connection

Site-to-site VPN was configured between the remote branch and internal network. To configure the IPsec VPN, the topology was redesigned. An ISP router was added to connect the internal network to the remote branch and external network. The remote branch's router connects to the ISP router (Figure 72). The ISP router in turn connects to the internal zone (on the zone router), acting as a pass-through router for encrypted packets between the routers.

All the router-router connections were switched to serial connections, and OSPF routing was enabled. Dynamic routing was used because the VPNs conceal the source IP addresses, rendering static routing faulty.

VPN was configured on both the zone router and remote branch router. The access list designed captures all the traffic between the remote branch and internal zone. The ISAKMP (Phase 1) and IPsec (Phase 2) parameters were set on the remote and the zone router. This included setting up pre-shared key (**vpnpass**) and encryption to secure the connection (Figure 73,74). Crypto maps were applied on their respective interfaces to establish a secure VPN tunnel. Each router was set up as the other's peer to establish the connection.

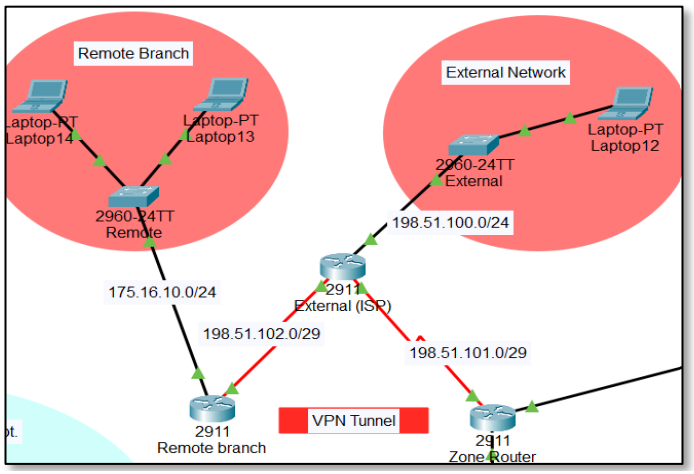

Figure 72. Network topology for site-to-site VPN connections between remote branch and internal network.

```
ZonesRouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ZonesRouter(config)#access-list 110 permit ip 172.16.10.0 0.0.0.255 175.16.10.0 0.0.0.255
ZonesRouter(config)#crypto isakmp policy 10
ZonesRouter(config-isakmp)#encryption aes 256
ZonesRouter(config-isakmp)#authentication pre-share
ZonesRouter(config-isakmp)#group 5
ZonesRouter(config-isakmp)#exit
ZonesRouter(config)#crypto isakmp key vpnpass address 198.51.102.2
ZonesRouter(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
ZonesRouter(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
ZonesRouter(config-crypto-map)#description VPN connection to R1
ZonesRouter(config-crypto-map)#set peer 198.51.102.2
ZonesRouter(config-crypto-map)#set transform-set VPN-SET
ZonesRouter(config-crypto-map)#match address 110
ZonesRouter(config-crypto-map)#exit
ZonesRouter(config)#interface s0/0/0
ZonesRouter(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
ZonesRouter(config-if)#
```

Figure 73. Configuring the VPN on the zone router.

```
Router#show access-list
Extended IP access list 110
    10 permit ip 175.16.10.0 0.0.0.255 172.16.10.0 0.0.0.255

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp key vpnpass address 198.51.101.1
Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Router(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#description VPN connection to R3
Router(config-crypto-map)#set peer 198.51.101.1
Router(config-crypto-map)#set transform-set VPN-SET
Router(config-crypto-map)#match address 110
Router(config-crypto-map)#exit
Router(config)#interface s0/0/0
Router(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#no crypto map VPN-MAP
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
Router(config-if)#exit
Router(config)#interface s0/0/1
Router(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#exit
```

Figure 74. Configuring the VPN on the remote branch's router.

VPN Verification

To verify the VPN was set up, an HTTP request was made from the remote branch (Laptop13) to the DMZ's web server. The command **show crypto ipsec sa** was used to verify the connection was successful (Figure 76). Figure 76 demonstrates packets passed from the remote branch, through the VPN tunnel, arriving at the DMZ (web server).

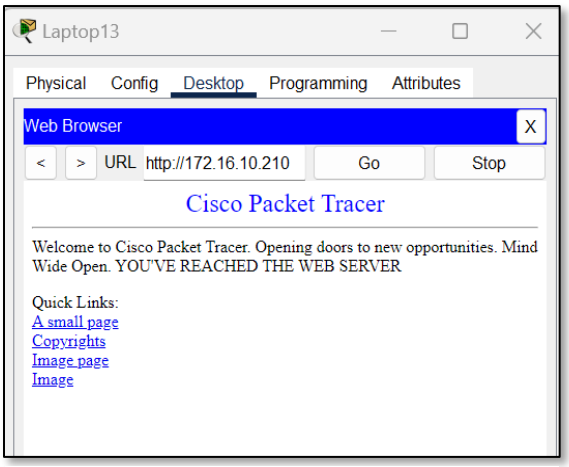

Figure 75. Sending HTTP request over the VPN connection from remote branch (Laptop13) to DMZ (web server).

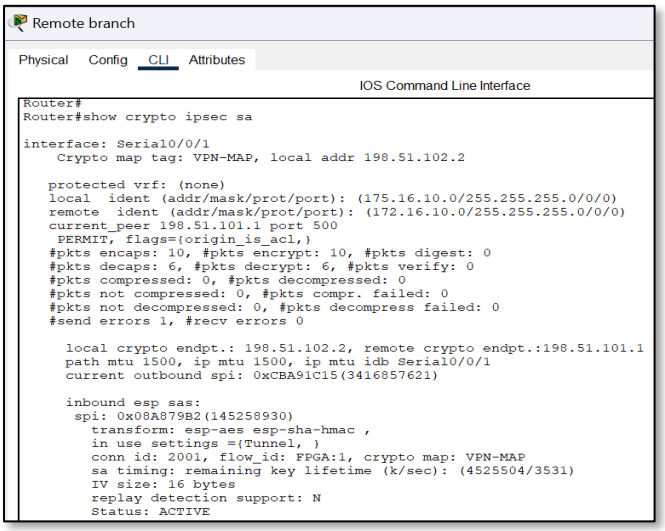

Figure 76. Results of the command show crypto ipsec sa on the remote branch's router.

Similarly, the remote branch could successfully access the FTP server, but devices from the external network could not (Figures 77-78).

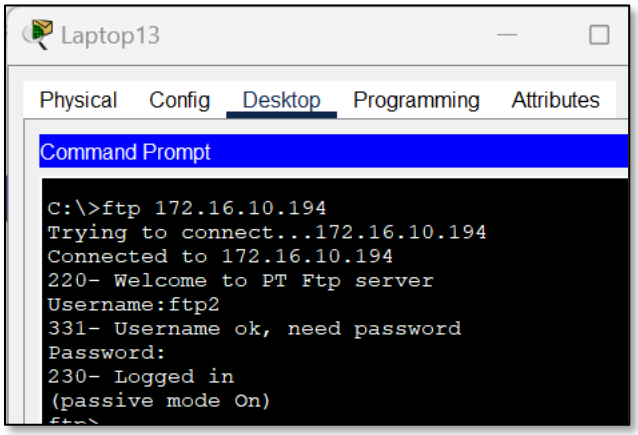

Figure 77. Successful request for FTP Server from remote branch (Laptop13).

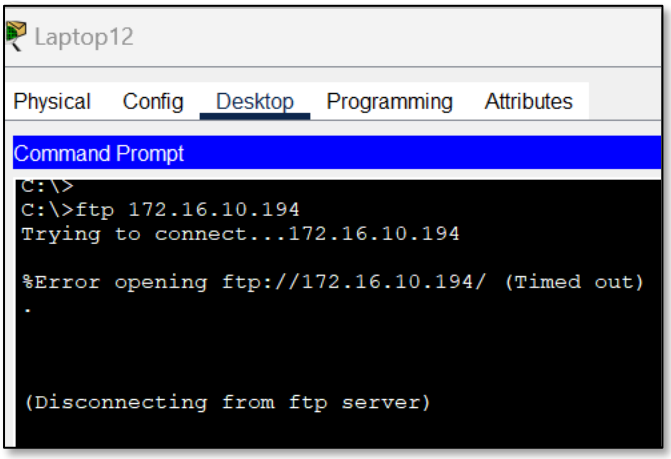

Figure 78. Failed request for FTP Server from external network (Laptop12).

3.3.4 Configuring the AAA server

A AAA server was configured to manage user authentication and authorization for network access (Figure 80). The AAA client is the Main Router, so an entry was created with the secret key secr and server type Tacacs (Figure 79). On the main router, AAA was configured on the console and vty. The remaining routers were externally facing, so AAA was not applied to them.

```
MainRouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MainRouter(config)#aaa new-model
MainRouter(config)#tacacs-server host 172.16.10.195
MainRouter(config)#tacacs-server key secr
MainRouter(config)#aaa authentication login default group tacacs+ local
MainRouter(config)#line console 0
MainRouter(config-line)#login authentication default
MainRouter(config-line)#exit
MainRouter(config)#line vty 0 4
MainRouter(config-line)#login authentication default
MainRouter(config-line)#exit
MainRouter(config)#exit
MainRouter#
```

Figure 79. Configuring AAA on the main router.

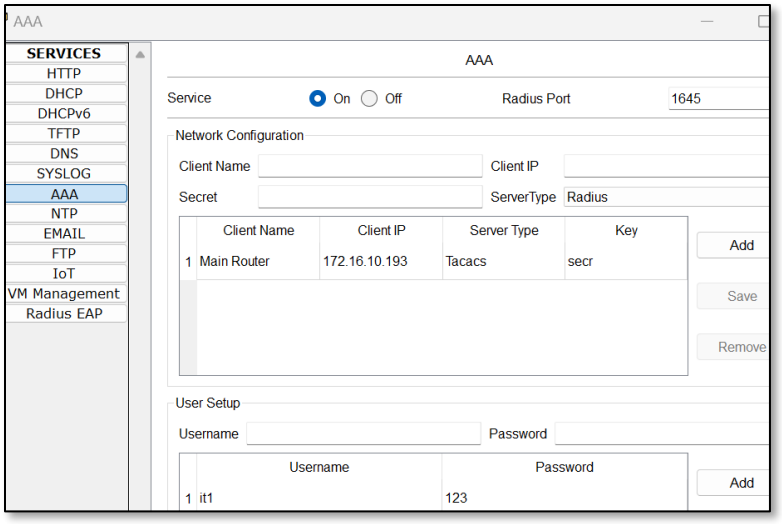

Figure 80. Setting up AAA server.

AAA Verification

The AAA was verified by accessing the main router and logging in with the **username it1** and **password 123** (Figure 81).

```
User Access Verification

Username: it1
Password:
MainRouter>
```

Figure 81. Using AAA to access the main router.

4. conclusion

This report outlines the proposed network topology for the company Tech Zolutions Inc. It divides the 150 employees into five departments, a conference room, and a server room. A remote branch simulation was also created to emulate the 10 remote employees. A DMZ was designed to allow external users access to public-facing resources, including the email and web server.

The proposed network topology was designed to support the company's functional needs. It also prioritized scalability, security, and efficiency. By implementing this design, the company can guarantee a reliable, high-performance network.