Cisco Packet Tracer Project

"Money"

By:

Shaul Kabla

Ran Atlas

**Table of Contents:**

* Introduction (Page 3)
* Company Background (Page 4)
* Company Structure (Page 5)
* Company Requirements (Page 6)
* Network Planning – Network Design (Page 7)
* Network Topology (Page 8)
* Implementation Steps (Page 9)
* Step 1: Basic Setting (Page 10)
* Step 2: Configure VLANs & Trunk (Page 12)
* Step 3: Port Security (Page 13)
* Step 4: IP Addressing (Page 14)
* Step 5: Configure OSPF (Page 15)
* Step 6: Configure Static IP (Page 16)
* Step 7: DHCP Server (Page 16)
* Step 8: Configure Inter-VLAN (Pages 16-17)
* Step 9: Configure Wireless Network (Page 17)
* Step 10: Configure Telephony (Page 18)
* Step 11: Configure ACL for SSH (Page 20)
* Step 12: PAT + ACL (Page 21)
* Step 13: Site-to-Site IPsec VPN (Page 22)
* Step 14: Configure Site-Server Router (Page 22)
* Summary (Page 23)
* Contact Information (Page 23)

**Introduction**

Greetings and welcome to the comprehensive project documentation for the transformation of the network infrastructure of "Money", a prominent financial institution. Within this document, you will have the opportunity to explore and gain insight into the meticulous planning, seamless implementation, and exceptional technical prowess utilized to fortify the backbone of this esteemed institution. As you delve further into the material, you will witness firsthand how I expertly navigated the intricate landscape of finance and technology to seamlessly align the institution's objectives with an innovative, efficient, and most importantly, secure network design.

It is my pleasure to extend to you a cordial invitation to engage in a comprehensive exploration of contemporary financial network architecture. This journey will commence from the initial stage of conceptualization and progress through to the final stage of execution. Our in-depth examination will cover various essential components, including VLAN configuration, the deployment of OSPF, and integration of VoIP. Together, we shall delve into the intricacies of this enlightening field and gain invaluable insights.

**Money: Forging a Financial Legacy**

Back in 2012, a financial institution with the name "Money" was established in the bustling city of Tel Aviv. The primary aim of this institution was to revolutionize and redefine the traditional finance sector by offering tailor-made solutions that cater to each client's unique needs and preferences. Furthermore, "Money" was committed to upholding the highest standards of excellence and integrity, which quickly earned the institution a reputation as a trustworthy brand that customers could rely on.

The institution's headquarters, a magnificent four-story building, became the epicenter of cutting-edge finance, where innovative ideas were born and strategic collaborations were forged. Over the years, "Money" achieved numerous significant milestones, including successful partnerships with third-party providers and the creation and deployment of its own powerful financial tools using the latest state-of-the-art technology. With a customer-centric approach and a focus on adaptability, "Money" continues to thrive, leading the way in finance innovation and setting the bar for excellence in the industry

**"Money" is not just a financial institution; it is a driving force of innovation. With growth, strategic partnerships, and advanced technology integration, "Money" redefines the future of finance, inspiring excellence and industry standards.**

**Company Structure:**

Money, a mid-size financial enterprise, was established in 2012. Its headquarters in Tel Aviv spans four floors to accommodate its operations.

**Headquarters (HQ):**

14th Floor:

* Department of Management
* Sales & Marketing Division
* Customer Service Unit

13th Floor:

* Human Resources Department
* Legal Management Team
* Accounts Division

12th Floor:

* Technology Development Hub
* Information Technology Department

11th Floor:

* Vibrant Trading Floor

In a progressive approach, Money works with third-party experts to manage and maintain its server room infrastructure. The company hosts a variety of servers, including DHCP, DNS, FTP, WEB & EMAIL servers, all of which are meticulously maintained. Notably, these servers operate with static IP addresses, enhancing stability and accessibility in the dynamic world of finance.

**Company Requirements:**

• Design Tool - Create a network topology using third-party software before implementation.

• Simulation Tool - Use Cisco Packet Tracer for network design implementation.

• Implement hierarchical network model to reduce network load.

• ISPs - Connect to 2 internet service providers: Bezeq and Partner, each router connecting to both.

• WIFI - Provide wireless network for each department.

• VoIP - Provide phone devices for communication between departments.

• VLAN - Each department should have its own VLAN and subnets.

• Basic Settings - Configure basic settings for devices: Hostname, Console Password, Device Password, Banner Message, Password Encryption, Disable IP-Domain Lookup.

• Inter-VLAN - Devices should communicate using Layer 3 switches and internal VLAN configuration.

• DHCP Server - Devices (excluding phones) will receive dynamic IP addresses from DHCP server located in the server farm.

• Routing Protocol - Use OSPF protocol for switches and routers.

• Port-Security - Configure Port-Security to allow only one computer to connect to its SwitchPort.

• SSH - Configure SSH for remote access.

• NAT+ACL – Configure PAT, define access lists.

• IPsec VPN + ACL – Establish IPsec VPN connection between main router and server farm with enforced access lists.

**• Test - Verify system functionality.**

**Network Planning – Network Design:**

The hierarchical topology model separates network functions into layers for stability and optimized performance. The core layer provides high-speed, reliable connectivity. The distribution layer forwards data and enforces security policies. The access layer provides connectivity and security for end-user devices.

**Core Layer:**

At the core layer, the main focus is to connect the internal network of the company with external resources such as internet service providers. The core layer ensures smooth communication between the organization's network and external entities by acting as a nexus for data aggregation and routing. The design of the core layer is aimed at high-speed, low-latency transmission and efficient data transfer. It is responsible for handling critical functions such as high-speed data switching, fault tolerance, and ensuring consistent availability.

**Distribution Layer:**

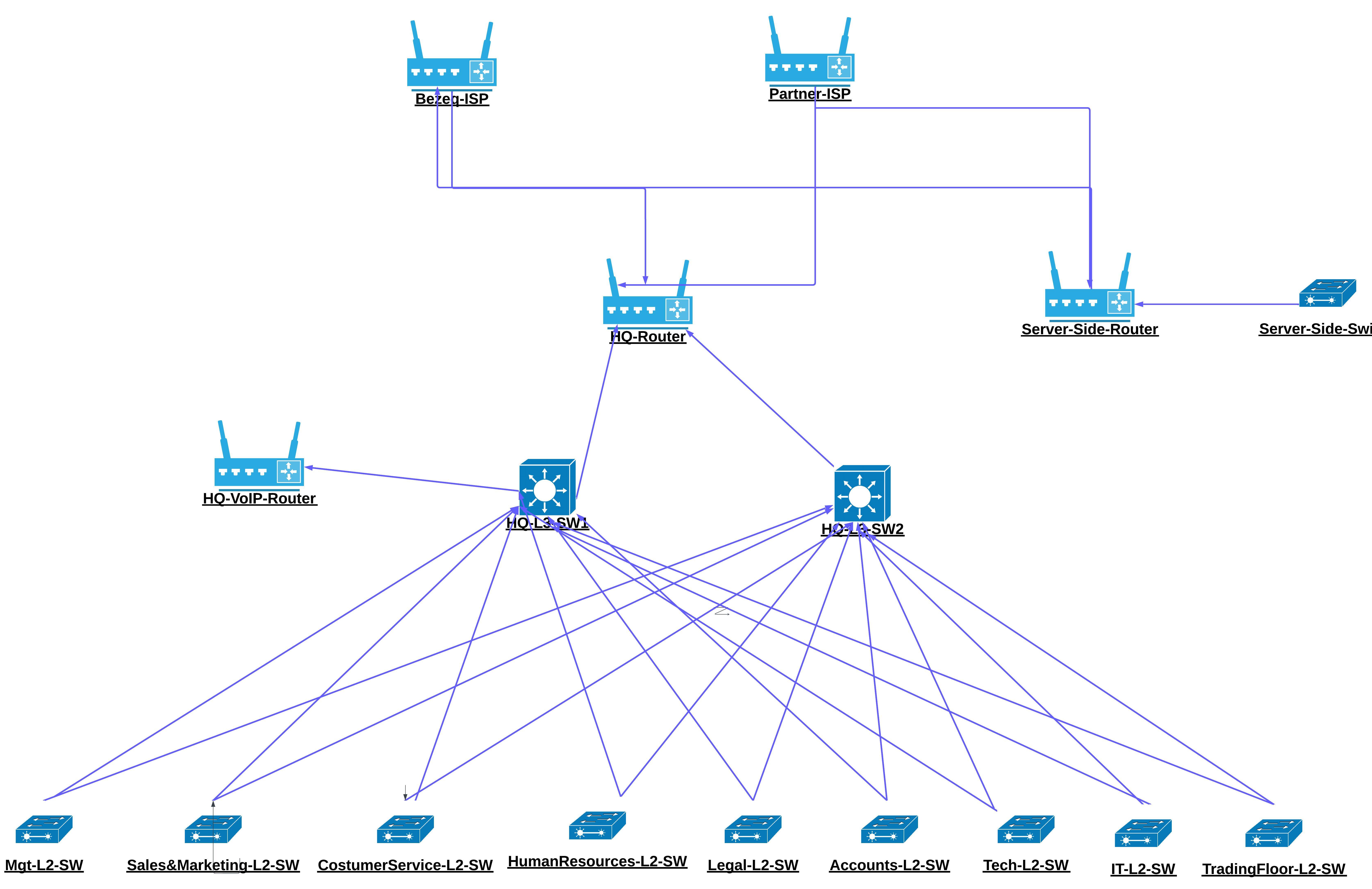
The distribution layer serves as a mediator between the core and access layers. It receives data from multiple access layer switches and efficiently forwards it to its intended destination, whether it is within the organization's internal network or external resources. This layer also plays a pivotal role in load balancing, effectively distributing network traffic to prevent congestion and bottlenecks. By managing the flow of data, the distribution layer enhances network performance and optimizes resource utilization. Additionally, it aids in enforcing security policies and facilitating inter-VLAN communication.

**Access Layer:**

The access layer is the point of entry for end-user devices and network resources. Its primary role is to provide connectivity and network access to various departments and devices within the organization. Access layer switches serve as the interface between end-user devices, such as computers and phones, and the underlying network infrastructure. This layer is responsible for implementing VLAN segmentation, allowing for efficient traffic management and enhancing security. Additionally, it enforces policies like port-security to regulate device connectivity, ensuring that only authorized devices can access the network. Through its configuration, the access layer guarantees a seamless and secure network experience for all users.

**Step 2: Network Topology**

**HQ Topology**



**CLI**

Order of action for TLV-HQ.

1. Basic setting to all devices + SSH on the routers and L3 switches
2. Configure VLANs(DATA&VOICE) + access and trunk ports on all the switches
3. Configure switchport security to server-side site dept.
4. Assign IP address
5. Configure OSPF on the routers and L3 switches
6. Assign a static IP address for server-site servers
7. Configure DHCP server – **DHCP Test**
8. Configure Inter-VLAN routing on L3 switches + IP DHCP helper addresses
9. Wireless network configurations
10. Telephony service configuration – **IP Addressing Test**
11. Standard ACL for SSH – Limit the access to IT dept only.
12. PAT + ACL
13. Site-to-site IPsec VPN + ACL

**Step 1: Basic Setting**

**Configure Access layer switches**

**enable**

**conf t**

**hostname "DeviceName"**

**enable password money**

**line console 0**

**password money**

**login**

**exit**

**banner motd #NO UNAUTHORISED ACCESS!!!#**

**no ip domain-lookup**

**service password-encryption**

**copy running-config startup-config**

**Step 1: Basic setting**

**Adding SSH to L3 switches**

**username money password money**

**ip domain-name money.com**

**crypto key generate rsa**

**1024**

**ip ssh version 2**

**line vty 0 15**

**login local**

**transport input ssh**

**exit**

**copy running-config startup-config**

**Step 2: Configure VLANs**

Configure VLANs for Departments. Voice VLAN will be 120.

**vlan "VLAN-NUMBER"**

**name "VLAN-NAME"**

**vlan 120**

**name VOICE**

**exit**

**interface range fa0/1-2**

**switchport mode trunk**

**exit**

**interface range fa0/3-24**

**switchport mode access**

**switchport access vlan "VLAN-NUMBER"**

**switchport voice vlan 120**

**exit**

**copy running-config startup-config**

**Step 2: Configure L3-SW Trunk**

Configure Trunk to all interfaces of the L3-SW except router interface.

**interface range gig 1/0/2-11(Or 10 for the other switch)**

**switchport mode trunk**

**exit**

**vlan 10**

**name MGT**

**vlan 20**

**name SM**

**vlan 30**

**name CS**

**vlan 40**

**name HR**

**vlan 50**

**name LM**

**vlan 60**

**name ACC**

**vlan 70**

**name TECH**

**vlan 80**

**name IT**

**vlan 90**

**name TF**

**vlan 120**

**name VOICE**

**exit**

**copy running-config startup-config**

**Step 3: Port-security**

Secure the access to the Servers + Closing unused ports

**interface range fa0/2-7**

**switchport mode access**

**switchport port-security**

**switchport port-security maximum 1**

**switchport port-security mac-address sticky**

**switchport port-security violation shutdown**

**exit**

**interface range fa0/8-24, gig0/1-2**

**switchport mode access**

**switchport access vlan 99**

**shutdown**

**exit**

**copy running-config startup-config**

**Step 4: IP Addressing to the interfaces**

Configure IP to each interface. (+1 from the last octet, Attention to not repeat IP address for used cable)

**Ip address "IP-Address" "Subnet mask"**

In L3-SW Configure **no switchport**

In the routers **clock rate 64000**

**Step 4: Configure sub-interfaces for VOICE VLAN**

Configure Sub-Interface with dot1Q on Voice router

**Interface fa0/0.120**

**Encapsulation dot1Q 120**

**Ip address 10.10.10.1 255.255.255.0**

**copy running-config startup-config**

**Step 5: Configure OSPF**

Configure OSPF protocol on L3 switches and routers – Important to enable IP-Routing for the L3 switches

**Ip routing**

Advertise networks foe each switch

**L3 method:**

**router ospf 10**

**router-id "Router-ID"**

**network 10.10.10.0 0.0.0.255 area 0**

**network 192.168.21.16 0.0.0.3 area 0**

**network 192.168.1.0 0.0.0.255 area 0**

**network 192.168.2.0 0.0.0.255 area 0**

**network 192.168.3.0 0.0.0.255 area 0**

**network 192.168.4.0 0.0.0.255 area 0**

**network 192.168.5.0 0.0.0.255 area 0**

**network 192.168.6.0 0.0.0.255 area 0**

**network 192.168.7.0 0.0.0.255 area 0**

**network 192.168.8.0 0.0.0.255 area 0**

**network 192.168.9.0 0.0.0.255 area 0**

**router method:**

**router ospf 10**

**router-id 4.4.4.4**

**network 192.168.21.16 0.0.0.3 area 0**

**network 192.168.21.20 0.0.0.3 area 0**

**network 192.200.100.0 0.0.0.3 area 0**

**network 192.200.100.4 0.0.0.3 area 0**

**copy running-config startup-config**

**Step 6: Configure static IP address for server-side room**

Ip configuration via GUI of the server

**Step 7: DHCP server configuration**

Creating pools via GUI of the server by the following method.

Default Gateway – Will be the first device of the netwrk

DNS Server – 192.168.21.6

Valid range hosts.

Subnet mask

Maximum number of users: 240

**Step 8: Configure Inter-VLANs on L3-SW**

Configure Inter-VLAN using sub-interfaces.

Assign IP address that based on the default gateway of the VLAN

**int vlan 10**

**ip add 192.168.1.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**int vlan 20**

**ip add 192.168.2.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**int vlan 30**

**ip add 192.168.3.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**int vlan 40**

**ip add 192.168.4.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**int vlan 50**

**ip add 192.168.5.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**int vlan 60**

**ip add 192.168.6.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**int vlan 70**

**ip add 192.168.7.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**int vlan 80**

**ip add 192.168.8.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**int vlan 90**

**ip add 192.168.9.1 255.255.255.0**

**ip helper-address 192.168.21.5**

**copy running-config startup-config**

**Step 9: Configure Wireless network**

GUI configuration with SSID & Password

**Step 10: Configure Telephony**

Creating a pool for voice on HQ-VoIP

**service dhcp**

**ip dhcp pool VOICE**

**network 10.10.10.0 255.255.255.0**

**default-router 10.10.10.1**

**option 150 ip 10.10.10.1**

**dns-server 10.10.10.1**

**ip dhcp excluded-address 10.10.10.1**

**telephony-service**

**max-ephones 20**

**max-dn 20**

**ip source-address 10.10.10.1 port 2000**

**auto assign 1 to 20**

**ephone-dn 1**

**number 401**

**ephone-dn 2**

**number 402**

**ephone-dn 3**

**number 403**

**ephone-dn 4**

**number 404**

**ephone-dn 5**

**number 405**

**ephone-dn 6**

**number 406**

**ephone-dn 7**

**number 407**

**ephone-dn 8**

**number 408**

**ephone-dn 9**

**number 409**

**ephone-dn 10**

**number 410**

**ephone-dn 11**

**number 411**

**ephone-dn 12**

**number 412**

**ephone-dn 13**

**number 413**

**ephone-dn 14**

**number 414**

**ephone-dn 15**

**number 415**

**ephone-dn 16**

**number 416**

**ephone-dn 17**

**number 417**

**ephone-dn 18**

**number 417**

**ex**

**copy running-config startup-config**

**Step 11: Configure ACL for SSH**

Deny access to all L3&Routers from any network that not belong to IT

**access-list 10 permit 192.168.8.0 0.0.0.255**

**access-list 10 deny any**

**line vty 0 15**

**access-class 10 in**

**exit**

**copy running-config startup-config**

**Step 12: PAT+ACL**

Configure NAT that include the entire local network

Inside NAT – HQ-Router

**int range gig0/0-1**

**ip nat inside**

**exit**

Outside NAT – HQ-Router

**int se0/3/0**

**ip nat outside**

**exit**

**int se0/3/1**

**ip nat outside**

**exit**

**access-list 50 remark Allow traffic from 192.168.1.0/24 to 192.168.9.0/24**

**access-list 50 permit 192.168.0.0 0.0.255.255**

**ip nat inside source list 50 interface se0/3/0 overload**

**ip nat inside source list 50 interface se0/3/1 overload**

**copy running-config startup-config**

**Step 13: Site-to-site IPsec VPN**

To encrypt all the data between the network to the server room

**Active securityk9**

**license boot module c2900 technology-package securityk9**

To create the IPsec VPN in HQ-Router

**access-list 110 remark Allow traffic from 192.168.1.0/24 to 192.168.9.0/24 summarized**

**access-list 110 permit ip 192.168.0.0 0.0.248.255 192.168.21.0 0.0.0.15**

**crypto isakmp policy 10**

**encryption aes 256**

**authentication pre-share**

**group 5**

**exit**

**crypto isakmp key vpnpa55 address 190.200.100.9**

**crypto IPsec transform-set VPN-SET esp-aes esp-sha-hmac**

**crypto map VPN-MAP 10 ipsec-isakmp**

**description VPN connection to SERVERSIDE-SITE**

**set peer 190.200.100.9**

**set transform-set VPN-SET**

**match address 110**

**exit**

**interface Se0/3/0**

**crypto map VPN-MAP**

**exit**

**Step 14: Configure site-server router**

**access-list 110 remark Allow traffic from 192.168.1.0/24 to 192.168.9.0/24 summarized**

**access-list 110 permit ip 192.168.21.0 0.0.0.15 192.168.0.0 0.0.248.255**

**crypto isakmp policy 10**

**encryption aes 256**

**authentication pre-share**

**group 5**

**exit**

**crypto isakmp key vpnpa55 address 190.200.100.1**

**crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

**crypto map VPN-MAP 10 ipsec-isakmp**

**description VPN connection to HQ-NETWORK**

**set peer 190.200.100.9**

**set transform-set VPN-SET**

**match address 110**

**exit**

**interface Se0/3/0**

**crypto map VPN-MAP**

**exit**

**Project Summary: "Money" Network Infrastructure Enhancement**

**My experience from this project has influenced my approach to future projects, demonstrating my capacity for innovation, strategic planning, and driving transformative changes in the Cybersecurity sector.**

**Thank You for Joining Me in Crafting "Money's" Network.**

**If you have any questions, feel free to contact me:**

**Shaul Kabla**

**Cybersecurity Student - PT**

**Junior**

**Lin:** [**https://www.linkedin.com/in/shaul-kabla/**](https://www.linkedin.com/in/shaul-kabla/)

**Phone: 052-314-4774**

**Email: Shaulk001@gmail.com**

**I am eager to utilize my expertise and abilities in the realm of cybersecurity to drive forward advancements and achievements.**