Network and Internet Security (95-978)
Final Project

Background

A privately-held company is facing severe challenges in securing the company network. There is low awareness of computer security measures that should be employed by staff and managers, and the IT helpdesk (which is the first layer of response to security incidents) is understaffed and under-skilled to deal with the issues being reported. The CIO has shared the challenges that the company has been facing. In addition to the phishing attempts, the department has other issues such as a lack of skill and knowledge which resulted in a failed external audit. We are tasked with redesigning of the company's network as the first step to
securing their environment. We have a budget of $65,000 for this project.

Organizational Structure

There are several departments with users: Marketing, Sales, HR, Executives, Accounting, IT (Systems) – Privileged users
New Addition: R&D Department

Existing Network Design

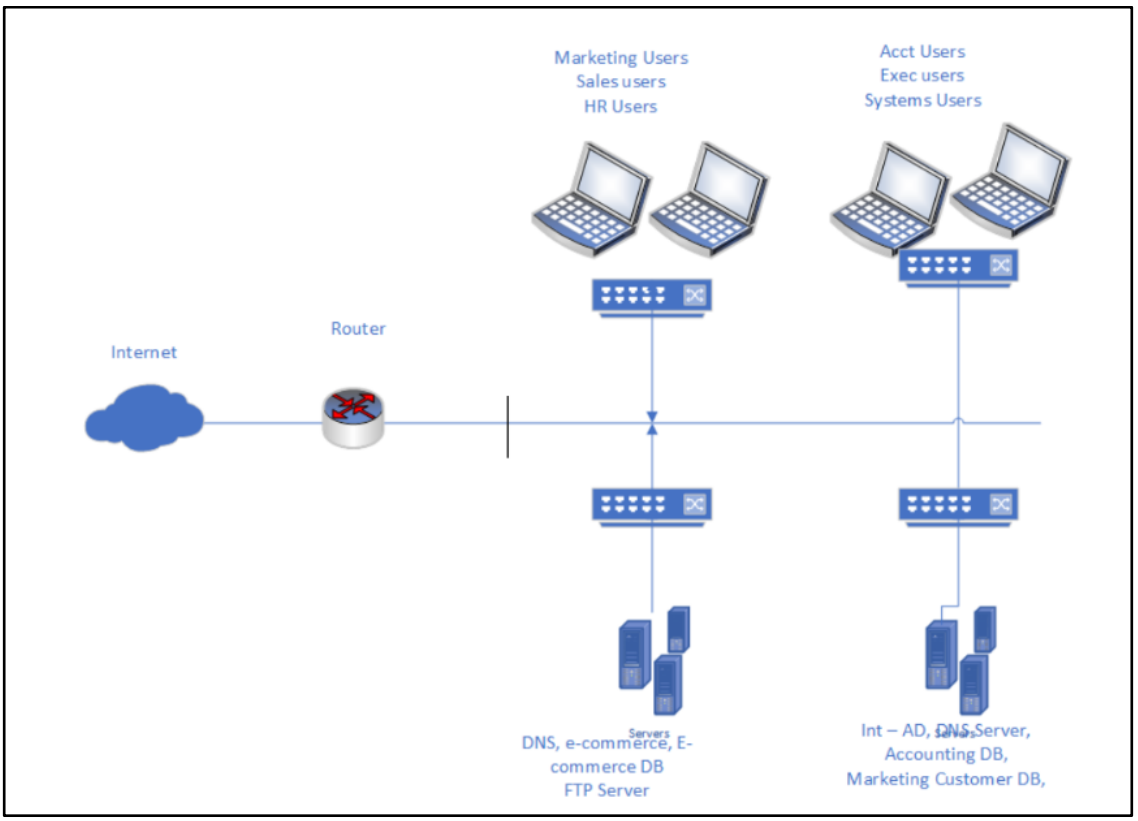

Image 1: The existing network diagram of the company

Technical information about the current network

- The assigned public IP network is 204.130.145.0/24
- Internal addresses are public IP network 38.25.128.0/24
- The Internal network will need to be in the RFC 1918 address space
- The company has 180 host systems (Note: for purposes of the assignment, you can allocate the host systems as you feel appropriate across the various departments/divisions of the company, including how you want to deploy the workstations used by the IT department and its privileged users.)
- The company uses testcorp.local as its Microsoft Windows domain
- The company uses testcorp.com as its public domain
- There is a need to install a new R & D division as part of the new network design.
- The organization has several public-facing servers:
    - Web servers (E-commerce)
    - Web connects to the E-commerce DB for appropriate lookups
    - DNS
    - FTP

- The organization has several internal use servers:
    - AD/DNS and DHCP Servers
    - Marketing DB
    - Accounting DB

Challenges with the Design

- A lack of network border security. Configuring a firewall and adding effective rules
- Internal IP addresses are routable. Need for RFC 1918 IP address configuration
- A lack of network and VLAN segregation
- No security devices within the internal network
- Internal servers, AD/DNS/DHCP services are routable
- No visible wireless infrastructure
- Using FTP instead of SFTP

Recommended Design

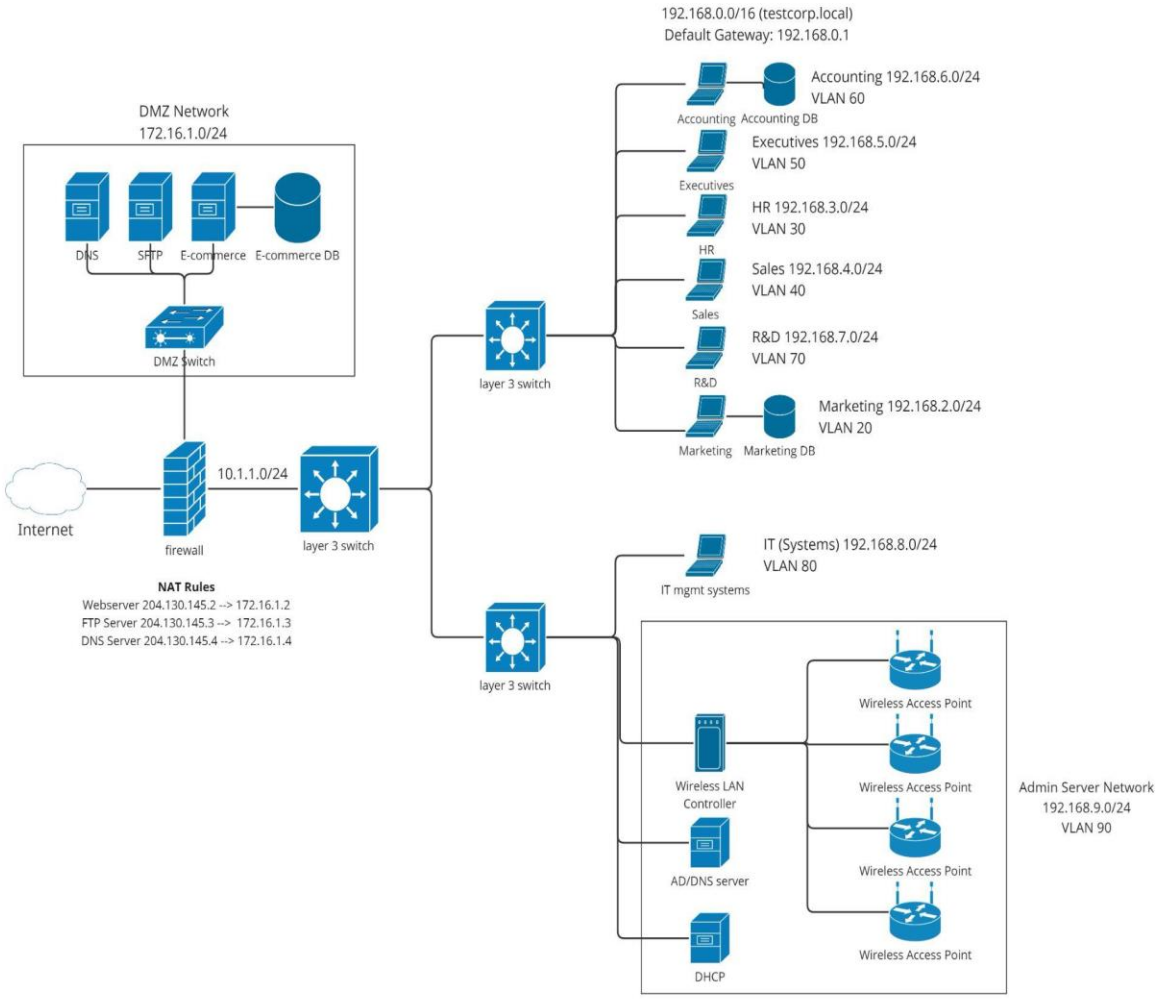

Image 2: The recommended network diagram of the company

Link to the diagram: https://miro.com/app/board/uXjVMPq2xhg=/

VLAN Configuration

To segregate traffic, we separate the internal network into department-specific Virtual LANs or VLANs. This would prevent inter-routability unless configures as well as helps us separate the IT and administration networks. The table below shows the configurations.

Department	IP Address	VLAN
Marketing	192.168.2.0	VLAN20
Sales	192.168.4.0	VLAN40
HR	192.168.3.0	VLAN30
Executives	192.168.5.0	VLAN50
Accounting	192.168.6.0	VLAN60
IT (Systems) – Privileged users	192.168.8.0	VLAN80
R&D	192.168.7.0	VLAN70
Admin Server Network	192.168.9.0	VLAN 90

Table 1: Department-wise VLAN Configuration

IP Address Scheme

External Network:

We have been allocated the public IP address space of 204.130.145.0/24

We assume that the public-facing servers have the following IP addresses:

Webserver 204.130.145.2

FTP Server 204.130.145.3

DNS Server 204.130.145.4

DMZ Network:

The DMZ is “a perimeter network”[1] that contains public-facing servers. It protects the hosts deployed in it from untrusted network traffic by adding an extra layer of security between the servers and the internet as well as between the servers and the internal network. The DMZ network would be allocated an internal IP address space of 172.16.1.0/24.

The Network Address Translation would map the public IP addresses of these servers to their internal ones. They are as follows:

Webserver 172.16.1.2
FTP Server 172.16.1.3
DNS Server 172.16.1.4
EcommerceDB 172.16.1.5 (No public-facing IP)

Firewall to Layer3Switch1 Network: 10.1.1.0/24

Internal Network:

The internal network would have an address space of 192.168.0.0/16. It is further subnetted according to departments as is shown in Table 1. Separate networks for IT management services and administration networks are created.

NAT Boundaries

The Network Address Translation is a way to map internal IP addresses to public-facing IP addresses[2]. We use this technology to configure a DMZ (Demilitarized Zone) in the network.

Static Rules
Webserver 204.130.145.2 --> 172.16.1.2
FTP Server 204.130.145.3 --> 172.16.1.3
DNS Server 204.130.145.4 --> 172.16.1.4

Dynamic Rules
For the internal network to connect to the internet
204.130.145.10 <--> 192.168.0.0/16

DHCP Addressing

The VLANs have the following DHCP configurations. Their address pools correspond to the IP address scheme specified in Table 1.

1. VLAN20: Marketing
    - DHCP enabled
2. VLAN30: HR
    - DHCP enabled
3. VLAN40: Sales
    - DHCP enabled
4. VLAN50: Executives
    - DHCP enabled
5. VLAN60: Accounting
    - DHCP enabled
6. VLAN70: R&D

    - DHCP enabled
7. VLAN80: IT systems, administration systems, wireless, etc.
    - No DHCP, static addressing

DNS Architecture

The DNS architecture for this network has been segregated as per the internal and external network's requirements. The external DNS only needs to hold the records of the public-facing servers - web and FTP. The internal network will hold the records for all the department-specific databases as well as the administration servers such as the DHCP and Active Directory (with the Domain Controller).

Internal

Server Name: dc.testcorp.local
Domain: testcorp.local

Name	Type	Data
dc.testcorp.local	A	192.168.9.2
dhcp.testcorp.local	A	192.168.9.3
marketing.testcorp.local	A	192.168.2.100
accounting.testcorp.local	A	192.168.6.100
rnd.testcorp.local	A	192.168.7.100

Table 2: Internal DNS Records

External

DNS Server Name: dc.testcorp.com
Domain: testcorp.com

Name	Type	Data
testcorp.com	A	204.130.145.2
ftp.testcorp.com	A	204.130.145.3

Table 3: External DNS Records

Network Management and Helpdesk Stations

Network management and helpdesk stations are critical components of an organization's IT infrastructure.

- Strong Authentication: Use complex passwords, and multi-factor authentication to access servers and resources. To manage accounts and enforce password policies implement authentication servers like Active Directory and delpoy multi-factor authentication.
- Privileged Management: Implement RBAC and ABAC to ensure privileged users can access to the specific resources they are allowed and monitor and audit their activities, Deploying privileged access management solutions to manage and monitor privileged user acess
- Limit Access: Limit access to servers and resources to the necessary users and provide access on need-to-know basis
- Security Audits: Perform regular audits to identify vulnerabilities to address them
- User Awareness Training: Provide training to all users and especially users who have privileged access to educate them on security best practices and the importance of secure network
- Patching: Keep all software and systems up-to-date with latest security patches and to keep them secure
- Encryption: Implement TLS or SSL to secure data at transit and at rest to protect against data from unauthorized access

Firewall Rules

1. Allow HTTP (port 80) and HTTPS (port 443) traffic from all VLANs to the internet for general web browsing.
Reason: To enable users to access the internet for work-related tasks.

2. Allow DNS (port 53) traffic from all VLANs to the internet.
Reason: To allow users to resolve domain names.

3. Allow SSH (port 22) traffic from the IT (Systems) VLAN (VLAN80) to all other VLANs.
Reason: To enable IT administrators to remotely manage and troubleshoot network devices.

4. Allow RDP (port 3389) traffic from the IT (Systems) VLAN (VLAN80) to all other VLANs.
Reason: To enable IT administrators to remotely access and manage user workstations.

5. Allow SMB (port 445) traffic within the Marketing (VLAN20), Sales (VLAN40), HR (VLAN30), Executives (VLAN50), Accounting (VLAN60), and R&D (VLAN70) VLANs.

Reason: To enable file sharing within each department.

6. Allow SMB (port 445) traffic from the IT (Systems) VLAN (VLAN80) to all other VLANs.

Reason: To enable IT administrators to manage shared files and resources.

7. Allow access to an intranet web server on port 8080 from all VLANs.

Reason: To provide access to an internal company portal or knowledge base.

8. Allow VoIP (port range 5060-5061) traffic within and between all VLANs.

Reason: To enable voice communication within the organization.

9. Allow access to a VPN server on port 1194 from all VLANs to the IT (Systems) VLAN (VLAN80).

Reason: To enable secure remote access for authorized users.

10. Allow access to a network monitoring tool on port 3000 from the IT (Systems) VLAN (VLAN80) to all other VLANs.

Reason: To enable IT administrators to monitor network performance and troubleshoot issues.

11. Allow traffic from wireless access points (WAPs) to the internet on TCP ports 80, 443, and 53.

Reason: This rule allows WAPs to access the internet for legitimate business purposes, such as providing wireless connectivity for employees and guests. Restricting access to only necessary ports (HTTP, HTTPS, DNS) helps to minimize the attack surface and reduce the risk of unauthorized access.

12. Deny all other traffic not mentioned above.

Reason: To secure network by preventing any other communication that does not fall under given firewall rules

Hardware

Most hardware selections come from Cisco's catalogue, both for Cisco's reputation as a reliable network device provider and for Cisco's support options. Below are our device selections and pricing.

- Firewall
  - 1x Cisco FirePOWER 1140 Next-Generation Firewall
    - Requires 1x Cisco Secure Firewall Small Business Edition 3-year license
    - 3.3Gbps throughput w/ full security, reasonable for number of users
    - Built-in threat screening, intrusion prevention system, and standard enterprise firewall services (URL blocking, etc.)
- Layer 3 Switches
  - 2x Cisco Catalyst 9300 24-port
    - Support layer 2 and layer 3 traffic
    - Stackable, easy expansion
    - One 24-port switch at network boundary, other connecting management networks/VLANs to internal network
  - 2x Cisco Catalyst 9300 48-port
    - Support layer 2 and layer 3 traffic
    - Stackable, easy expansion
    - 48-port switches stacked (96 ports total) and used for user VLANs
  - 3x Cisco Digital Network Architecture Essentials - Term License (3 years)
- Wireless LAN
  - 1x Cisco Catalyst 9800-L Wireless Controller
    - Manage WiFi security and availability
  - 4x Cisco Catalyst 9105AXI Wireless Access Point
    - Requires 4x Cisco DNA 3-year license
- Intrusion Prevention System
  - 3x Juniper Networks Intrusion Prevention System - subscription license (1 year)
    - IPS monitoring at multiple points in the network
    - Configured on existing hardware

Software

There are no extra softwares (open source or proprietary) that need to be installed in the proposed architecture.

FTP can be shifted to SFTP on the public-facing server. Considering we are using a domain certificate for HTTPS connections, we can use the same certificate to encrypt our FTP data.

Purchasing Costs

Device	Specific Product Name	Count	Price for each item	Link to the site where the device can be purchased
Firewall	Cisco FirePOWER 1140 Next-Generation Firewall - firewall	1	$4,014.99	https://www.cdw.com/product/cisco-firepower-1140-next-generation-firewall-firewall/5617299?pfm=srh
Layer3 Switch	Cisco Catalyst 9300 - switch - 24 ports - managed - rack-mountable	2	$5,319.99	https://www.cdw.com/product/cisco-catalyst-9300-switch-24-ports-managed-rack-mountable/6192817?pfm=srh
	Cisco Catalyst 9300 - Network Essentials - switch - 48 ports - managed - rack-mountable	2	$6,939.99	https://www.cdw.com/product/cisco-catalyst-9300-network-essentials-switch-48-ports-managed/4696730?pfm=srh
Wireless access points	Cisco Catalyst 9105AXI - wireless access point - Bluetooth, Wi-Fi 6	4	$369.99	https://www.cdw.com/product/cisco-catalyst-9105axi-wireless-access-point-bluetooth-wi-fi-6/6418290?pfm=srh
IPS	Juniper Networks Intrusion Prevention System - subscription license (1 year) - 1 gateway	3	$772.99	https://www.cdw.com/product/juniper-networks-intrusion-prevention-system-subscription-license-1-year/4082746?pfm=srh
Wireless controller	Cisco Catalyst 9800-L Wireless Controller - network management device - Wi-Fi 6	1	$6076.99	https://www.cdw.com/product/cisco-catalyst-9800-l-wireless-controller-network-management-device-wi/5777697?pfm=srh
Wireless Licenses	Cisco DNA 3-year license	4	$441.99	https://www.cdw.com/product/c

				isco-digital-network-architecture-advantage-term-license-3-year/4933912
Warranty/Service Agreement	Cisco SMARTnet extended service agreement (For all the hardware)	9	$269.99	https://www.cdw.com/product/cisco-smartnet-extended-service-agreement/7204646?pfm=srh
Firewall License	Cisco Secure Firewall Small Business Edition - subscription license (3 years) - 1 license	1	$1,618.93	https://www.cdwg.com/product/cisco-secure-firewall-small-business-edition-subscription-license-3-year/6404781
Switch License	Cisco Digital Network Architecture Essentials - Term License (3 years) - 48 ports	3	$849.99	https://www.cdw.com/product/cisco-digital-network-architecture-essentials-term-license-3-year/4696735
TOTAL			$46,777.64	

Table 4: Purchasing Costs

References

[1]https://www.fortinet.com/resources/cyberglossary/what-is-dmz
[2]https://www.comptia.org/content/guides/what-is-network-address-translation
https://learn.microsoft.com/en-us/windows-server/networking/technologies/ipam/add-a-dns-resource-record

END OF DOCUMENT