Azure SaaS/PaaS
Zero-Trust Topology

Christina James

Objective: Design secure physical and logical network architectures for wired and wireless networks.

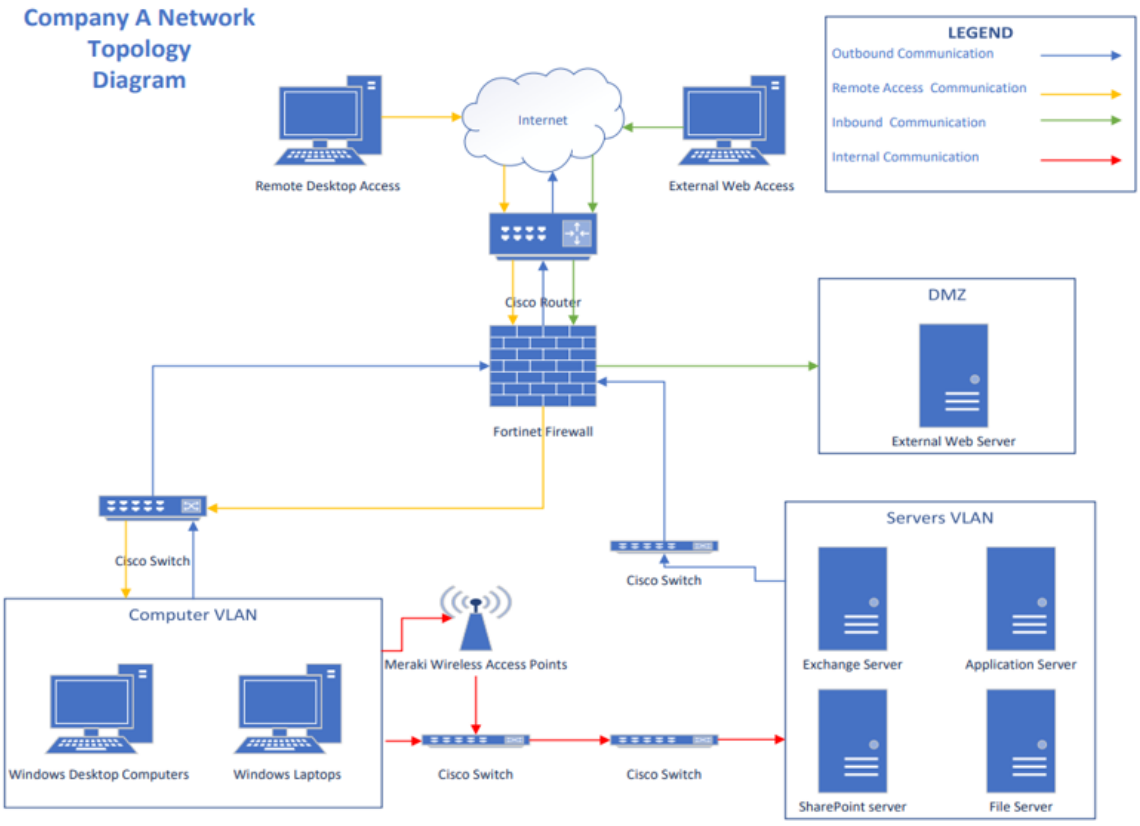
Scenario: You are the cybersecurity professional for Company A and are responsible for protecting the information of the company. Your roles include managing the company's cybersecurity capabilities and tools, conducting vulnerability management, and assessing risk to sensitive information. Company A has recently purchased Company B and wants to merge both networks.

Executives of Company A have tasked you with making risk-based decisions on integrating Company B's network with Company A's existing network. Company B has provided its latest vulnerability scans, network diagrams, and existing cybersecurity capabilities and tools. As a deliverable to the executives, you will submit your recommendations for a secure network design that merges the two networks and allows remote access for employees of both companies in the form of a merger and implementation plan.

For this project, you will use the above given scenario and the following supporting diagrams and analyses to complete your network merger and implementation plan:

Company A is a global company based in the United States that operates in the financial industry. Company A serves its customers with financial products, such as checking accounts, bank cards, and investment products. Company A has recently acquired Company B and needs to integrate with or remove similar capabilities and tools from Company B. Company B is smaller in size, has no dedicated cybersecurity professional role, and utilizes third-party support for infrastructure needs. Company B offers specialized software to medical providers and accepts credit cards as a payment option.

The executives of the newly merged company have expressed interest in integrating the use of the cloud to allow for scalability and redundancy. As the security professional of the merged networks, you are tasked with creating a secure network design that includes the use of zero trust principles and that utilizes both on-premises and cloud infrastructure. You also have been tasked with ensuring compliance with all regulatory requirements of the merged company, along with utilizing cloud-based technologies to provide security capabilities. Company executives have provided a budget of $50,000 in the first year to create a secure network design to utilize cloud-based services.



Company A Risk Analysis

Company A performed an internal risk analysis in anticipation of system integration with Company B. This risk analysis was performed in accordance with NIST SP 800-30 Rev 1 to identify the following:

- vulnerabilities
- risk likelihood

Table A. Risk Classifications

Risk Level	Description
High	The loss of confidentiality, integrity, or availability may be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The loss of confidentiality, integrity, or availability may be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	The loss of confidentiality, integrity, or availability may be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Table B. Data Sensitivity

Type of Data	Sensitivity		
	Confidentiality	Integrity	Availability

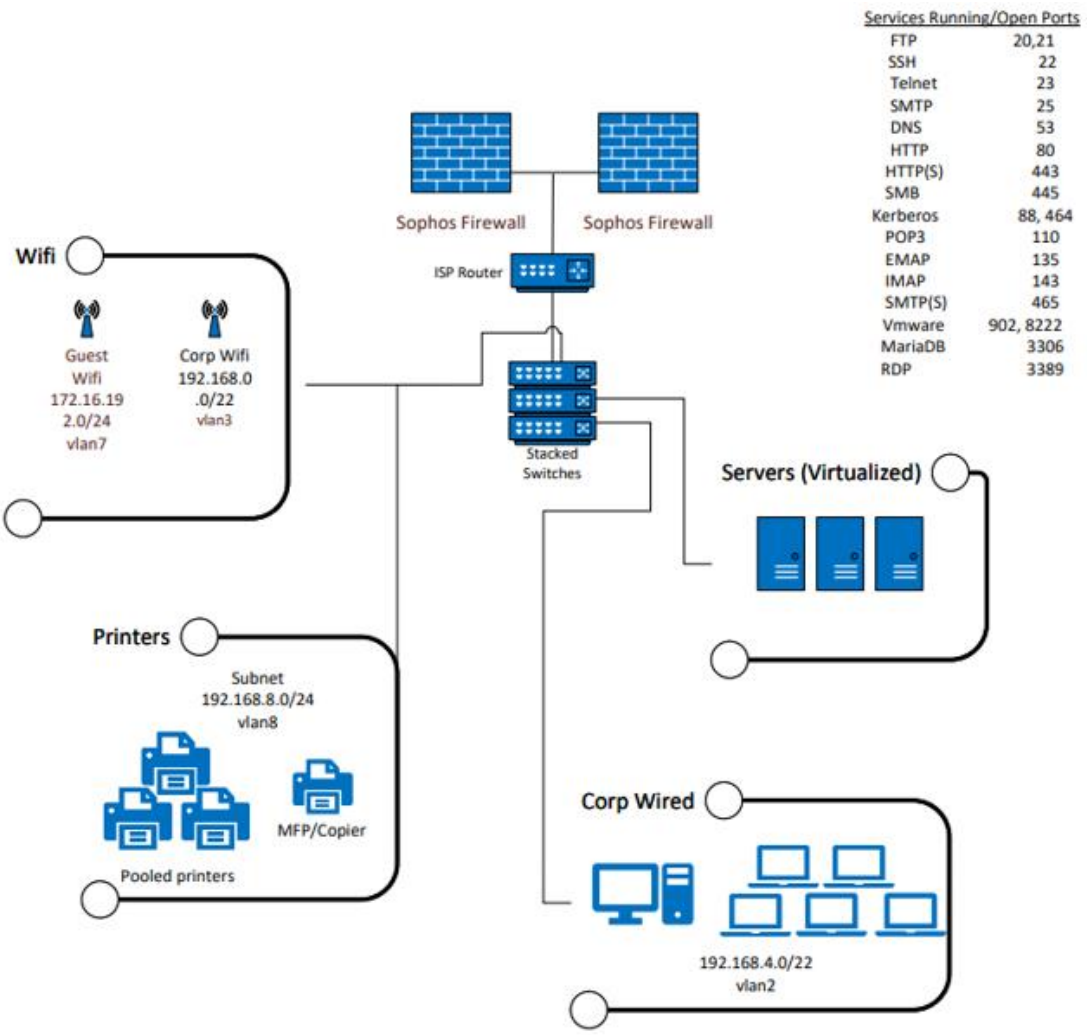
Customer PII (e.g., Account Numbers, Social Security Numbers, and Phone Numbers)	High	High	Moderate
Employee PII (e.g., Social Security Numbers and Employee Identification Numbers)	High	High	Moderate
Company intellectual property (e.g., credit scoring calculations)	High	High	Moderate
Marketing and advertising	Moderate	Moderate	Low

Table C. System Inventory

System Components	
Servers	Windows server 2019; role: internal SharePoint server Windows server 2019; role: Exchange server Windows server 2012; role: Application server Windows server 2012R2; File server DMZ Windows server 2012; role: FTP and external Web Server
Workstations	75 - Windows 10 Pro 20 - configured for remote desktop access
Switches	4 - Cisco 3750X
Firewall	Fortinet's Fortigate 800D NGFW
Border router	Cisco 7600
Laptops	14 - Windows 7 6 - Windows 11
Wireless Access Points	2 - Meraki MR28
Cable plant	Cat5e

Table D. Risk Identification

Risk #	**Vulnerability**	**Risk Likelihood**
1	Open ports 21-90, 3389	High
2	All users use eight-character passwords	High
3	User accounts no longer required are not removed	Moderate
4	All users have local administrative privileges	Moderate
5	Regular password changes are not enforced	Moderate
6	End-of-Life Equipment in use	Low



Company B Vulnerability Report

Company B performed this vulnerability assessment in anticipation of system integration with Company A. This assessment was performed by a qualified third-party assessor, and this report has been generated with the results. This assessment was performed in accordance with a methodology described in NIST 800-30 Rev 1 to identify the following:

- Vulnerabilities using the CVSS model
- Severity
- Likelihood of occurrence

Table A. Risk Classifications

Risk Level	Description
High	The loss of confidentiality, integrity, or availability may be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The loss of confidentiality, integrity, or availability may be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	The loss of confidentiality, integrity, or availability may be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Table B. Severity

Severity Level (CVSS Model)	Description
Critical	• Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. • Exploitation is usually straightforward in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims and does not need to persuade a target user, for example, via social engineering, to perform any special functions.
High	• The vulnerability is difficult to exploit. • Exploitation could result in elevated privileges. • Exploitation could result in significant data loss or downtime.
Medium	• Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. • Denial of service vulnerabilities that are difficult to set up. • Exploits that require an attacker to reside on the same local network as the victim. • Vulnerabilities where exploitation provides only very limited access. • Vulnerabilities that require user privileges for successful exploitation.
Low	Exploitation of such vulnerabilities usually requires local or physical system access and would have little impact on the organization.

Table C. Level of Effort

Level of Effort	Description
High	This requires a high level of dedicated effort from one or more teams on critical systems, including patching, multiple configuration changes, or highly technical changes that risk bringing services down.
Moderate	This is a medium-level effort that requires substantial dedication from a partial or entire team. This could impact services or cause a partial outage.

Low	These are individual or small team efforts generally requiring a minimal time commitment and require running an update or remedial command or series of commands that will not impact production services.

Table D. System Inventory

System Components	
Servers	Virtualized farm running on Hyper-V (2 hosts). Windows Server 2019 and Ubuntu Linux. Approximately 20 virtualized servers (across the 2 hosts), including the following roles: • (Ubuntu Linux) FTP server for EDI Incoming Operations • 3x Domain Controllers (1 used for M365 identity sync) • 1x File Storage/Server • 1x Ruby On Rails server • 3x ElasticSearch servers (cluster) • 5x web application servers (Ubuntu Linux cluster, 1x PostGRESQL, 1x MariaDB SQL, 3x running nginX Plus w\reverse caching proxy, 1x running Apache Tomcat, PHP 8, hosting SSL/TLS certificates) • 4x Remote Desktop Servers for internal shared/applications • 2x legacy Exchange servers (post-migration)
75 Workstations	Windows XP, 7, 10/11 Pro, Ubuntu Linux, MacOS
Switches	HPE JL262A Aruba 2930F 48G PoE+
Firewall	2x Sophos XG firewalls
Border router	Verizon FIOS router (CR1000A)
Laptops	Windows 10, 11, Ubuntu 22.04 LTS, MacOS (Ventura, Monterey, Big Sur)
Wireless Access Points	10x HPE JZ337A Aruba AP-535
Cable plant	Cat6a

Table E. Risk Identification

Risk #	**Vulnerability (NVT Name)**	**NVT OID**	**Severity**	**Risk**	**Level of Effort**
1	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	1.3.6.1.4.1.25623.1.0.108010	Critical	High	High
2	MFA not enforced across all users		High	High	High
3	Rexec service is running	1.3.6.1.4.1.25623.1.0.100111	High	High	Low

4	All users have local administrative privileges		Medium	Moderate	High
5	Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability on publicly-facing server	1.3.6.1.4.1.25623.1.0.140051	Critical	High	Moderate
6	Operating System (OS) End of Life (EOL) Detection	1.3.6.1.4.1.25623.1.0.103674	Critical	High	Low
7	rlogin Passwordless Login	1.3.6.1.4.1.25623.1.0.113766	High	Moderate	Low
8	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	1.3.6.1.4.1.25623.1.0.143545	Critical	High	Moderate
9	PostgreSQL weak password	1.3.6.1.4.1.25623.1.0.103552	High	High	Low
10	PostgreSQL admin is reachable from internet		Critical	High	Low
11	VNC Brute Force Login	1.3.6.1.4.1.25623.1.0.106056	High	High	Low
12	FTP Brute Force Logins Reporting	1.3.6.1.4.1.25623.1.0.108718	High	High	Low
13	phpinfo() output Reporting	1.3.6.1.4.1.25623.1.0.11229	High	Moderate	Low
14	vsftpd Compromised Source Packages Backdoor Vulnerability	1.3.6.1.4.1.25623.1.0.103185	High	High	Moderate
15	rsh Unencrypted Cleartext Login	1.3.6.1.4.1.25623.1.0.100080	High	Moderate	Moderate

16	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1.3.6.1.4.1.25623.1.0.105042	High	Moderate	Moderate
17	Anonymous FTP Login Reporting	1.3.6.1.4.1.25623.1.0.900600	Moderate		Low
18	Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	1.3.6.1.4.1.25623.1.0.108011	High	Moderate	High
19	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1.3.6.1.4.1.25623.1.0.111012	Moderate	Moderate	Moderate
20	Weak Host Key Algorithm(s) (SSH)	1.3.6.1.4.1.25623.1.0.117687	Moderate	Moderate	Moderate

Company B Cyber Security Tools

Company B has provided this list of cyber security tools in anticipation of being acquired by Company A. This list is assumed to be complete.

Table A. Cyber Security Tools

Tool Name	Purpose
Sophos/Intercept X	Endpoint Detection and Response
OneTrust	Data privacy/Data lifecycle management
Code42	Data-centric security
Sophos XG	Next-Gen Firewalls
No tool available	Mobile Device & Application Management
DUO	Identity and Access Management
Akamai	Application Security
Mimecast	Messaging Security
Arctic Wolf	Managed Security Services Provider
Cisco Umbrella	DNS Security
In progress	Cyber security policy
In progress	Written Information Security Policy (WISP)

In progress	Written procedures
Minimal	Documentation of environment

A. Analyze the given network diagram and vulnerability scan for both companies by doing the following:

1. Describe **two** existing vulnerabilities for *each* company.

Company A:

- Open ports 21 – 90, and open port 3389 are not secured when they are kept open.
- The 8 - character password rule that is still being used, in my professional opinion, is an antiquated approach to password creation. 8-character passwords may not be complex enough for the level of account security needed.

Company B:

- Distributed Ruby (dRuby/DRb) has an execution vulnerability associated with mishandling the sending of syscalls which can work in favor of hackers.
- Multi-factor authentication (MFA) is not enforced among all users. For a company providing proprietary software to support medical providers, single-factor authentication isn't sufficient.

A2. Explain the impact, risk, and likelihood associated with *each* described vulnerability from part A1 as it relates to *each* company.

Company A:

- Open ports 21 – 90, and open port 3389 are not secured when they are kept open.

Impact: Keeping these ports open increases surface attack area and can lead to exploitation causing breach of data, and system infections like malware.

Risk: Risk of exploitation is high; Port 3389 is the default for Remote Desktop (RDP) and often subject to ransomware and brute force attacks.

Likelihood: This is the highest ranked risk in the analysis done on Company A, there is a high likelihood of occurrence.

- The 8 - character password rule that is still being used, in my professional opinion, is an antiquated approach to password creation. 8-character passwords may not be complex enough for the level of account security needed.

Impact: A short password has less possible combinations and can lead to dictionary attacks, or data breaches via brute force which will be damaging to company systems and reputation.

Risk: Risk is high due to lack of password complexity requirements, and it is further heightened due to substandard use of MFA across the entire organization.

Likelihood: There is a high likelihood, weak passwords are an easy way for unauthorized access to occur since online dictionaries have become sophisticated often using automation to crack shorter passwords.

Company B:

- Distributed Ruby (dRuby/DRb) has an execution vulnerability associated with mishandling the sending of syscalls which can work in favor of hackers.

Impact: The potential misdirection of syscalls could lead to companywide system compromise and the theft or tampering of critical business data. Downtime, and costs associated with remediation could be substantial. Damage to the public corporate image may never be fully recovered from.

Risk: There is high risk of occurrence, this vulnerability is easily exploitable as hackers only need simple combinations of syscalls to arbitrarily gain access to a system.

Likelihood: Likelihood is high due to the widespread use of the Ruby, and the fact that this is a known vulnerability associated with its operation. Any improper handling of syscalls will work in a hacker's favor, this is an easily exploitable vulnerability.

- Multi-factor authentication (MFA) is not enforced among all users. For a company providing proprietary software to support medical providers, single-factor authentication isn't sufficient.

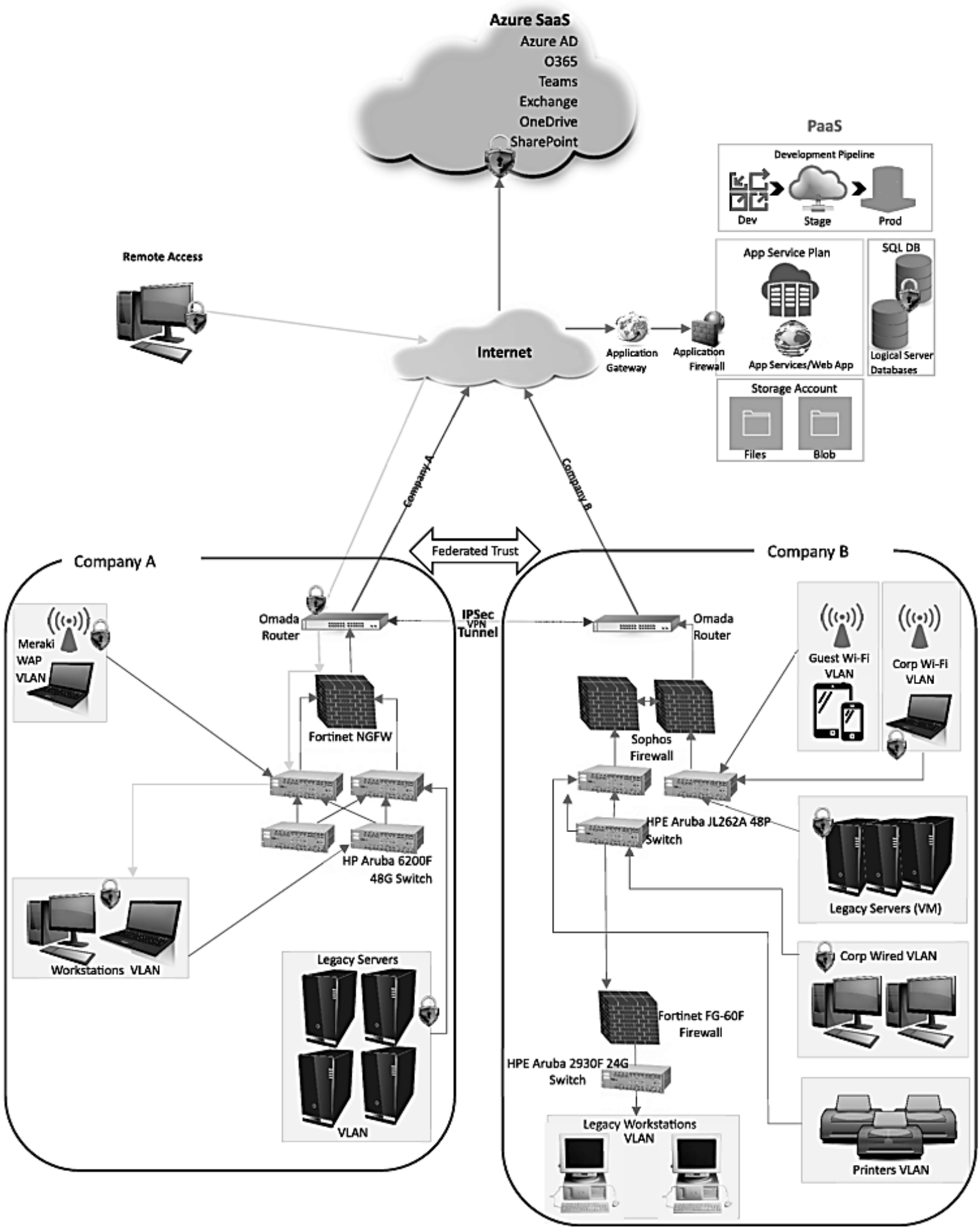
Impact: Without strong MFA, phishing emails that compromise passwords will allow bad actors system entry as there is no second point of defense. Since Company B has a proprietary software that supports medical providers, using just a password alone is insufficient and means that any segment of the network can be subject to data loss or corruption at any time without record of activity.

Risk: There is no form of secondary verification across many parts of the network, and password requirements are also weak, the risk is high.

Likelihood: Likelihood of this being exploited is high. Phishing attempts are increasing in volume and are becoming harder to identify. Once a password is obtained, lack of MFA use will allow compromised access.

B. Create a network topology diagram that merges both Company A and Company B diagrams (above) and include details of the proposed merged network requirements.

(see below)


Azure SaaS
Azure AD
O365
Teams
Exchange
OneDrive
SharePoint
PaaS
Development Pipeline
Dev
Stage
Prod
Remote Access
App Service Plan
SQL DB
Internet
Application Gateway
Application Firewall
App Services/Web App
Logical Server
Databases
Storage Account
Files
Blob
Company A
Company B
Federated Trust
Omada Router
IPSec VPN Tunnel
Omada Router
Meraki WAP VLAN
Fortinet NGFW
Sophos Firewall
Guest Wi-Fi VLAN
Corp Wi-Fi VLAN
HP Aruba 6200F 48G Switch
HPE Aruba JL262A 48P Switch
Legacy Servers (VM)
Workstations VLAN
Legacy Servers
VLAN
Corp Wired VLAN
Fortinet FG-60F Firewall
HPE Aruba 2930F 24G Switch
Legacy Workstations VLAN
Printers VLAN

C. Identify the layer for *all* components in the topology diagram referencing the layers of the OSI model and TCP/IP protocol stack.

Component	OSI Layer	TCP/IP
Servers	Layer 7: Application	Layer 4: Application
Workstations	Layer 7: Application	Layer 4: Application
Laptops ThinkPad E16 G2 (16" AMD) (14x) Windows 11 (>6) Windows 10 Ubuntu 22.04 LTS MacOS	Layer 7: Application	Layer 4: Application
Printers	Layer 7: Application	Layer 4: Application
Firewalls Fortinet Fortigate 800D NGFW Sophos XG firewalls (2x) Fortinet Fortigate FG-60F	Layer 7: Application	Layer 4: Application
Azure Application Service Plan	Layer 7: Application	Layer 4: Application
Routers Omada VPN Router (2x)	Layer 3: Network	Layer 2: Network
Switches HP Aruba 6200F (4x) HPE JL262A Aruba 2930F 48G (3) HPE Aruba 2930F 24G	Layer 3: Network	Layer 2: Network
Wireless Access Points HPE JZ337A Aruba AP-535 (10x)	Layer 3: Network	Layer 2: Network
Cable Cat6a	Layer 1: Physical	Layer 1: Network Access

D. Explain the rationale for adding, deleting, or repurposing network components in the newly merged network topology diagram, including details of how *each* component addresses budgetary constraints.

Azure Application Service Plan - Executives of the newly merged company expressed interest in cloud integration. Microsoft Azure Software-as-a-Service and Platform-as-a-Service Azure can improve security and increase productivity by integrating with company tools like MS Office and Teams. Azure Application Service works with active directory (AD) and domain services and will enable the company to take advantage of cloud elasticity meaning they can add, change, and remove services as necessary based on volume. This will improve scalability for long-term growth. Additionally, based on the vulnerability report for Company B, there is minimal documentation of the overall environment. Azure will allow for creation of a dev pipeline that will help to fast track the coding documentation process by allowing each stage to be recorded in sequence as it is carried out. Over time, the merged company will realize significant cost savings from adding app services to the cloud.

Servers - As part of the merge, the hardware servers for both companies will be moved to the cloud; servers for Exchange, SharePoint, file/application server, and web app will undergo migration. The web server for Company A will be moved to a newly added VLAN and the demilitarized zone (DMZ) will be retired, removing any potential access to the public will work to bolster network security. The VM server hardware used by Company B will also be added to a server VLAN. Servers on the VLAN are considered

legacy. They will be maintained during the timeframe that cloud services are transitioning and phased out over a period of 6 - 8 months. Exorbitant costs associated with managing on-premise servers and end-of-life equipment can be limited with partial cloud transition allowing for successful operations within budget constraints.

Workstations and Laptops - Existing workstations and laptops that are on Windows 10/11 will be repurposed. There are still security updates being released for them. This is a cost-efficient approach considering patching is still available, there is no need to write off equipment. The laptops that are utilizing Windows 7 will be no longer be in commission, 14 new ThinkPad E16 Gen2 laptops will be purchased in place of them. Ubuntu 22.04 LTS and MacOS laptops will continue to be maintained and utilized on the network, any updates will continue to be applied as they become available.

Printers - The printers shown in the original topology for Company B, are not addressed in the final vulnerability report that was presented for Company B. For this reason, they were repurposed as they do not appear to be a security risk. During the merge, the pooled printers were been added to their own segment on the internal network. There are no new costs associated with bringing over the existing printers as they were already in use prior to merging.

Firewalls - The Fortinet Fortigate 800D NGFW will be repurposed since support is still provided by the vendor who provides global technical assistance. There is no further associated cost with this and the configurations already afford a high degree of security control. Two Sophos XG firewalls will also be repurposed and will remain positioned side-by-side in the topology merger for added security of internal switch and router. Due to the inherited security risk of keeping aged equipment on the network, legacy devices that are being phased out are segmented on the network for isolation and a Fortinet Fortigate FG-60F firewall was purchased within budget constraints for further protection.

Routers - The Cisco 7600 router used by Company A is no longer supported and is therefore a continued security risk the longer it remains in use. It will be removed and replaced with a newly purchased Omada VPN Router. This offers VPN access for remote users, but will also work to create VPN tunneling with Company B. A second Omada VPN Router was purchased for use in place of the router provided by Company B's ISP. Replacement of the ISP router will increase throughput and better control in creating point-to-point connection with Company A.

Switches - The Four Cisco 3750X switches that Company A uses are end-of-life and will be removed. They will be replaced with four HP Aruba 6200F switches. In replacing end-of-life switches, security posture of the network and its systems is heightened as devices are continuously updated with the newest enhancements. Three JL262A Aruba switches will be repurposed because they are still vendor supported; this is in line with the proposed business constraints as this many replacement switches will engulf the allotted budget. An HPE Aruba 2930F 24G switch was purchased for isolated segmentation of legacy devices, the cost can be justified due to the inherited security risk of keeping aged equipment on the network.

Wireless Access Points - There are known vulnerabilities associated with the Meraki MR28 wireless access points. These devices pose a surface attack risk and will be removed. The existing Aruba AP-535 wireless access points used by Company B will be used instead. The latest upgrades will be done so that any patching or fixes can be applied. Since the Aruba AP-535 devices were purchased before the merge, there will be no added costs associated with reuse.

Cable - Company A has been using Cat5e cable for their network. This does not have the same speeds and throughput as the Cat6a that Company B has been using. A large portion of the network will now utilize the cloud, and the Cat6a will be replacing the Cat5e cabling allowing for increased frequency bandwidth. This is an existing resource and as such it will not need to be factored into the budget.

E. Explain **two** secure network design principles used in the proposed network topology diagram.

Defense in Depth - A multi-layered approach was applied through tailoring the topology to meet the varying degrees of technical and administrative depth of the company including available budget. First, hardening of the environment was considered. The list of system components provided for Company A and Company B were investigated for their potential security risk to the organization, and were subsequently supplemented with new components, removed, or repurposed. Zero Trust was another layer that was employed. This was heavily relied on in many of the design decisions for the proposed network topology. Just because a user had access, doesn't mean that they always should. Multifactor authentication was placed at all main points of network entry requiring strict authorization for all devices and applications each time they are accessed. The Principle of Least Privilege (PoLP) is applied with Azure, account permissions are compared against the total permissions enabled on an account. Users without entitlements will be flagged

Redundancy and Scalability - Data reliance is vital for the success of continued operations. Information should be accessible at all times when it is needed. Load balancing and numerous firewalls eliminate single points of failure to maintain a high degree of availability, or redundancy. In a few instances, microsegmentation eliminates redundant hardware and need for added firewalls. The organization has potential for growth in the future, this was taken into consideration when proposing the topology. Redundant load balancers and servers contribute to scalability, or the ability to accommodate increased traffic. As workloads increase, scalability will enable the company to quickly adapt to changing technologies and market conditions.

F. Summarize your recommendations for implementation of this proposed merged network based on the scenario and budgetary requirements, including the following in the summary:

- a justification for your recommendations to implement the proposed secure merged network design

Justification:

The proposed topology can provide a robust defense against modern threats ensuring the confidentiality, integrity, and availability of critical systems. Due to an evolving threat landscape, bad actors are using advanced techniques to breach legacy security models. Implementing the secure merged network design with leading Zero Trust architecture will help to protect sensitive customer data, meet regulatory requirements, and minimize attack surfaces thereby enhancing overall security posture. The company will be better positioned for defense against internal and external threats through endpoint detection and response to strengthen business continuity in the increasingly complex digital landscape.

Replacement of end-of-life equipment and dated software is rooted in the need to further address ongoing security vulnerabilities and improve operational efficiency. Over time, attackers stockpile a catalog of known vulnerabilities in outdated systems. Once they are widely known, malicious actors can exploit them at-will. The longer a system remains in use past its end-of-life, the higher the likelihood it will be targeted. It's no longer a question of if improvements like this are necessary, but when they should be adopted to stay ahead of emerging threats.