Assignment 5.6

Prolix Corporation

Network/Security Diagram

Iirai Costner
Jose Krasniansky
Anna Liza Smith

Prolix Corp Diagram

Prolix Corp provides both online and retail sales. Its motto is “We Sell Anything!”
Its environment includes the following resources (in no specific order):

- Retail store with PoS systems
- Customer web application
- HR/ERP system(s)
- Microsoft Active Directory for identity and authorization
- Additional identity services for customer and vendor management
- Employee hosts
- Internal servers for storage, database, printing, etc.

Using your newly acquired knowledge and experience as a cybersecurity analyst, design a secure network that incorporates security controls for confidentiality, integrity, and availability. Remember to account for concepts such as:

- Network segmentation
- High availability / fault tolerance
- Defense in depth
- Control types, including preventative, collective, analytical, etc.

Deliverable:

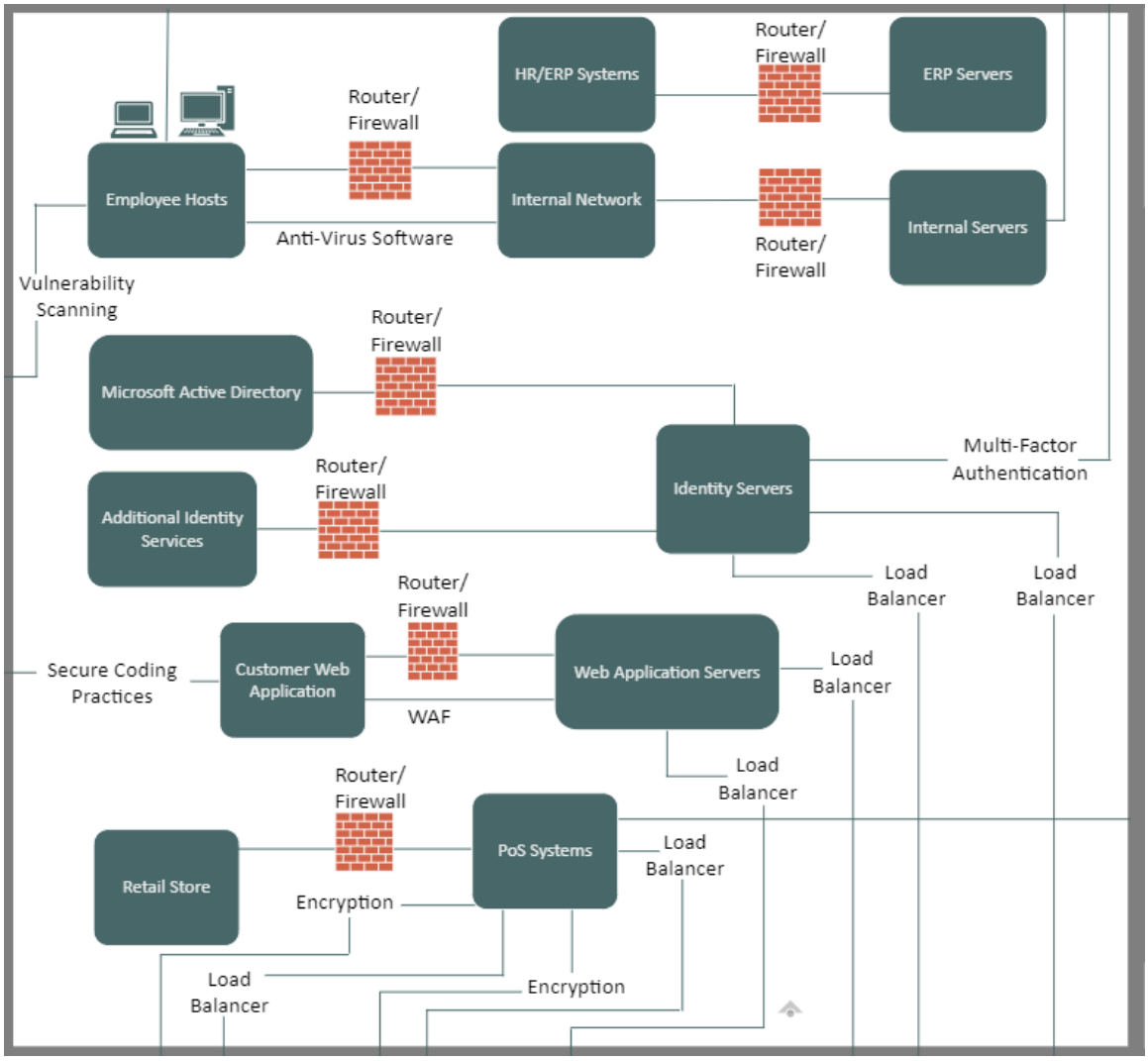
Working as a group, develop a diagram that takes these security features into account. Some assumptions such as sales volume, employee workforce, applications, and platforms will have to be deduced. Ensure that your solution is appropriate to those assumptions.

To begin designing a secure network for Prolix Corp that incorporates security controls for confidentiality, integrity, and availability, accounting for the specified concepts and specifications, the following assumptions must be established:

1. Sales Volume: Since this scenario involves a retail store with Point of Sale (PoS) systems, we can assume that the store has a certain level of sales volume and transactions that need to be processed securely and be PCI DSS-compliant.
2. Employee Workforce: The network design considers employee hosts and mentions employee training. Therefore, we can assume that there is an employee workforce within the organization that requires access to the network and its resources.
3. Applications: The network design mentions specific applications such as the Customer Web Application, HR/ERP systems, Microsoft Active Directory, and additional identity services. We can assume that these applications are critical for the organization's operations and require secure connectivity and protection.
4. Platforms: The network design includes various platforms, such as PoS systems, web application servers, ERP servers, identity servers, and internal servers for storage, database, and printing. These platforms suggest a diverse infrastructure supporting different functions within the organization.

As new cybersecurity analysts, designing a secure network that ensures the security controls for confidentiality, integrity, and availability are considered, we have incorporated the following concepts into this diagram:

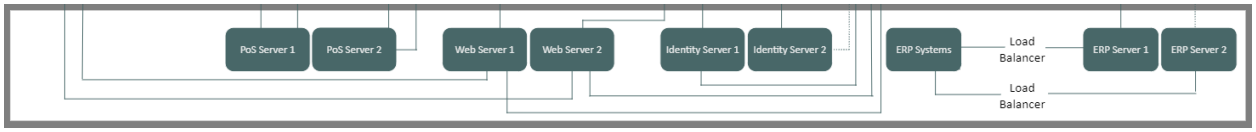
1. **Network Segmentation**:



Network segmentation has been implemented into separate components of the network based on their function and security requirements. The network has been divided into distinct segments for the retail store, customer web application, HR/ERP systems, Microsoft Active Directory, additional identity services, employee hosts, and internal servers. This, in addition to applying encryption to the PoS systems, ensures the network is PCI-DSS compliant.

The use of firewalls and routers to control traffic flow between network segments allow only necessary communication and block unauthorized access.

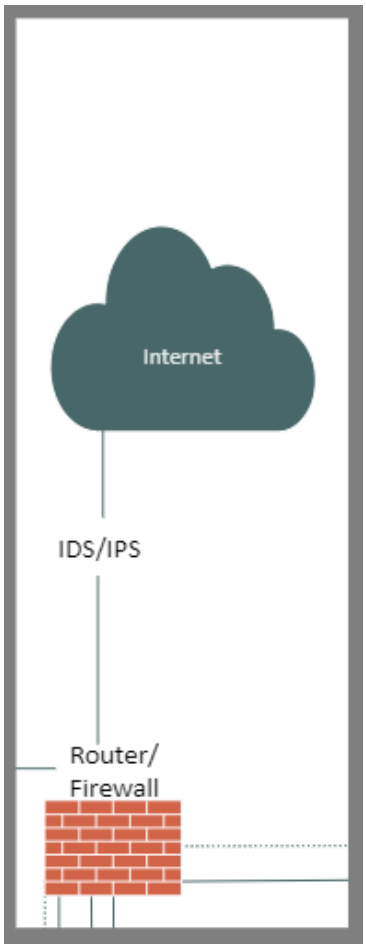
2. **High Availability/Fault Tolerance**:



All routers have redundancies, which ensures high availability and fault tolerance. Using technologies like Virtual Router Redundancy Protocol (VRRP) can also provide failover capabilities.

Load balancing techniques have been implemented to distribute traffic evenly across multiple servers, enhancing availability and performance.

3. Defense in Depth:



Implementing multiple layers of security controls to provide defense in depth, which includes using a combination of network, host, and application-level security measures.

Employ intrusion detection and prevention systems (IDS/IPS), antivirus software, and web application firewalls (WAFs) to detect and block various types of attacks.

Use secure coding practices for the development of the customer web application to mitigate common vulnerabilities.

4. Control Types:

A reasonable range of control types to address security needs is implemented:

- Preventative controls: firewalls, access controls, encryption
- Detective controls: intrusion detection systems, log monitoring
- Corrective controls: incident response plans, backup, and recovery mechanisms

Performing regular security assessments, vulnerability scanning, and penetration testing to identify weaknesses and improve security posture is also included and highly suggested.

5. Additional Measures:

- Keep all systems and software up to date with the latest security patches,
- Apply strong authentication and authorization mechanisms, such as multi-factor authentication, for accessing critical systems and services,
- Regularly back up important data and test the restoration process to ensure data integrity and availability, and
- Train employees in security best practices, including password hygiene, social engineering awareness, and incident reporting procedures.

This approach/diagram will help establish a secure network that safeguards the confidentiality, integrity, and availability of the retail store's PoS systems, customer web application, HR/ERP systems, Microsoft Active Directory, additional identity services, employee hosts, and internal servers.

The other attachment shows the PDF version of the Prolix Corporation diagram. <Mic drop>