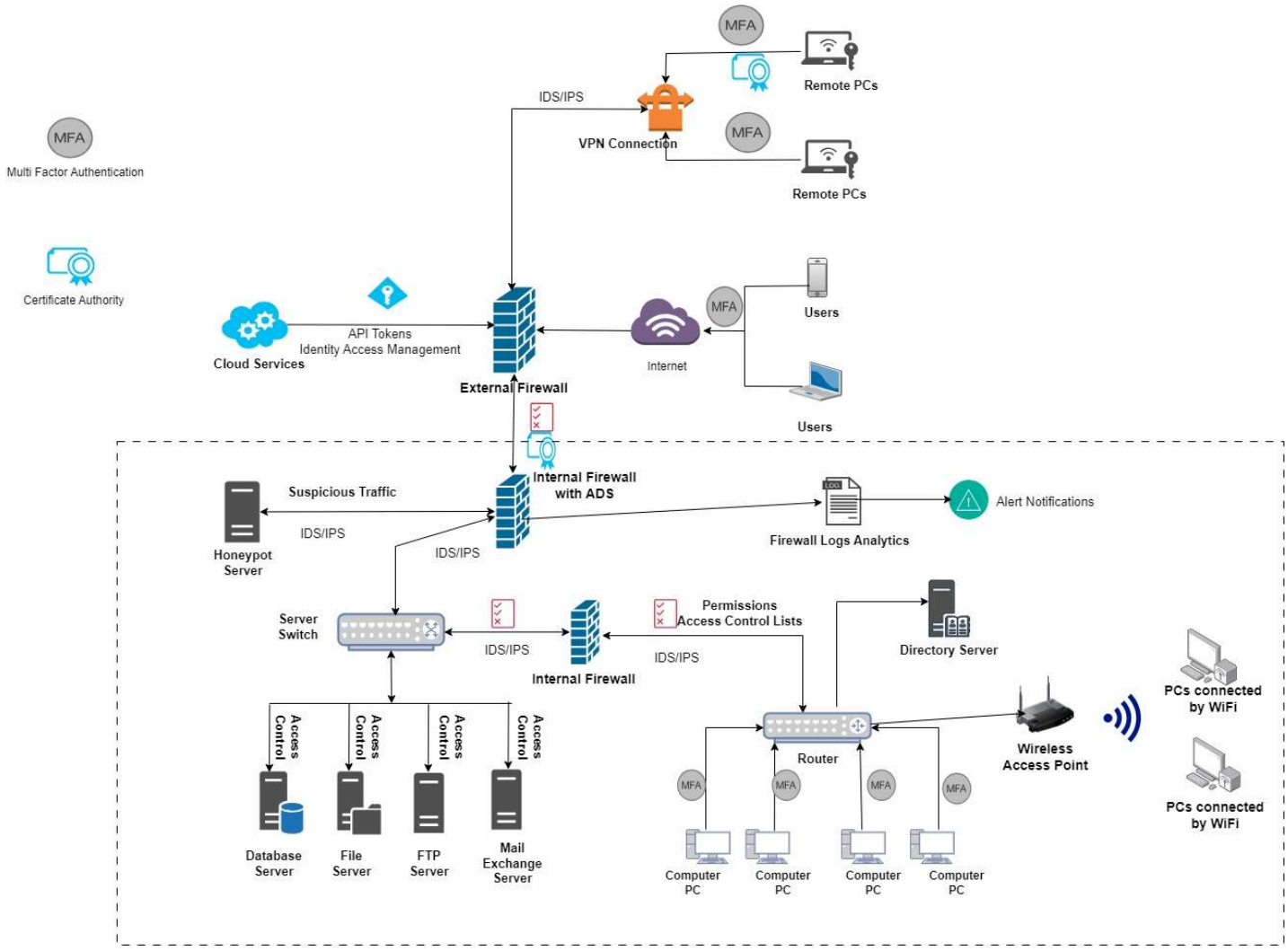
Task 1: Secure Network Diagram



This is a secure network diagram for a mid-size company. We will look into the security configurations for each type of user(VLAN user, remote use through VPN, Cloud service user) as well as details about the security implementations/configurations used.

Remote workers use the Internet as an outside network.

Remote workers are required to complete a series of processes before accessing the internal network. They would use VPN connections, i.e., **encrypted tunnel** for secure remote access. Users must use **Multi-Factor Authentication (MFA)** to connect and login to a company-provided VPN service. Therefore, Only authorized users and devices allowed access.
The VPN travels via an intrusion detection and prevention system (**IDS/IPS**). The network is then routed through an external firewall to screen out dangerous information and ensure user integrity. The network is routed through an internal firewall, which checks for connections and diverts suspicious traffic to a honeypot server.

Once all tests are completed, connections to databases and internal software can be established.

VPN security can be ensured by 2 methods:

1. IP Based VPN Rules: subset of firewall rules used to control access to a VPN network based on the source or destination IP address
2. **Certificate based** VPN rules : Uses digital certificates for both client and server, offering stronger security and mutual authentication.

In addition to internet security protocols, remote employees should attend monthly security awareness workshops to stay up-to-date and alert to potential threats like phishing emails.

Users(Internet)

The users are the most important security layer and must be properly monitored. The security procedure remains unchanged: users will not have access to any business-related services or files. The user connection must travel through two firewalls: an external one that filters for dangerous information and confirms the user's integrity, and an internal firewall that takes the ultimate choice and checks for the connection. Any suspicious traffic is directed to the **Honeypot** server. The internal firewall checks the user's access and prevents them from connecting to unauthorized services.

Access Control Lists used to control network traffic by limiting the number of users accessing files, systems, and information.

Whitelisting involves creating a list of trusted entities that are explicitly allowed access to a resource

Additionally, we will restrict access to our services and systems to authorized individuals. We prevent unauthorized users or features from accessing anything. User accounts assigned **least privilege** based on job function. Proper **authorization** processes will be followed.

WiFi network

Defining multiple SSIDs – few employees or certain teams can access only particular SSIDs, this can be defined in Access Control Lists.

Authentication and MAC Binding to verify and restrict the devices connected to a Wireless Access Point.

Cloud Services

Cloud security is crucial for companies that heavily rely on cloud services at the network layer. Cloud security measures will be followed while connecting to each network. We would employ **Identity and Access Management (IAM)** protocols to enhance the trustworthiness of the connection and provide only necessary rights. We will utilize **API tokens and keys** to authenticate service access and usage.

Additionally, as previously stated, we will restrict access to our services to specific API tokens and keys for cloud services. This approach strengthens and secures the connection, allowing the cloud to only access necessary resources.

Internal Network

We must establish security mechanisms on the PCs connected to the LAN network. Users require **multi-factor authentication (MFA)** to access computers and servers. Each user computer connects to

a router, which is monitored by IDS/IPS. Next, the connection is routed through an internal firewall. The connection is scanned for suspicious traffic, followed by access restrictions(ACLs). Access to diverse servers requires correct authorization for each machine and user.

Here 2 concepts would be implemented :

1. **VLAN Segregation**: We would create separate VLANs for each team in the firm to maintain segmentation and modularity. Each of these VLANs would have different rules set in **UTM/Firewall**.
2. **MAC Binding** : associates a specific device's unique MAC address with a permitted IP address in the network. This means that only devices with authorized MAC addresses can connect and access the network, restricting unauthorized access and potentially enhancing security.

To enhance security, we installed anti-virus software on each machine. We propose adding the ability to remotely erase sensitive data from a PC in case of a breach. This function is exclusive to a few individuals and cannot be performed by others. These precautions enhance computer security within the LAN.

Additional security measures include a honeypot server to detect unusual activity. A honeypot server prevents malicious traffic and improves security.

File, Mail Exchange, FTP, Database, and Directory Servers

Access controls ensure security for these servers, which are connected to the mainframe. Any of these servers cannot be accessed without the appropriate permissions. They are also monitored with IDS/IPS software.

Additionally, Tokens and Keys can enhance the security of the software. Implementing these features and managing access to them can improve the security of the software.

Security Configurations(Additional)

Unified Threat Management:

UTM is used nowadays with multiple security features than a firewall. UTM or Next Generation Firewall includes anti-virus, anti-spam, content filtering, and web filtering.

Enterprise antivirus server:

- **Centralized Management:** Manage and deploy antivirus software to all endpoints from a single console, simplifying administration and ensuring consistent security across the network.
- **Real-time Protection:** Continuously scan for and block malware threats in real-time, including viruses, worms, ransomware, and other malicious software.
- **Automatic Updates:** Automatically download and deploy security updates to all endpoints, ensuring they have the latest protection against evolving threats.
- **Threat Detection and Response:** Utilize advanced threat detection technologies like sandboxing and behavioural analysis to identify and respond to sophisticated attacks.
- **Endpoint Control:** Manage and enforce security policies on endpoints, such as blocking unauthorized applications or websites.
- **Reporting and Monitoring:** Generate reports and track security events across the network to gain insights into threats and improve overall security posture.

- **Proactive defense:** Regularly updated security software and firmware patches address vulnerabilities quickly.

To enhance security, we may provide mandatory cybersecurity training for all employees in our organization. We understand that we are only as strong as our weakest links. To enhance security, consider implementing cybersecurity training and phishing email screening for employees. To ensure the safety of our organization, we must establish physical security measures such as a secure location with restricted access.

Task 2: Recent Security Event Article

Data Breach at Vanderbilt University Medical Center

In late November 2023, Vanderbilt University Medical Center (VUMC) confirmed a cybersecurity incident involving a compromised database potentially containing patient information. Details remain unclear, but the leak site of the Meow ransomware gang listed the hospital. Initial investigations suggest no patient or employee data breach, though Meow claimed otherwise. Regardless, the incident raises concerns about potential vulnerabilities and data security.

Why the event happened – Root Causes?

While specific details are lacking, several factors contribute to healthcare's susceptibility to cyberattacks:

- **Legacy Systems:** Many healthcare institutions rely on outdated IT infrastructure, increasing attack surface and patching difficulties.
- **Data Treasure Trove:** Patient records hold valuable personal and financial information, making them a lucrative target for attackers.
- **Ransomware Rise:** Ransomware attacks are increasingly prevalent, targeting critical infrastructure like hospitals with the threat of service disruption.
- **Unclear Motive:** Meow's motivations remain unclear, whether solely financial or "bug bounty" related, raises ethical questions.

Prevention and Mitigation

While preventing every attack is impossible, proactive measures can mitigate risks:

- **Modernize infrastructure:** Invest in updated systems with robust security features and regular patching procedures.

- **Data Security:** Implement data encryption, access controls, and multi-factor authentication to protect sensitive information.
- **Cybersecurity Awareness:** Training staff on identifying and reporting suspicious activity strengthens the human firewall.

Broader Issues

This incident raises ethical and societal concerns:

- **Patient Privacy:** Breaches compromise sensitive health data, potentially impacting trust and future care access.
- **Public Health:** Disruptions to healthcare systems can have cascading effects on patient well-being and emergency response.
- **Cybersecurity Ecosystem:** The incident shines a light on the ongoing arms race between attackers and defenders, requiring continuous adaptation and collaboration.

A data breach at a healthcare institution carries far-reaching consequences. Patients entrust hospitals with their most sensitive information, and a breach shatters that trust. Beyond lost confidence, compromised data can lead to identity theft, discrimination based on medical history, and even physical harm in some cases. Furthermore, disruptions to healthcare systems caused by cyberattacks can have cascading effects, delaying critical care and impacting public health.

Responses: Containing the damage and preventing future incidents requires action from various stakeholders:

- **Public:** Stay informed about security risks and practices, adopting secure online habits.
- **Policymakers:** Develop regulations and incentives to promote stronger cybersecurity practices in healthcare.
- **Corporations:** Invest in robust security measures and share best practices to create a more resilient ecosystem.
- **Media:** Encourage responsible reporting that educates the public without sensationalizing or jeopardizing ongoing investigations.

The Cybercriminal Landscape:

- Meow, a relatively new player, may not be directly linked to known ransomware groups.
- Their "bug bounty" approach, claiming to expose vulnerabilities for a fee, raises ethical concerns and highlights the blurred lines in cybersecurity.

- The incident underscores the increasing sophistication and diverse tactics of cybercriminals targeting healthcare institutions.

Conclusion

Healthcare organizations like VUMC hold a treasure trove of sensitive information: patient records containing names, addresses, medical diagnoses, and even financial details. This data, while vital for delivering patient care, also makes healthcare institutions highly attractive targets for cybercriminals. Ransomware attacks, where attackers encrypt data and demand ransom for its release, have become increasingly common, disrupting hospitals and jeopardizing patient care.

Several factors contribute to the increased risk in healthcare. Many institutions still rely on outdated IT infrastructure, lacking the modern security features and patch management capabilities found in newer systems. This creates a larger attack surface for malicious actors to exploit. Additionally, the growing adoption of connected medical devices introduces new entry points for attackers, further expanding the potential avenues for infiltration.

References:

[1] https://www.databreaches.net/vanderbilt-university-medical-center-security-breach-affects-3000-patients-officials-say/

[2] https://therecord.media/vanderbilt-university-medical-center-investigating-cyber-incident-meow-ransomware?&web_view=true