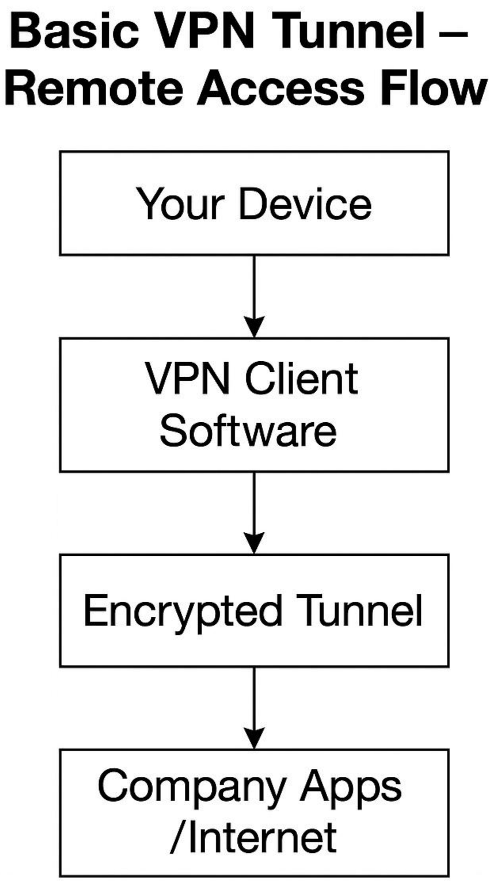
VPN Access Models – Visual Learning Project

1. Basic VPN Tunnel – Remote Access

This diagram illustrates a typical remote work VPN connection. A VPN client on the user's device establishes an encrypted tunnel to the company's VPN server. Once connected, all internet or internal traffic flows securely through this tunnel, protecting data and access.

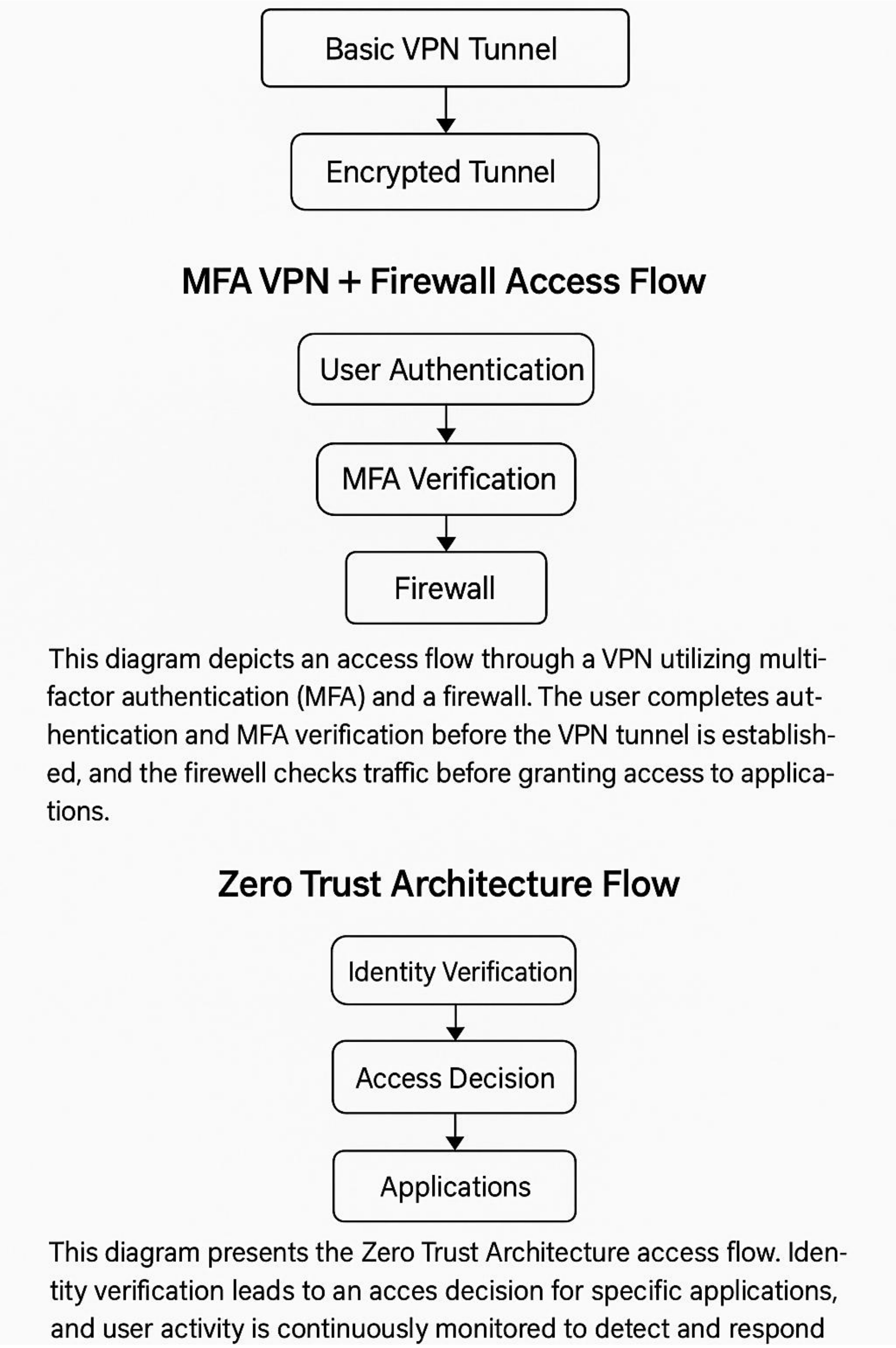


Basic VPN Tunnel – Remote Access Flow

This diagram illustrates a typical remote work VPN connection. A VPN client on the user’sdevice establishes an encrypted tunnel to the company’s VPN server. Once connected, all internet or internal traffic flows securely through this tunnel, protecting data and access.

2. MFA + Firewall and Zero Trust Access Flows

This diagram compares two access models. In the first (top), access is granted via VPN using multi-factor authentication (MFA) followed by firewall filtering. In the second (bottom), Zero Trust principles require identity verification and make real-time access decisions per session, continuously monitoring behavior.



MFA VPN + Firewall Access Flow

This diagram depicts an access flow through a VPN utilizing multi-factor authentication (MFA) and a firewall. The user completes authentication and MFA verification before the VPN tunnel is established, and the firewell checks traffic before granting access to applications.

Zero Trust Architecture Flow

This diagram presents the Zero Trust Architecture access flow. Identity verification leads to an acces decision for specific applications, and user activity is continuously monitored to detect and respond