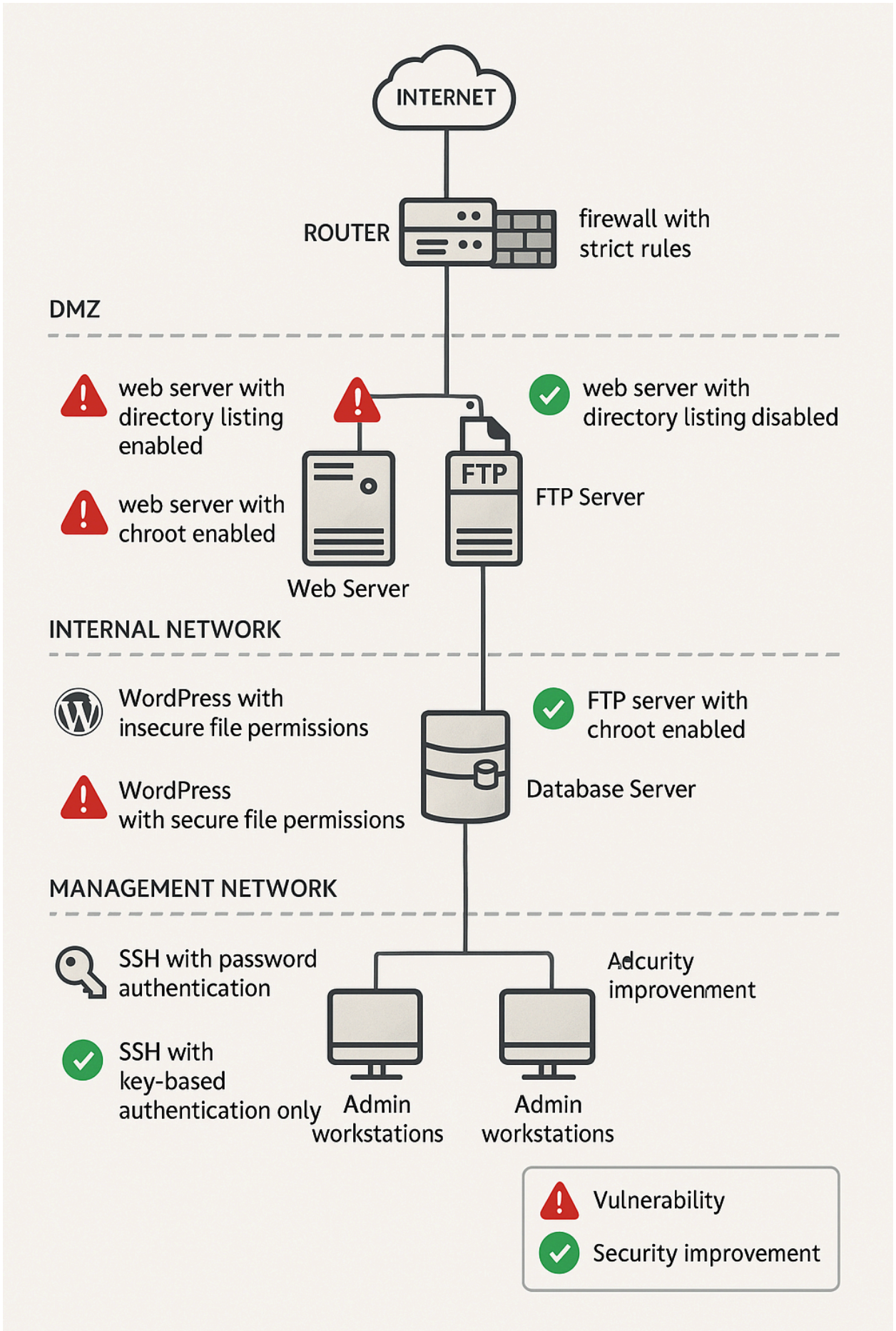
Network diagram

Explanation

- **Internet, Router, and Firewall:** The diagram starts with an **Internet Connection** that feeds into a **Router**. From the router, traffic passes through a **Firewall** where it is enforced with strict rules (marked with a green check "✅").
- **Network Segments:** Three subgraphs represent distinct security zones:
    - **DMZ Network:** Contains the **Web Server** and **FTP Server**. Each server lists its initial (vulnerable) configuration:
        - The **Web Server** was previously set to allow directory listing and had WordPress file permissions that were insecure (both flagged with red "⚠️"). The improvements—directory listing disabled and secure file permissions—are shown with green checks "✅".
        - The **FTP Server** is noted as having no chroot enabled (vulnerable) and shows the improvement with chroot enabled.
    - **Internal Network:** Hosts the **Database Server** and **Staff Workstations**.
    - **Management Network:** Contains the **Admin Workstations**, which are linked to an **SSH Service** note.
- **SSH Service Note:** The separate SSH node explains that insecure password authentication (red "⚠️") has been replaced by key-based authentication only (green "✅").
- **Legend:** At the bottom, a legend clarifies that the red warning symbol (⚠️) indicates a vulnerability, while the green check (✅) signifies the corresponding security improvement.


INTERNET
ROUTER
firewall with strict rules
DMZ
web server with directory listing enabled
web server with chroot enabled
Web Server
FTP
FTP Server
web server with directory listing disabled
INTERNAL NETWORK
WordPress with insecure file permissions
WordPress with secure file permissions
Database Server
FTP server with chroot enabled
MANAGEMENT NETWORK
SSH with password authentication
SSH with key-based authentication only
Admin workstations
Admin workstations
Adcurity improvenment
Vulnerability
Security improvement