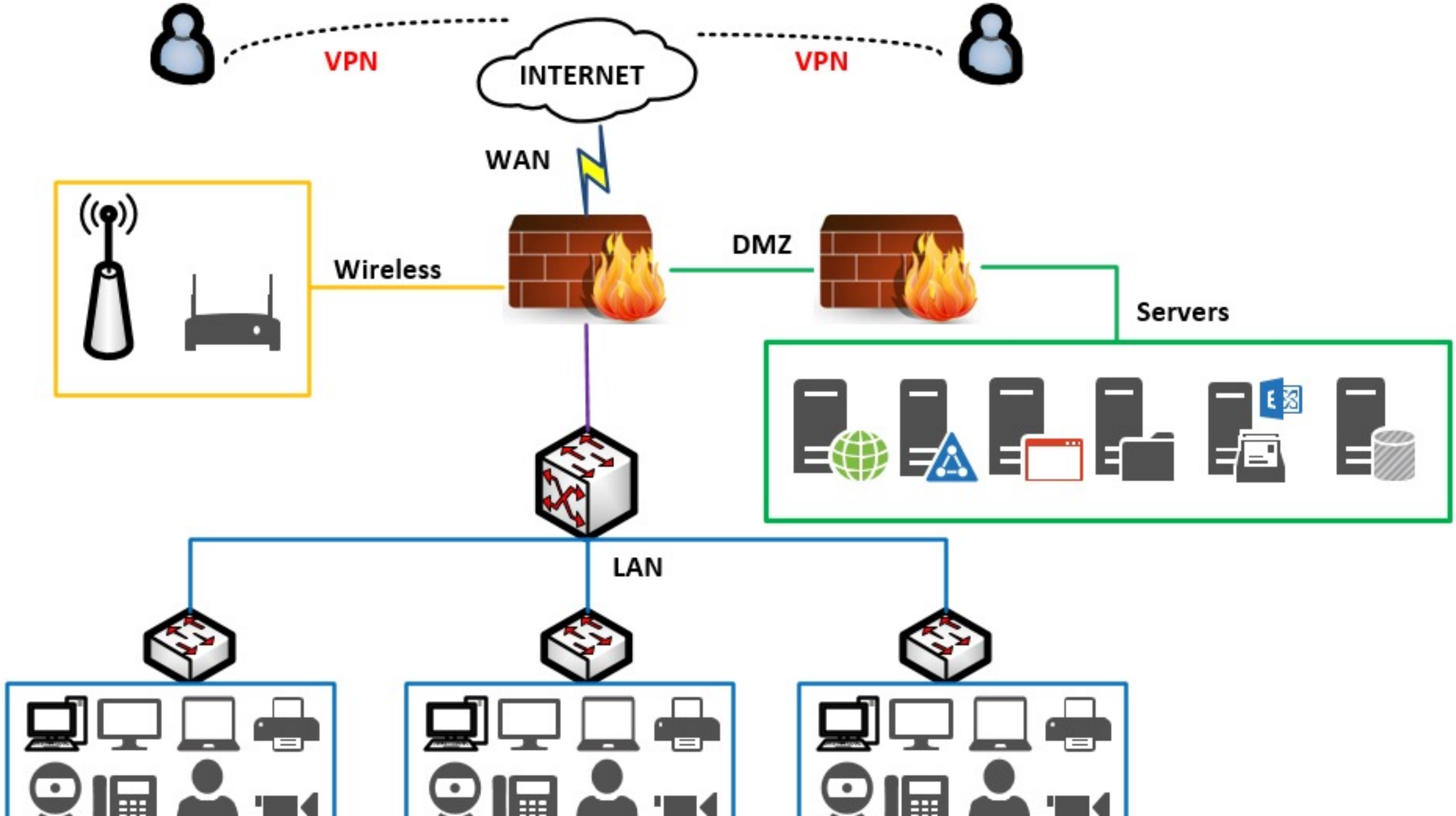
INC250306

Background:

- **Apex Financial:** A company providing online banking, investment management, and financial consulting.
- **Target:** Sensitive customer financial data and intellectual property related to a new proprietary trading algorithm.
- **Threat Actor:** A well-resourced Advanced Persistent Threat (APT) group known for financial espionage, ”APT 52"
- **Initial Vector:** A spear-phishing campaign targeting employees in the finance and IT departments.
- **Objective:** To exfiltrate data and establish long-term persistence within Apex Financial's network.


DAILY NEWS
CYBER ATTACK!
Apex Financial


VPN
INTERNET
VPN
WAN
Wireless
DMZ
Servers
LAN

Incident Notification: Critical Security Alert

EDR Alert

- **Severity:** Critical
- **Created:** 2025-03-06T16:45:32.208599 EST
- **Hostname:** WORKSTATION-01
- **User:** apexfinancial\analyst1
- **Tactic:** Execution, Persistence
- **Technique:** Malicious Macro (T1204.002), Scheduled Task/Job (T1053)
- **Description:**

EDR has detected the execution of a malicious macro on WORKSTATION-01.

Incident Response Activated

- **Message:**
  - "We need your expertise to analyze the evidence, contain the attack, and recover critical systems."
  - "Collaboration and effective communication are essential for a successful response."

Deliverables: **Incident Detection and Analysis:**

- Analyze provided log files (firewall, IDS/IPS, endpoint detection and response (EDR), system logs).
- Identify the initial attack vector and lateral movement
- Determine the scope and impact of the incident.
- Create a timeline of events.
- Any email related to this incident should have the subject INC250306_5689_ with your group number.
- **Initial Incident Notification (Internal):** An email to all employees informing them of the incident, advising them of security measures (e.g., password changes), and providing contact information for reporting suspicious activity.