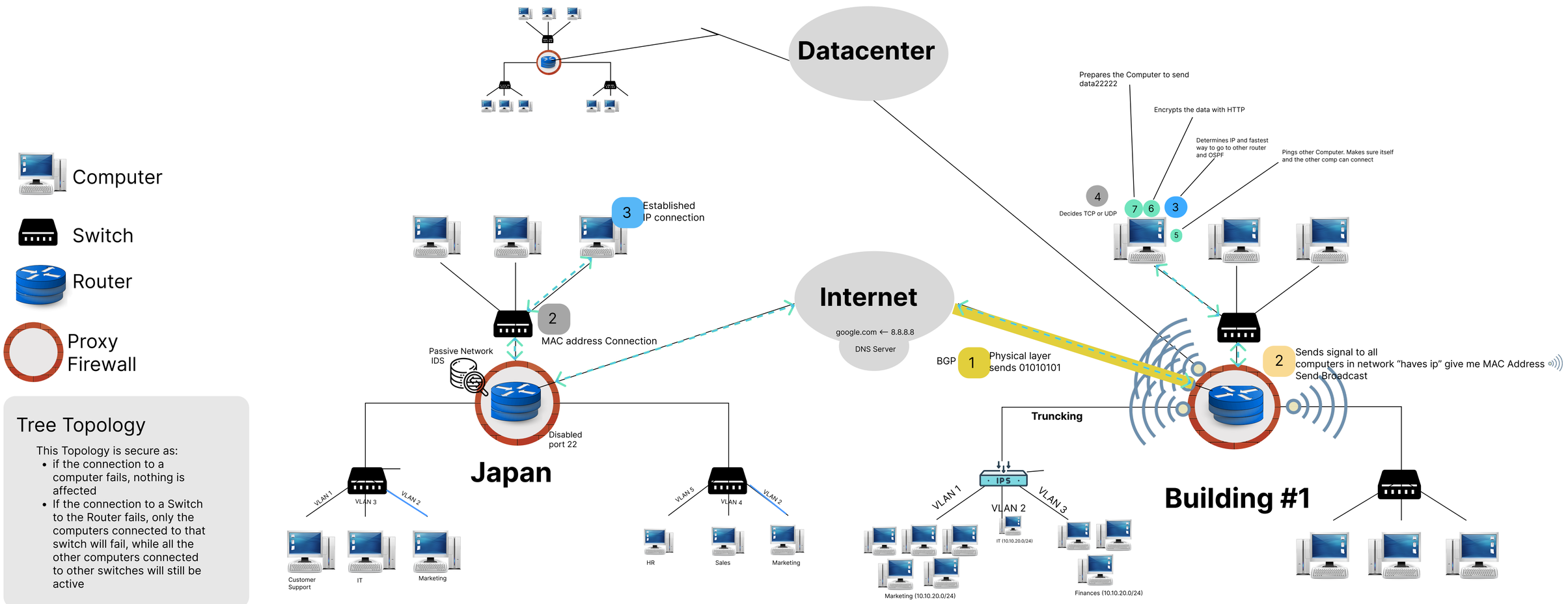
WAN



TREE TOPOLOGY

The TCP/IP Model

This model demonstrates the wy data is transferred through all seven layers of the model
security protocols:

- Firewall in the server. Protect malware and WAM from leaving and coming into the server
- SSL/encryption occurs during the presentation layer

Network Security Fundamentals

- In this map, we used a Proxy firewall as its safe, but a less expensive option.
- Building #1 bottom right side of the building used IPS to block and secure anything that gets past the buildings Router
- Japans firewall disabled port 22 as its highly vulnerable
- Japan Also used a Passive Network IDS to get notified if any possible vulnerabilities enter
- Example of detected events: Japan received a notification that someone is trying to login to their system.
- Building #1 IPS detected that a file extensions changed when passing through firewall. It prevents the process from going through the network

Access Control Measures

For building #1

- Members of the developers group have read-only access by default
- We will be using MAC
- In order for IT to sign in, they’ll need the password to sign in and a physical key to sign in.

Utilize Network Security Tools

- Wireshark Capture and Analysis
- Scenario: Detect anomalous traffic.
  - Captured packets identified malicious traffic.
  - Device was disconnected.
- Vulnerability Scanner Report
  - Tool: Nessus
  - Result: Outdated software patched.
- Penetration Testing Tool Output
  - Tool: Metasploit
  - Result: Verified system resilience post-patch.

Secure Wireless Networks

For building #2

- WPA2 enterprise with a radius server, for employee authentication
- Separate a separate VLAN WPA2, personal for guest acsess
- all acsess points have strong passwords, MAC filtering and updated firmware.
- keeping up with updates
  - Deployed WIPS on the network to monitor for rogue access points.
  - Configured alerts for unauthorized devices attempting to connect.

Monitor and Respond to Network Security Events

- User Access LevelLevels: Administrator, Standard User, Guest.
- Example:
  - Administrator: Full system control (e.g., admin_user).
  - Standard User: Limited resource access (e.g., john).
  - Guest: Read-only access (e.g., guest).
- Configuration:
- usermod -aG admin_group admin_user usermod -aG project_group john chmod 755 / public
- Monitor and Respond to Network Security Events
- Scenario: Suspicious logins detected.
- Actions:
  a. Reviewed logs.
  b. Blocked IP via firewall:
  c. ufw deny from 192.168.1.100
  d. Enabled 2FA and updated credentials.
  e. Notified users of the breach.
- Evidence: Log and firewall screenshots..