Basic Network Design

Agenda

- Review Basic Network Design Considerations

- Examine Typical Network Designs

- Discuss Wireless Network Designs

Data Security

- Reminders:

    - Data Security is Critical

    - Data Security Policy is Critical

    - Network Security is a Only Part of the Information Security Program

- See Also: TrueCrypt, PGP Desktop, Microsoft EFS, Microsoft BitLocker, Axcrypt, Credent Mobile Guardian, etc.

- There is a trend in the industry to focus much more highly on Data

Basic Network Design

- <u>Network Security Architectures</u> (Cisco Press) Sean Convery

- Numerous Design Examples

- Note: Wireless LANS p424-441

- Threat Analysis and Policy Driven Designs

- Special Considerations for Deployment Types: Applications, Identity Management, VPNs, VOIP, Wireless, Etc.

- Small, Medium, and Large Networks

Design Considerations

- Business Goals

- Security Requirements

- Size of the Organization

- Available Staff

- Budget

- Industry Standards "Best Practice"

Design Considerations

- Network Devices
- Security Devices
- Application Usage
- Identity Management
- Network Topology
- Security Zones
- Infrastructure, Power/Wiring/Cooling
- Redundancy and High Availability

Security System Design

- Sean's Ten Steps to Designing Security Systems, p467

  - Review Security Policy

  - Analyze Current Network

  - Select and Evaluate Products

  - Design a Rough Draft

  - Test Components

- Evaluate/Revise Design

- Finalize Design

- Implement 1st Phase
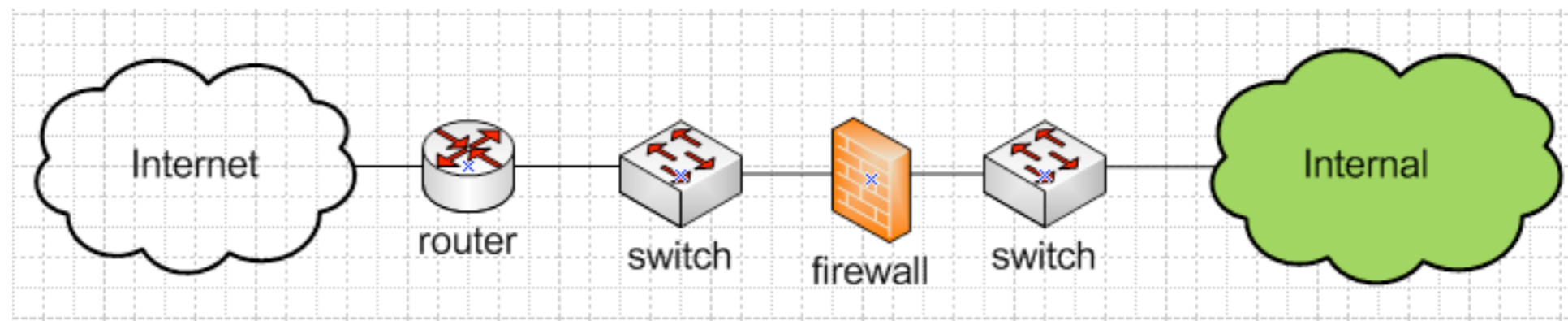
- Implement Remaining Phases

- Reevaluate

Simple Firewall Designs

- Router with ACL's, No Firewall

- Firewall Single Segment

- Firewall Unprotected DMZ
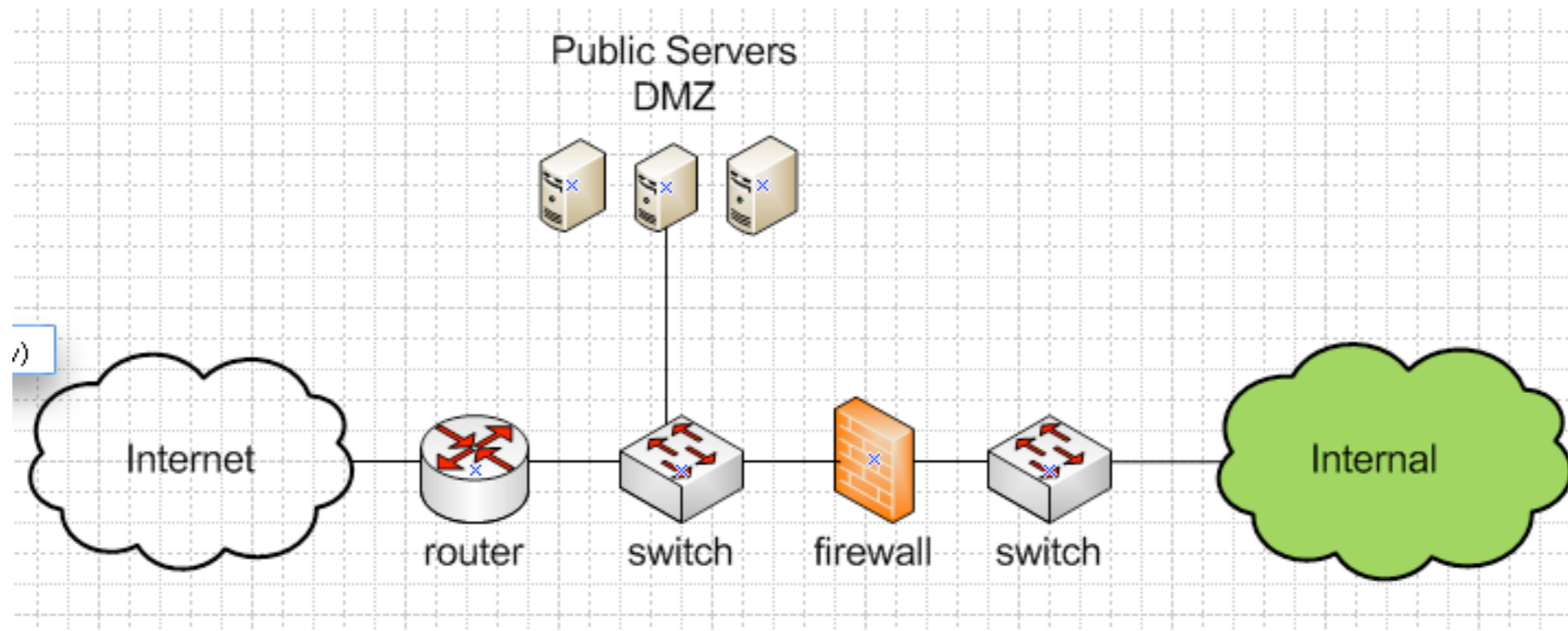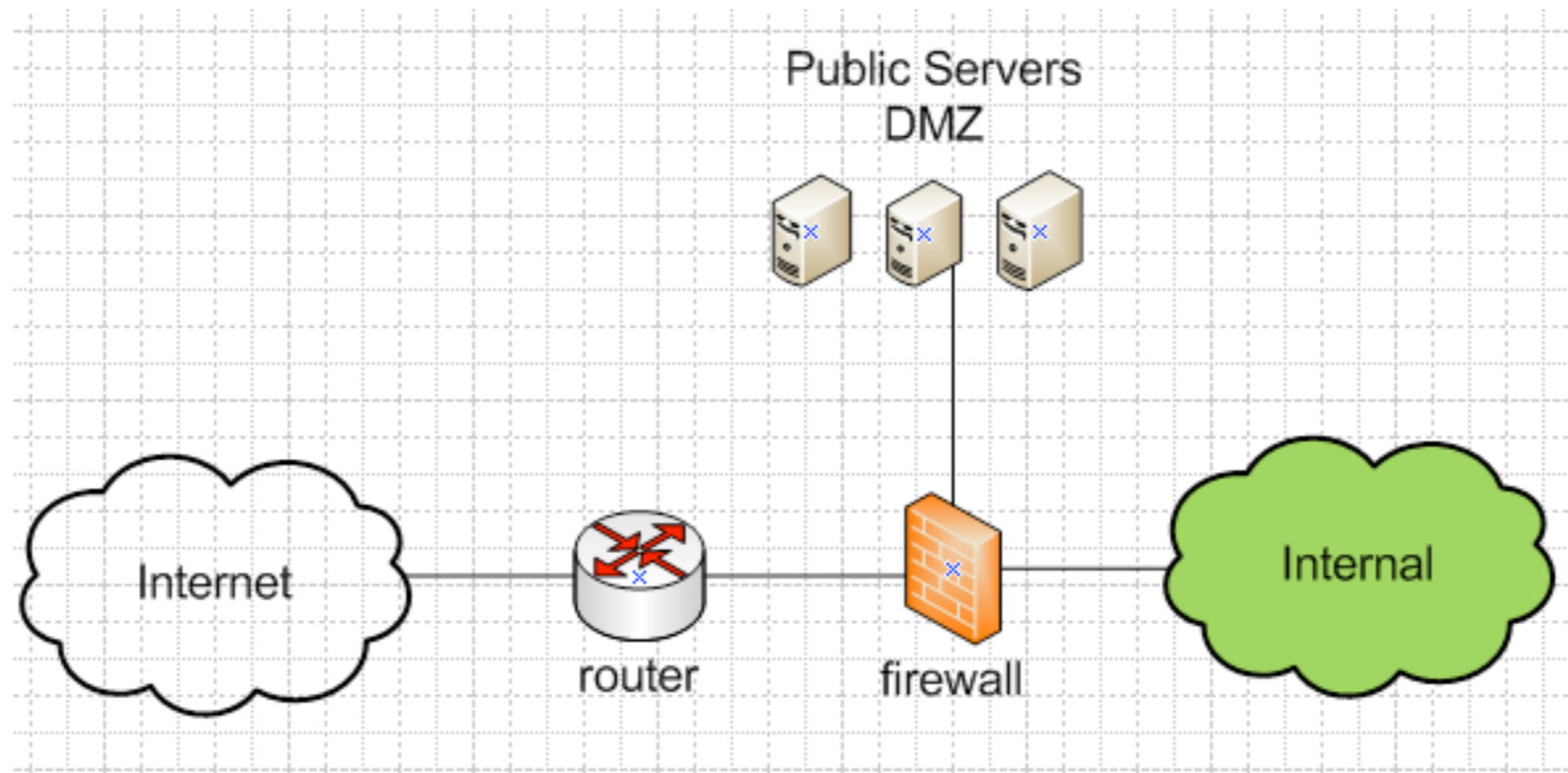
- Firewall With DMZ Segment

Router With ACLs
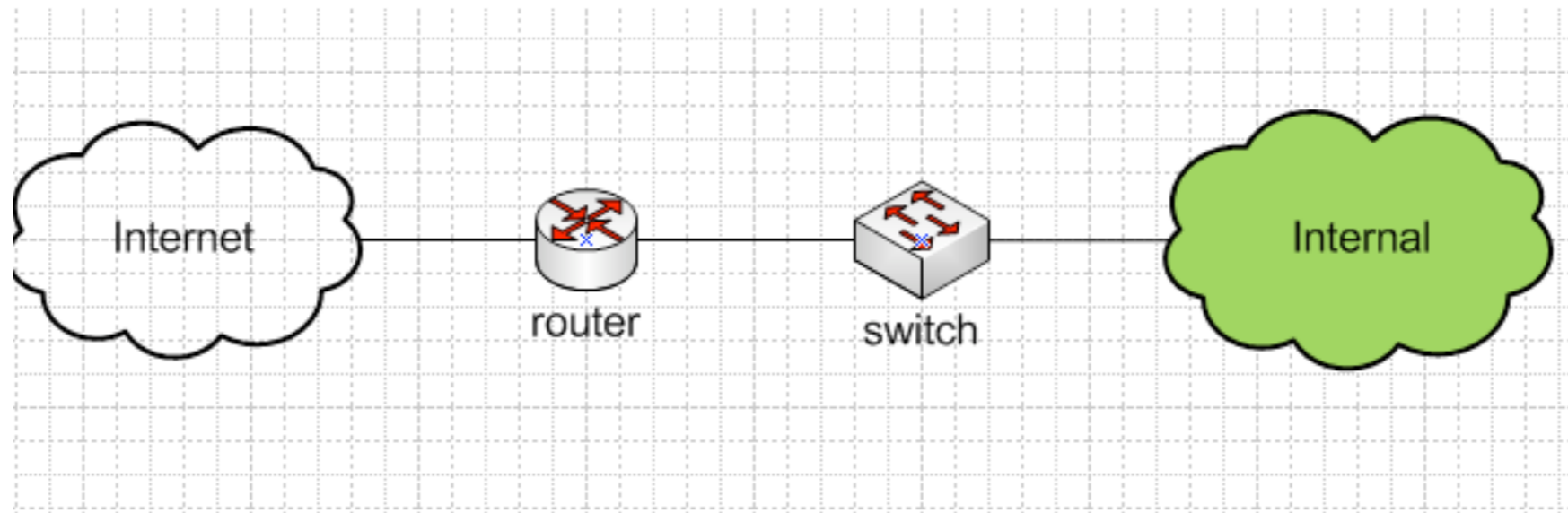
Firewall, Single Segment

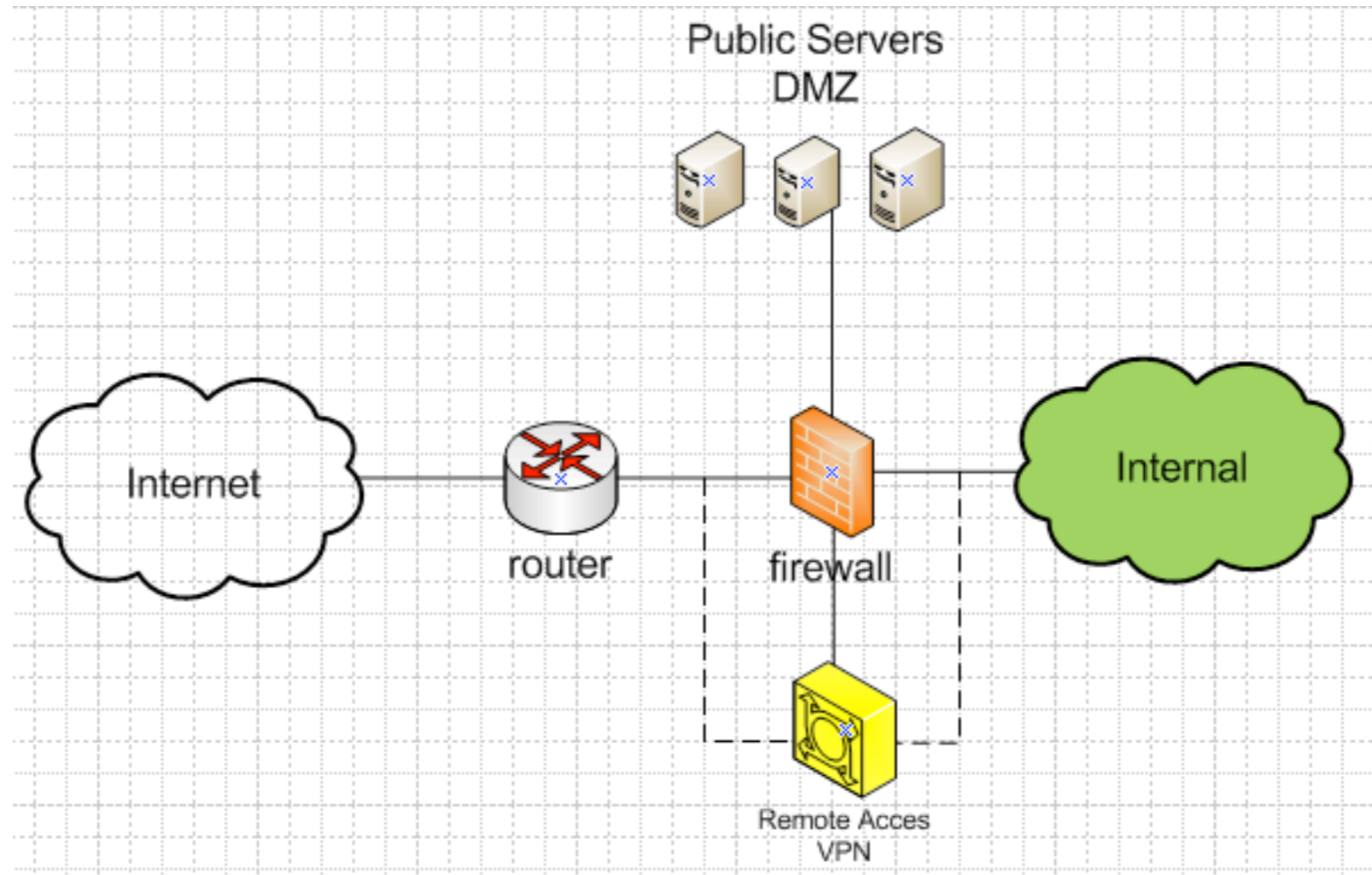# Firewall, Unprotected DMZ

Firewall, DMZ Segment

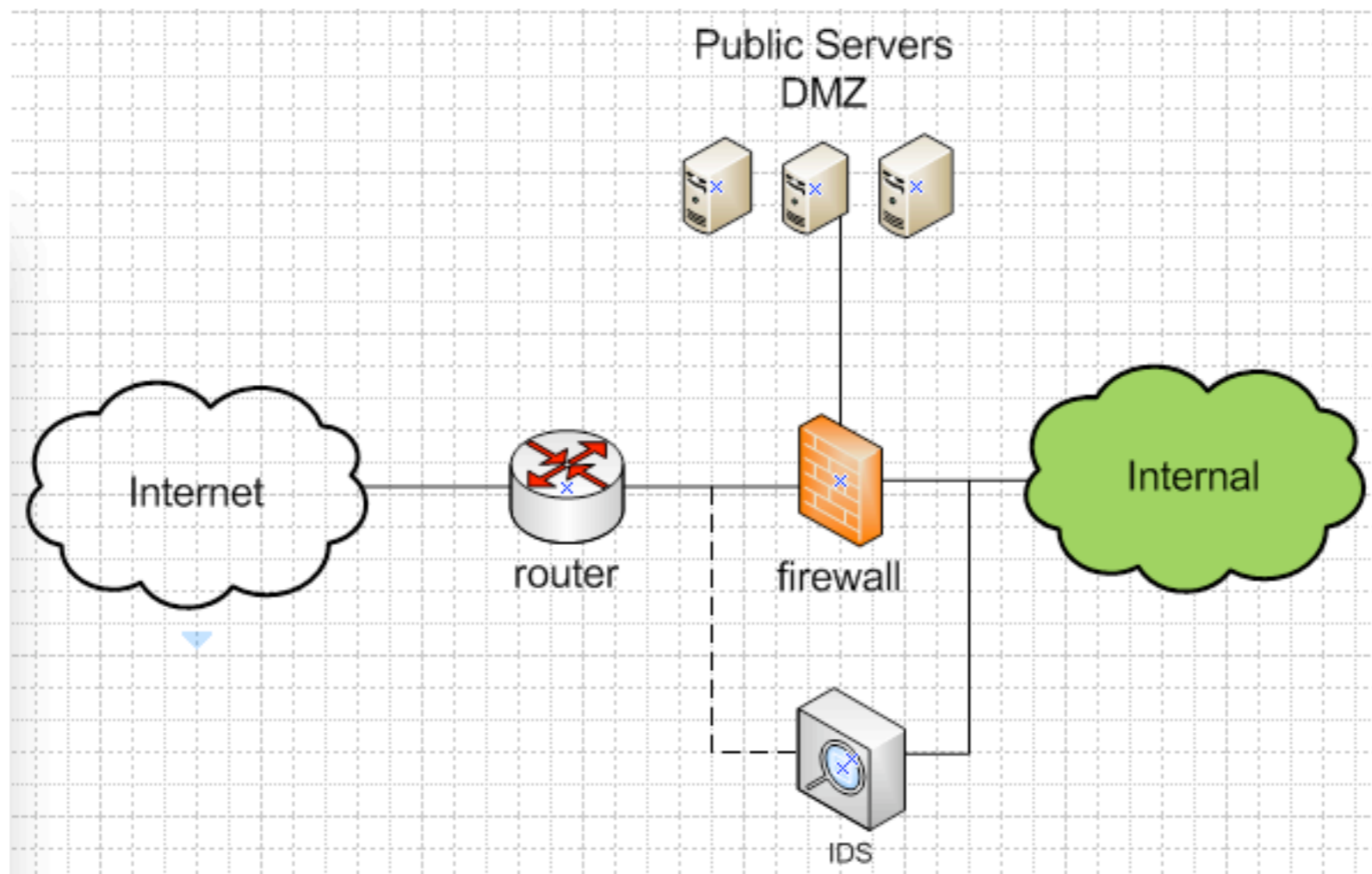Note: switches not shown to improve readability

VPN and IDS/IPS Designs

- VPN and IDS Designs

- Firewall Location Issues

- Security Permiter Issues

- IPS Is More Like a Firewall Than an IDS
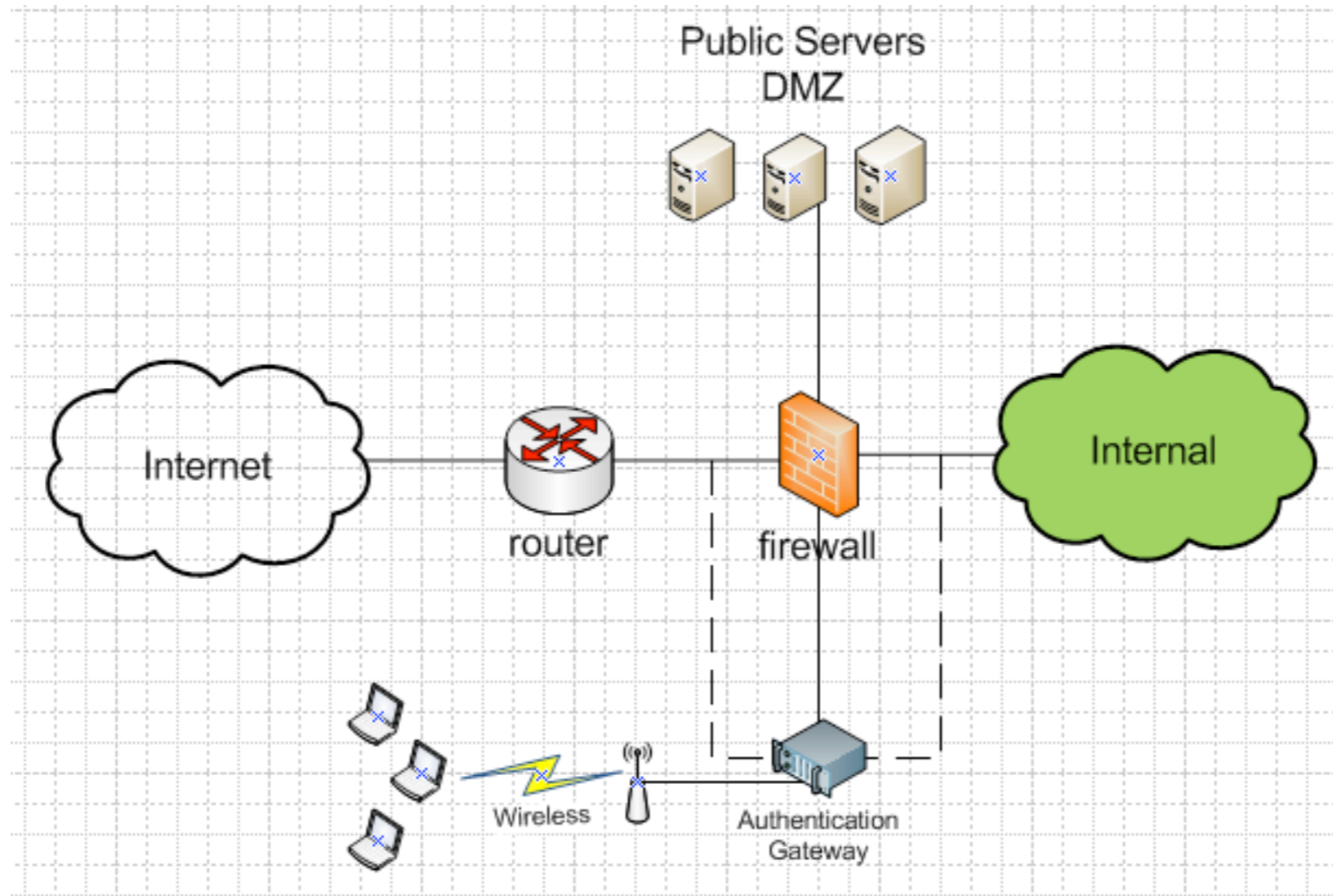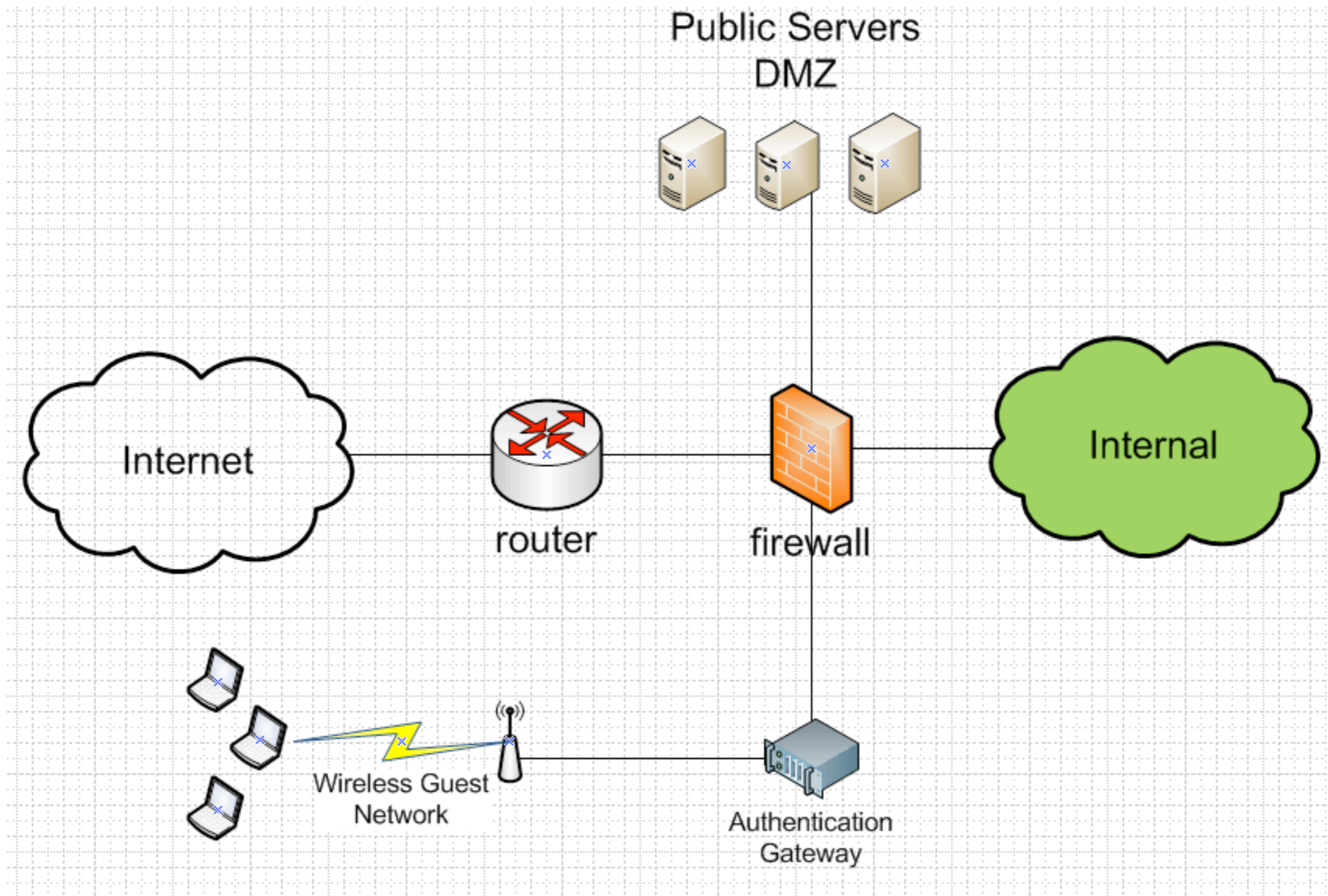
VPN and Firewall

IDS and Firewall

Wireless Designs

- Wireless LANS p424-441

  - Access Point Configuration

  - Rogue APs

  - Radio Issues

  - 802.1x, 80211i, SSL/TLS, IPSEC

  - Differentiated Group VLANS

    - Tend to be Proprietary

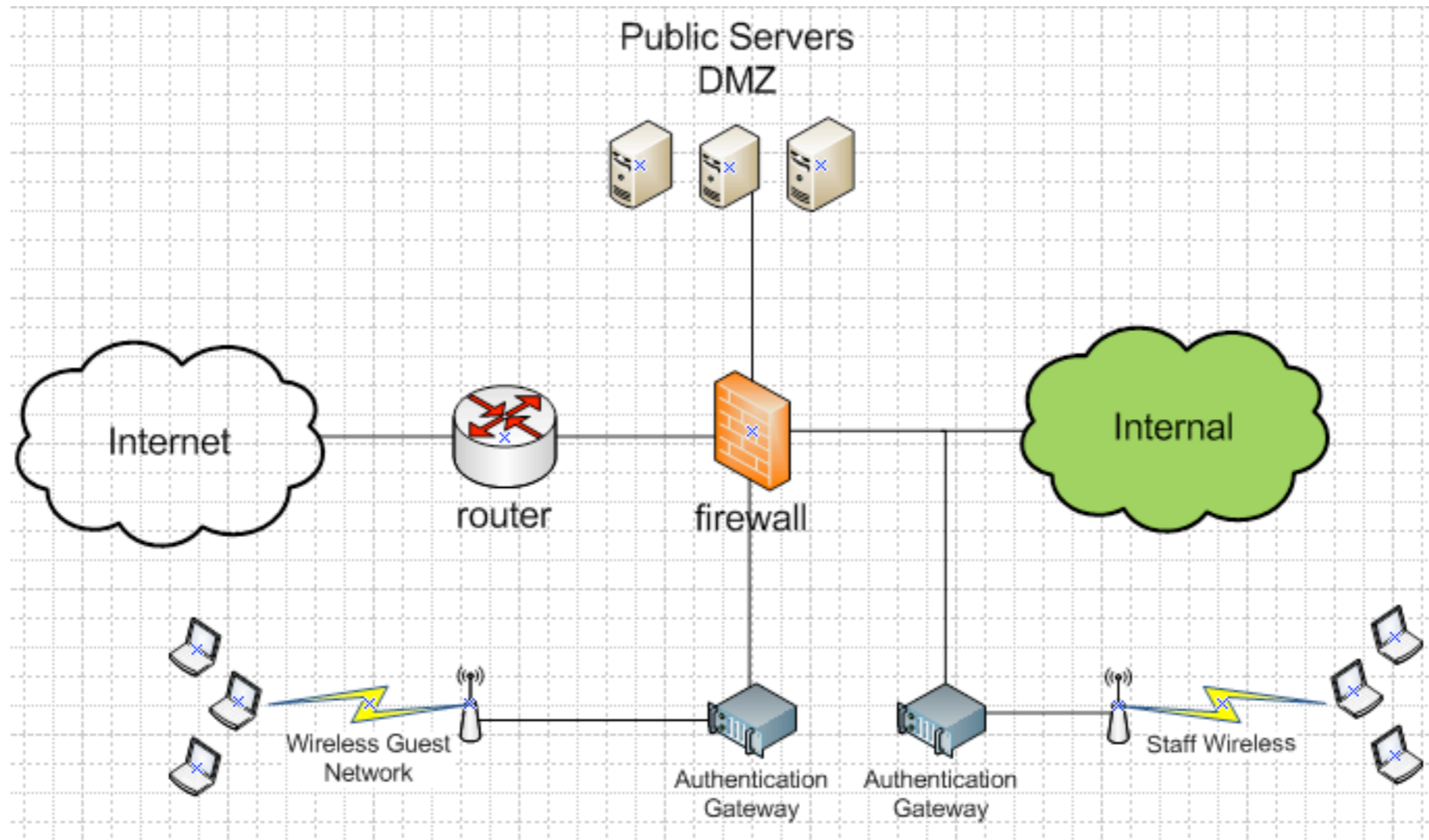   - Match each SSID to a VLAN

- More on All of the Above Later

Wireless Authentication Gateway

Wireless Guest

Wireless Multi-VLAN

Enterprise Designs

- Things can Get Complex Very Quickly

- How Large Is Your Enterprise

- What Kind of Design Is Manageable

Enterprise Design