Network Security (Principles & Practices)

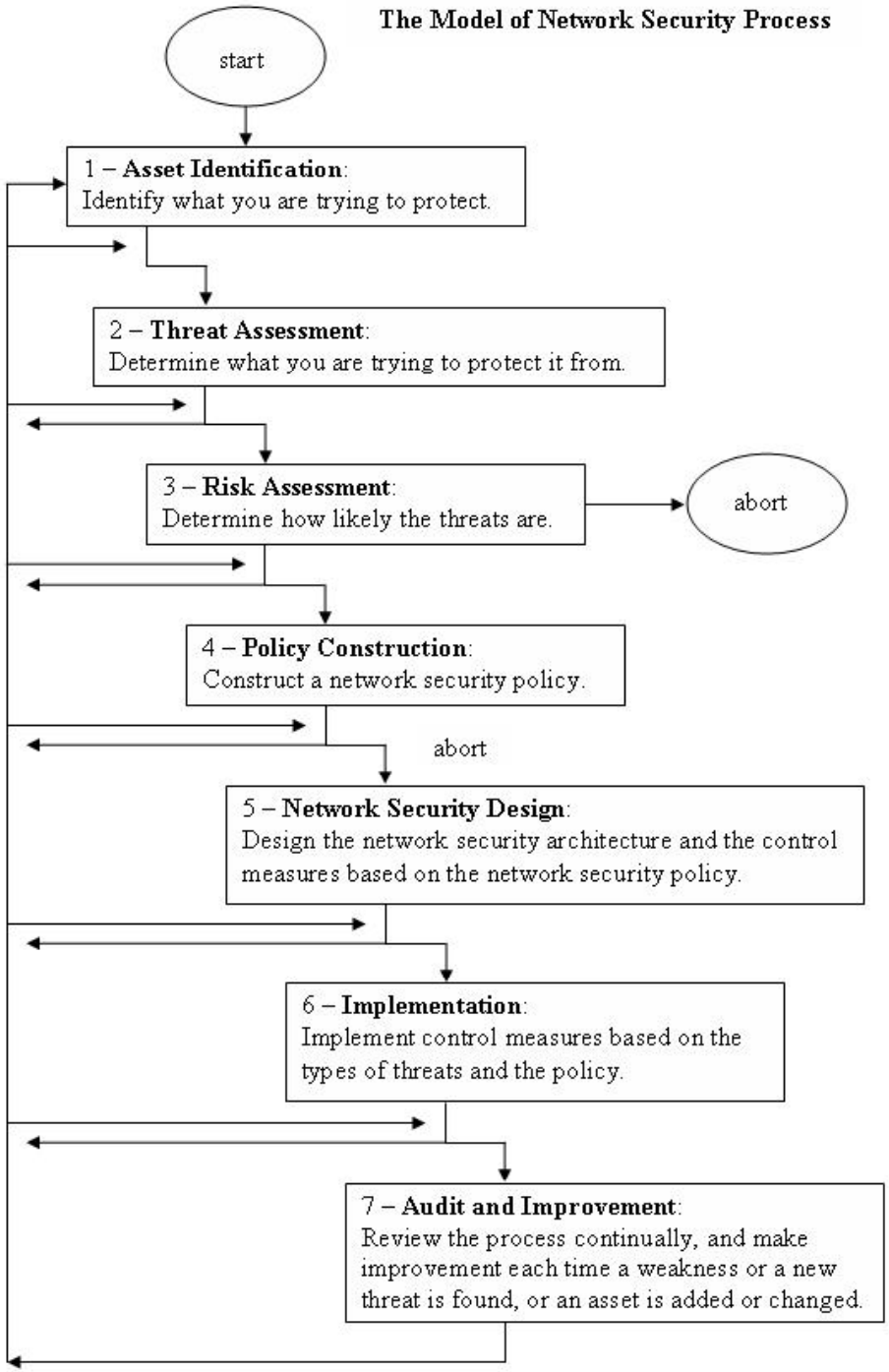
Outlines:

- Introduction to Network Security
- Defining Security Zones
- DMZ

By: Arash Habibi Lashkari
July - 2010

Introduction to Network Security

- Model of Network Security Process
- Elements of Network Security Policy
- Elements of Network Security Design
- Case Study


The Model of Network Security Process
start
1 – Asset Identification:
Identify what you are trying to protect.
2 – Threat Assessment:
Determine what you are trying to protect it from.
3 – Risk Assessment:
Determine how likely the threats are.
abort
4 – Policy Construction:
Construct a network security policy.
abort
5 – Network Security Design:
Design the network security architecture and the control measures based on the network security policy.
6 – Implementation:
Implement control measures based on the types of threats and the policy.
7 – Audit and Improvement:
Review the process continually, and make improvement each time a weakness or a new threat is found, or an asset is added or changed.

Elements of a Network Security Policy

1. Computer technology purchasing guidelines
   - security features
2. Privacy policy
   - emails, user data
3. Access policy
   - control of access to assets
4. Accountability policy
   - roles/responsibilities, auditing, incident handling
5. Authentication policy (identity management)
   - passwords, remote authentication, smart cards
6. Availability statement
   - expected availability, QoS, hours
7. Maintenance policy for IT system & network
   - esp. remote admin, outsourcing
8. Violations reporting policy
   - types of violations, anonymous reporting?
9. Supporting information
   - point(s) of contact, publicity, company policies, …

Network Security Design

Policies + Threats + Risk -> Policies

Policies + Policy Control measures (tools, procedures, etc.) -> Design

Elements of Network Security Design

- Device security features

  Admin passwords, Secure Shell
- Firewalls
- VPN

  Client-server VPN, site-to-site VPN
- IDS
- IPS
- Access control

  Access Control Lists, Committed Access Rate
- And more

Case Study

- Draw a network diagram to show the network security design of your department in the university
- There are four criteria in security please define them:

  confidentiality

  integrity

  availability

  and non-repudation

Defining Security Zones

- What are security zones?
- DMZ

Network Architecture

- The topological design of a network is one of the best defenses against network attacks.
- Using *zones* to segregate various areas of the network from each other.
- Different zones of the same network have different security needs.
- Better *scalability*

Zoning strategies

1. Greater security needs, more secure zones
2. Controlled access to zones
3. Publicly accessed servers are placed in separate zones from private servers.
4. To achieve highest security, each server is placed in a separate zone. Why?
5. The ‘defense in depth principle’

   - Firewalls are used to separate the zones.

DMZ

- Different ways of creating demilitarized zones:
  1. Using a 3-legged firewall
  2. Placing the DMZ outside the firewall

     'Bastion hosts' are placed in the DMZ.

     a) In the path between a firewall and the Internet

     b) Dirty DMZ

     Rationale ?
  3. Placing the DMZ between stacked firewalls

DMZ Categories

Simple DMZ

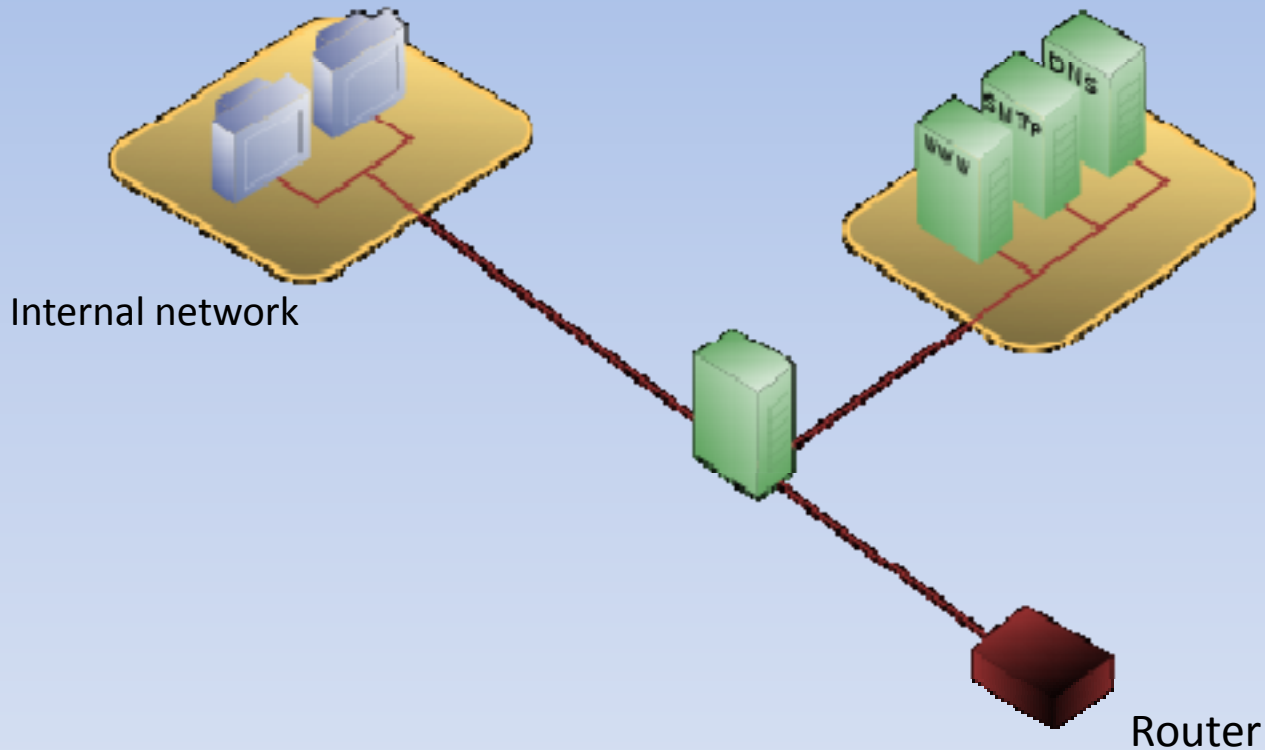
single subnet between the internet and intranet and

contains all the servers that have some public exposure

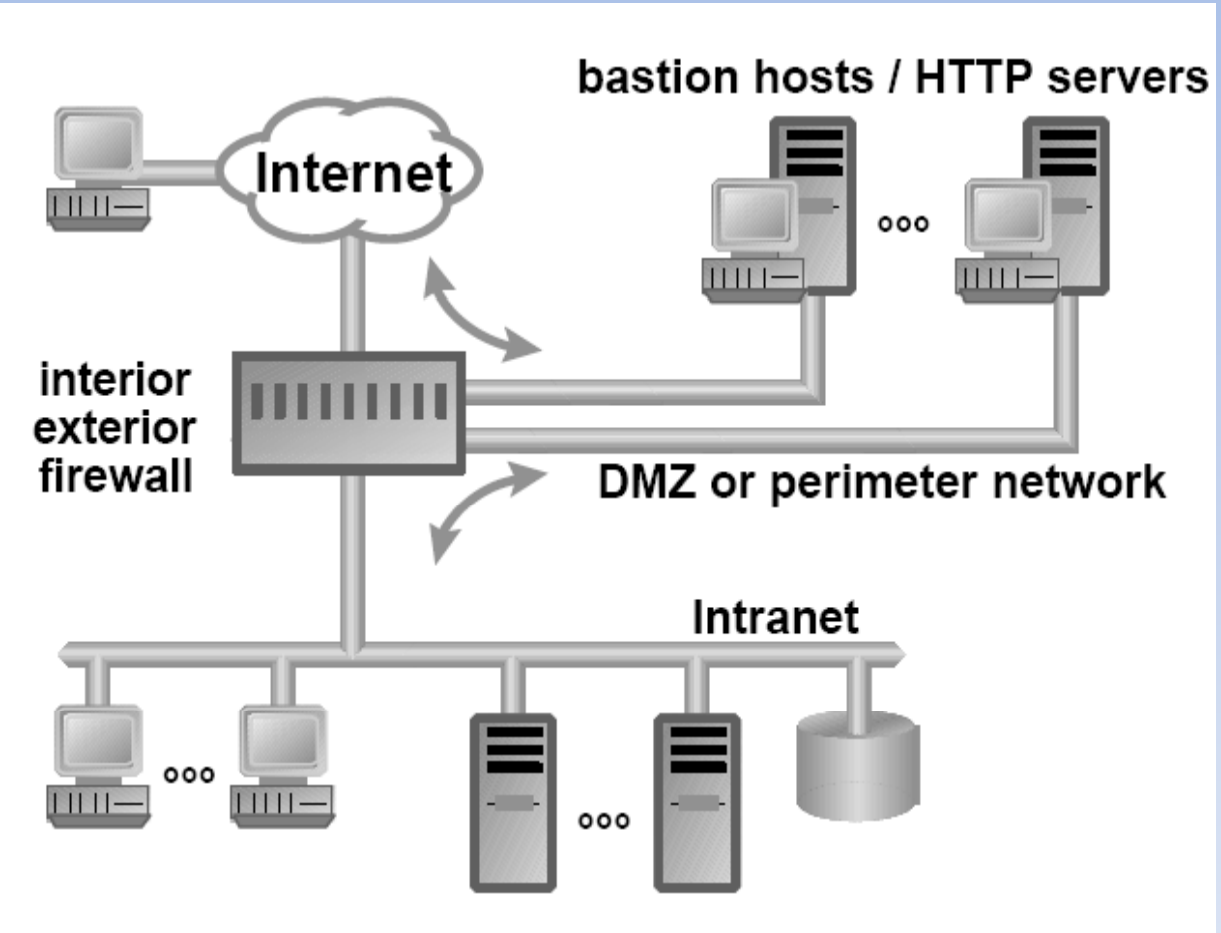
Tiered DMZ

Multi subnet between the internet and intranet.

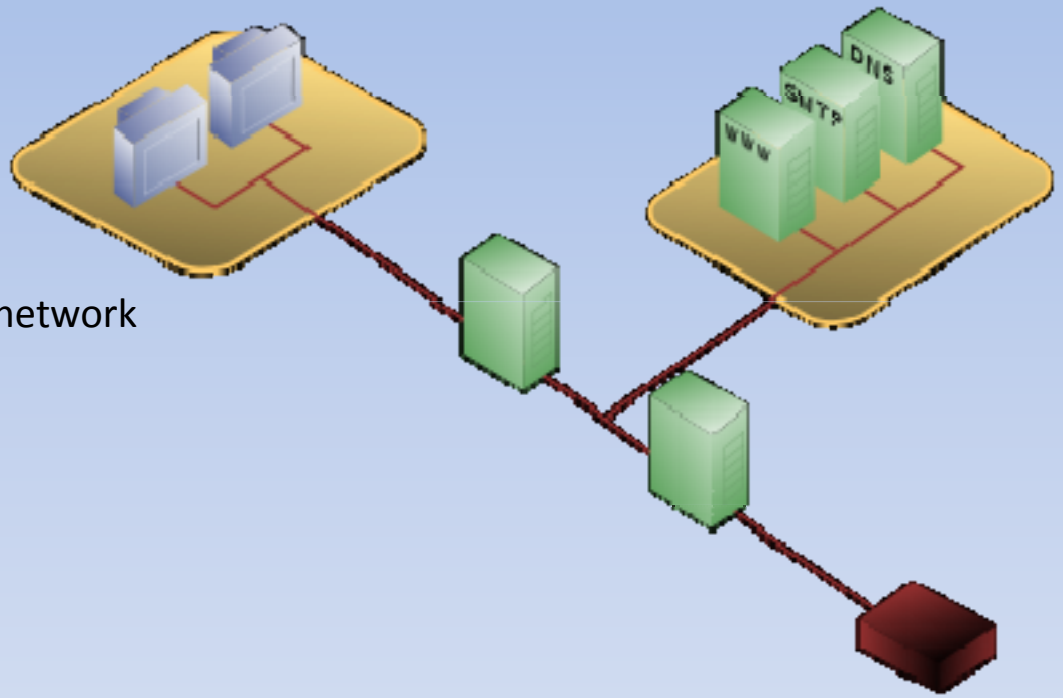
Simple DMZ



Simple DMZ


bastion hosts / HTTP servers
Internet
ooo
interior
exterior
firewall
DMZ or perimeter network
Intranet
ooo
ooo

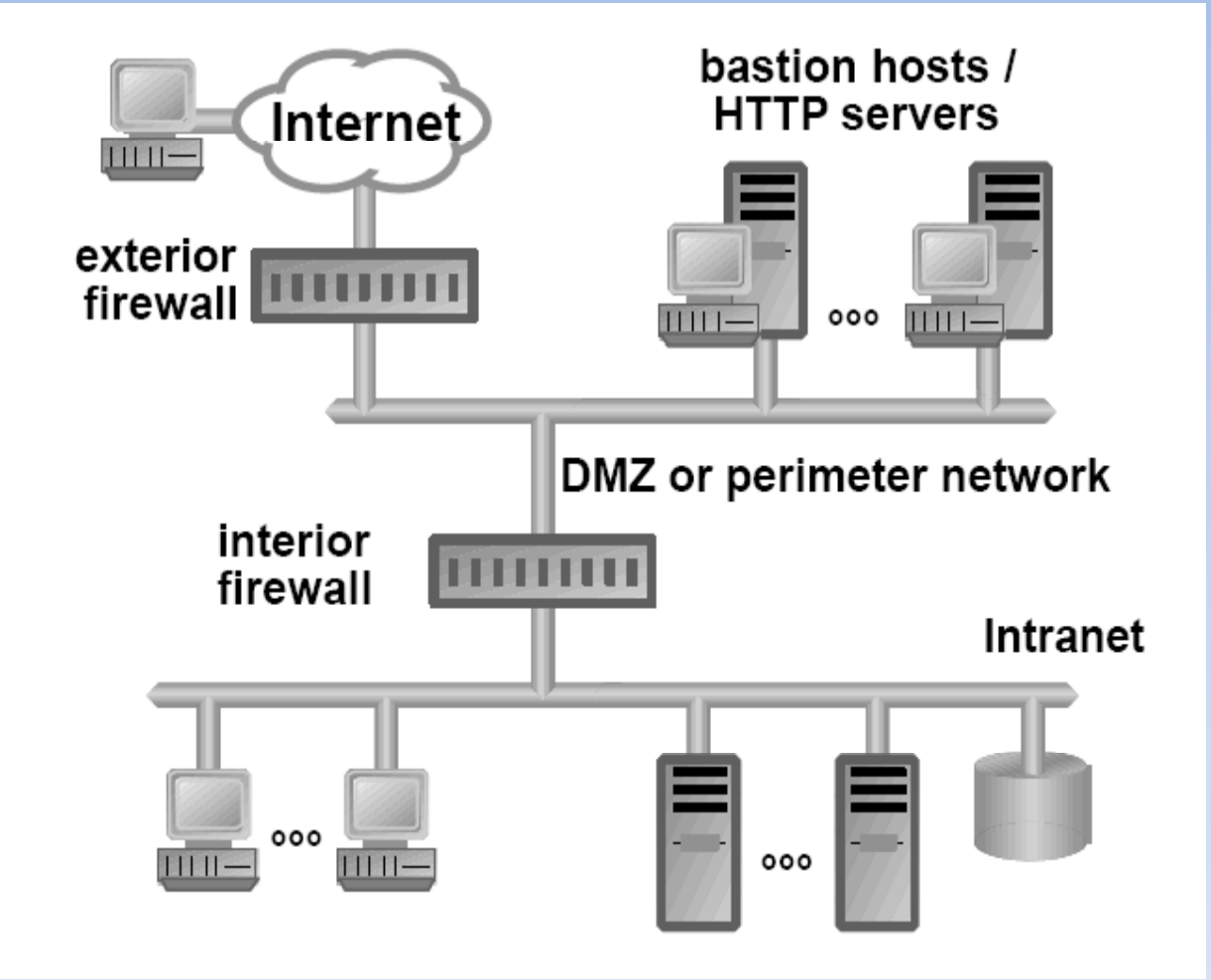
Two tier DMZ



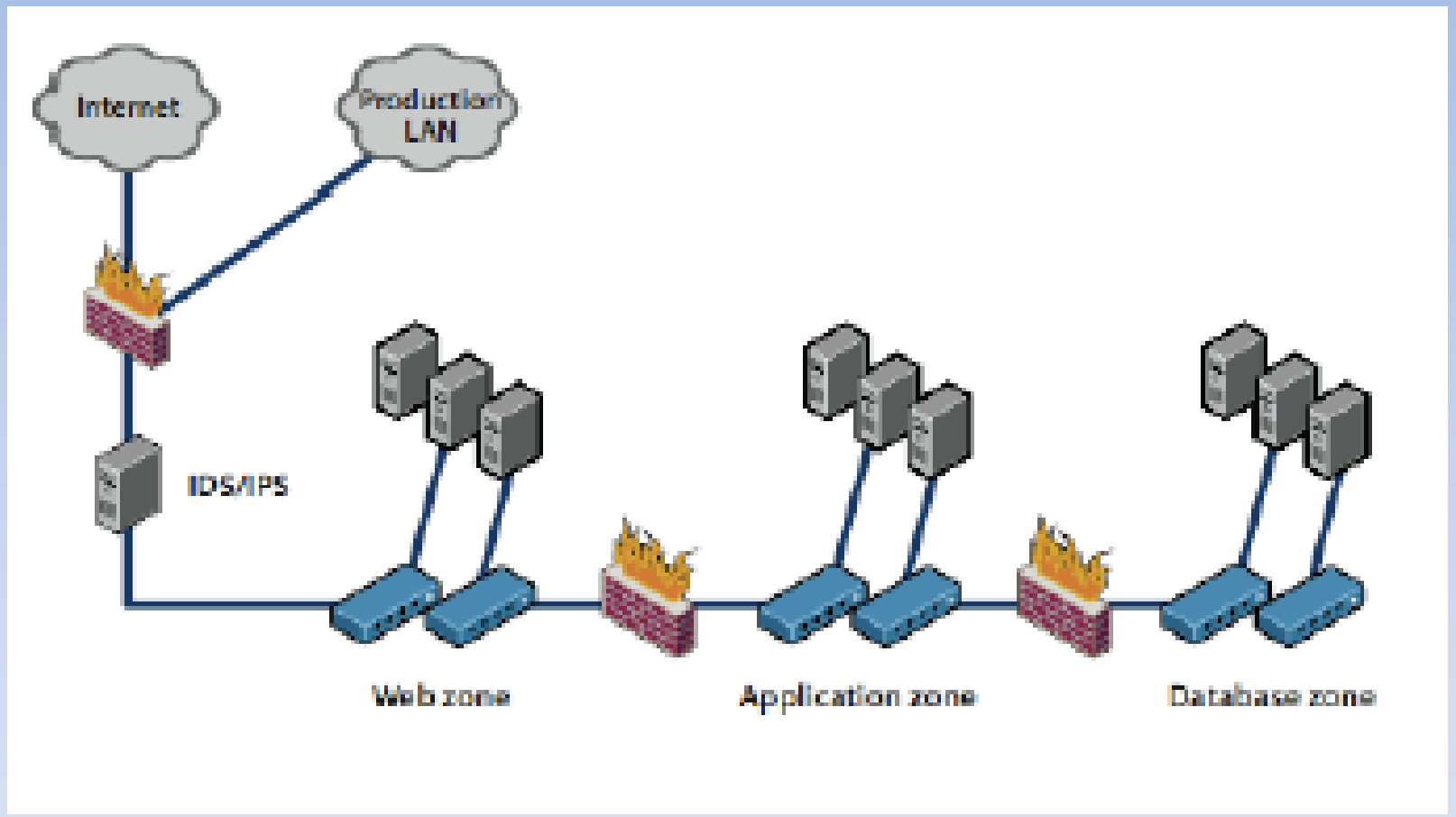
Internal network

Router to external network

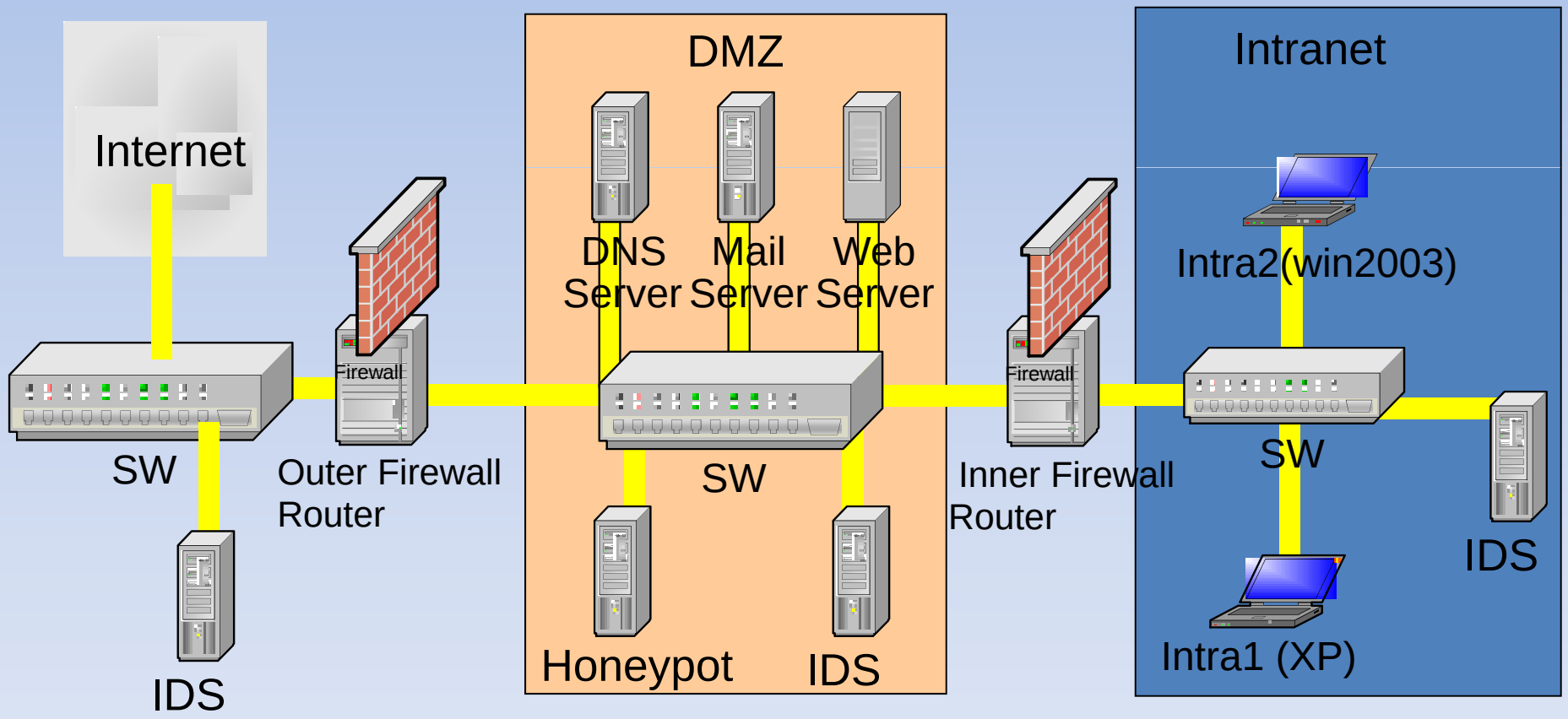
Two tier DMZ


Internet
bastion hosts /
HTTP servers
exterior
firewall
DMZ or perimeter network
interior
firewall
Intranet

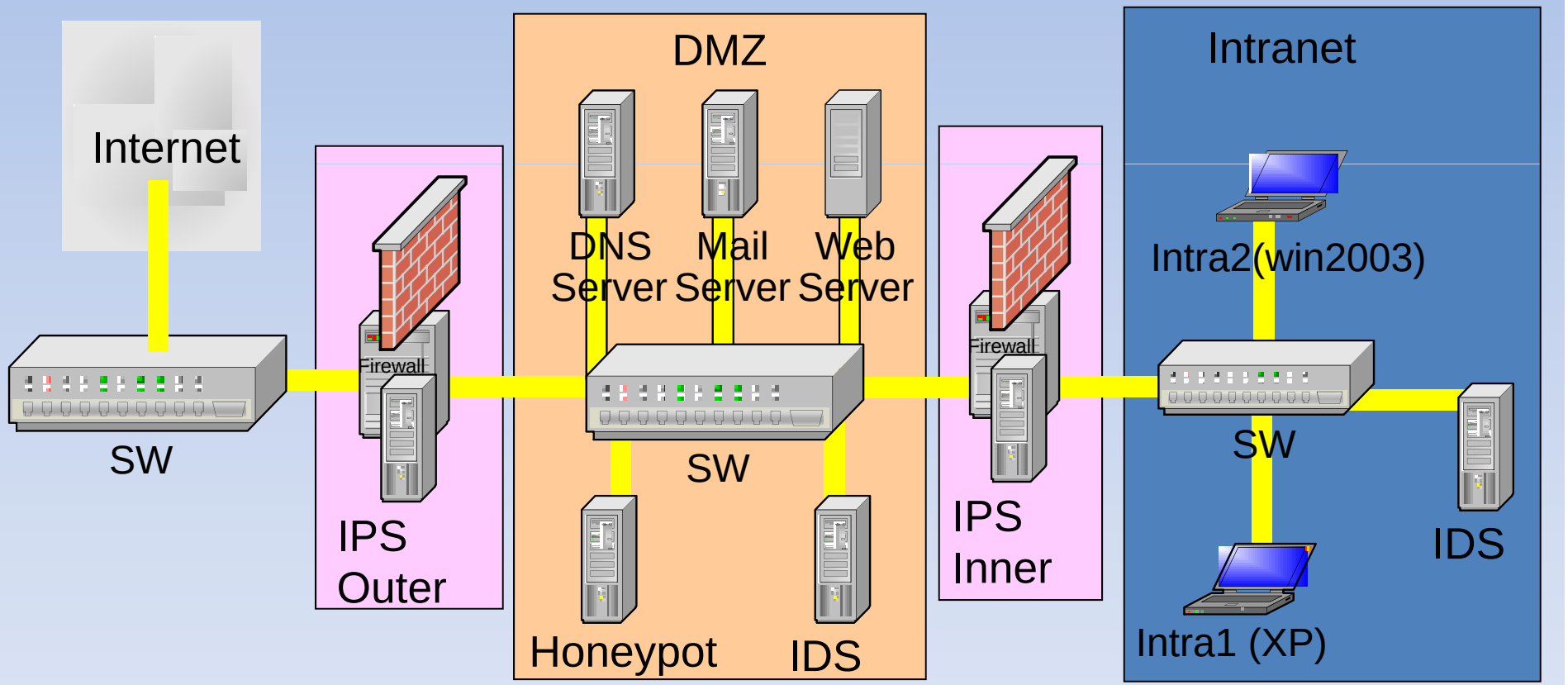
Three tier DMZ



Perimeter Defense and Firewall



Intrusion Prevent System (IPS) combining Firewall with IDS



Sample Security Policies (1)

- The DMZ servers are typically not allowed make connections to the intranet.
- Systems in Internet not allowed to directly contact any systems in the intranet.
- Systems in Intranet not allowed to directly contact any systems in the Internet. (least privilege principle)
- Systems in DMZ serve as mediator (go-between). Password/certificate/credential are presented for allowing mediating services.
- No dual interface from DMZ servers directly to systems Intranet except the inner firewall.

Sample Security Policy (2)

- Intranet system typically uses Private LAN addresses: 10.x.y.z/8; 172.a.x.z/16; 192.168.x.y/24.
- Complete Mediation Principle: inner firewall mediate every access involves with DMZ and Intranet.
- Separation of privileges; with different DMZ server running different network functions; firewall machines are different entities than the DMZ servers.
- It is also related to least common mechanism principle.
- The outer firewall allows HTTP/HTTPS and SMTP access to DMZ server. Need to detect virus, malicious logic.

Questions