An Introduction to Firewall Technology

Amirkabir University of Technology
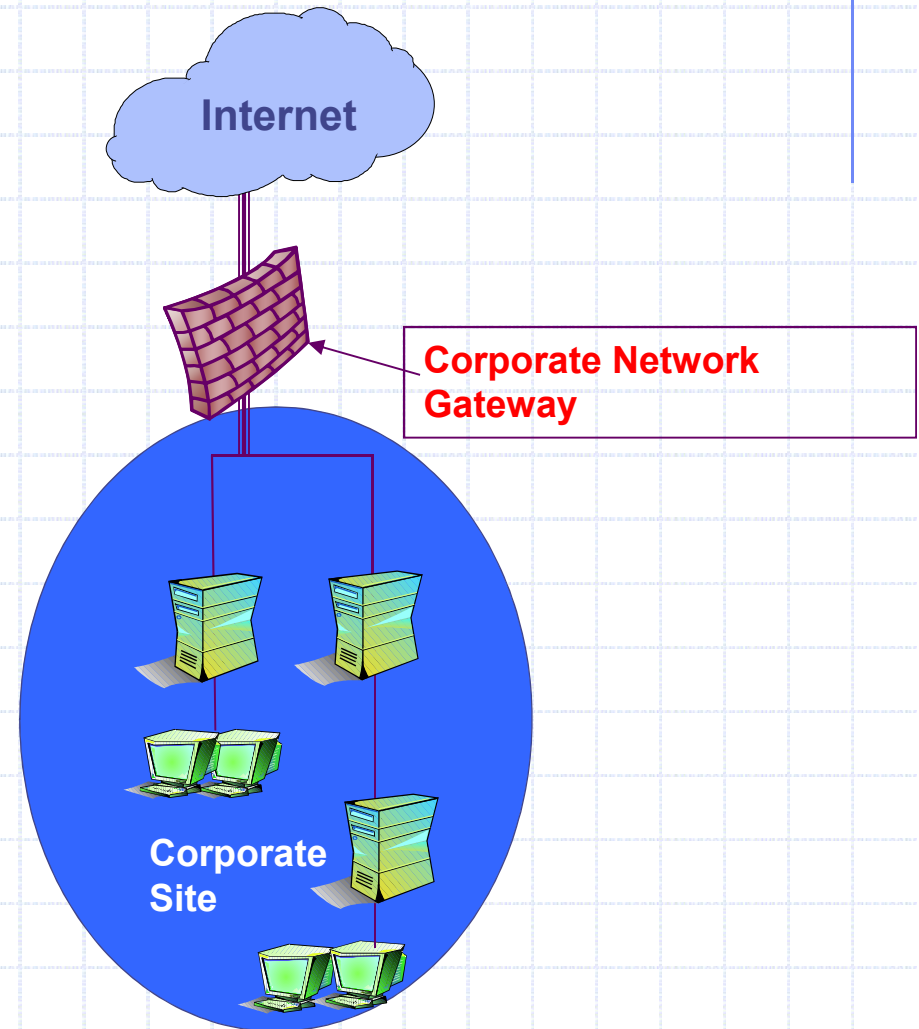
Agenda

- What is a firewall
- Why an organization needs a firewall
- Types of firewalls and technologies
- Deploying a firewall

What is a Firewall ?

◆ A firewall :

- Acts as a security gateway between two networks

  - ◆ Usually between trusted and untrusted networks (such as between a corporate network and the Internet)

Internet

Corporate Network Gateway

Corporate Site

What is a Firewall ?

◆ A firewall :

- Acts as a security gateway between two networks

- Tracks and controls network communications

  - Decides whether to pass, reject, encrypt, or log communications (Access Control)
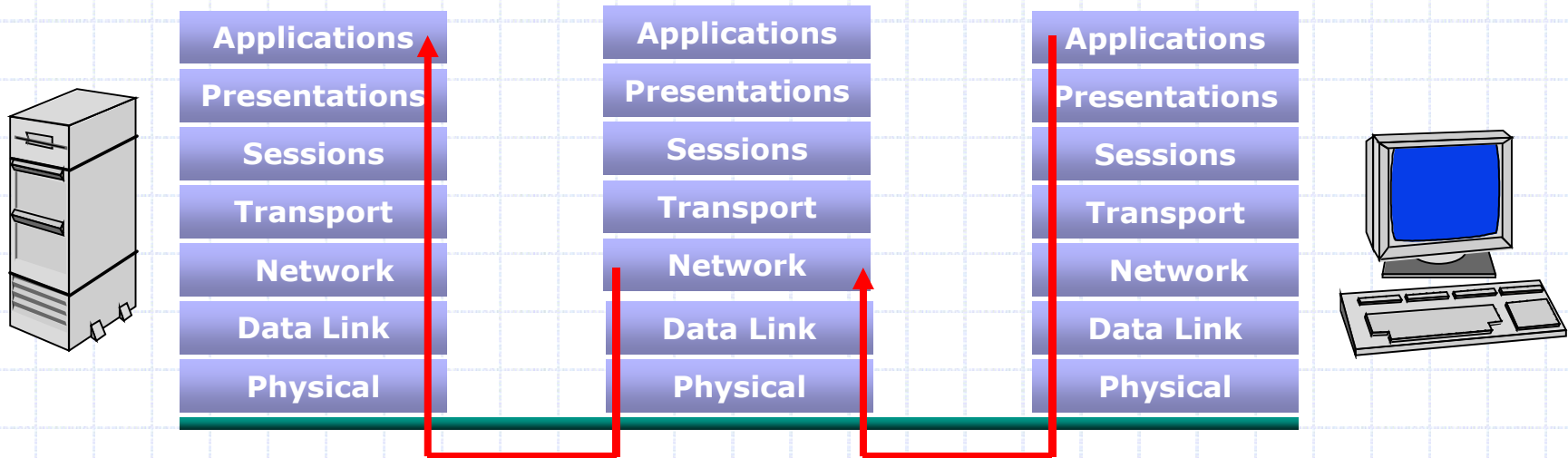
Internet

Corporate Site
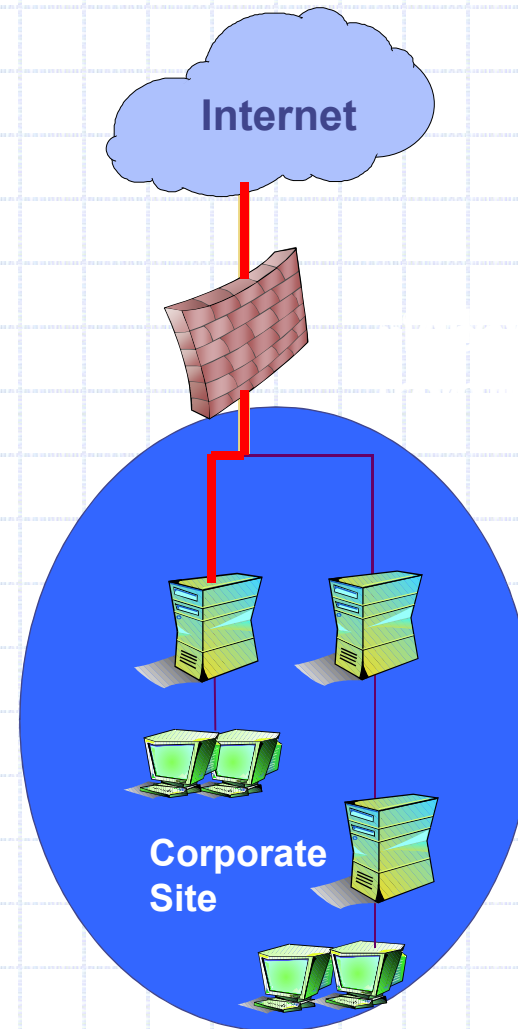
Why Firewalls are Needed

- Prevent attacks from untrusted networks
- Protect data integrity of critical information
- Preserve customer and partner confidence

Evolution of Firewalls

Stateful Inspection

Application Proxy

Packet Filter

Stage of Evolution
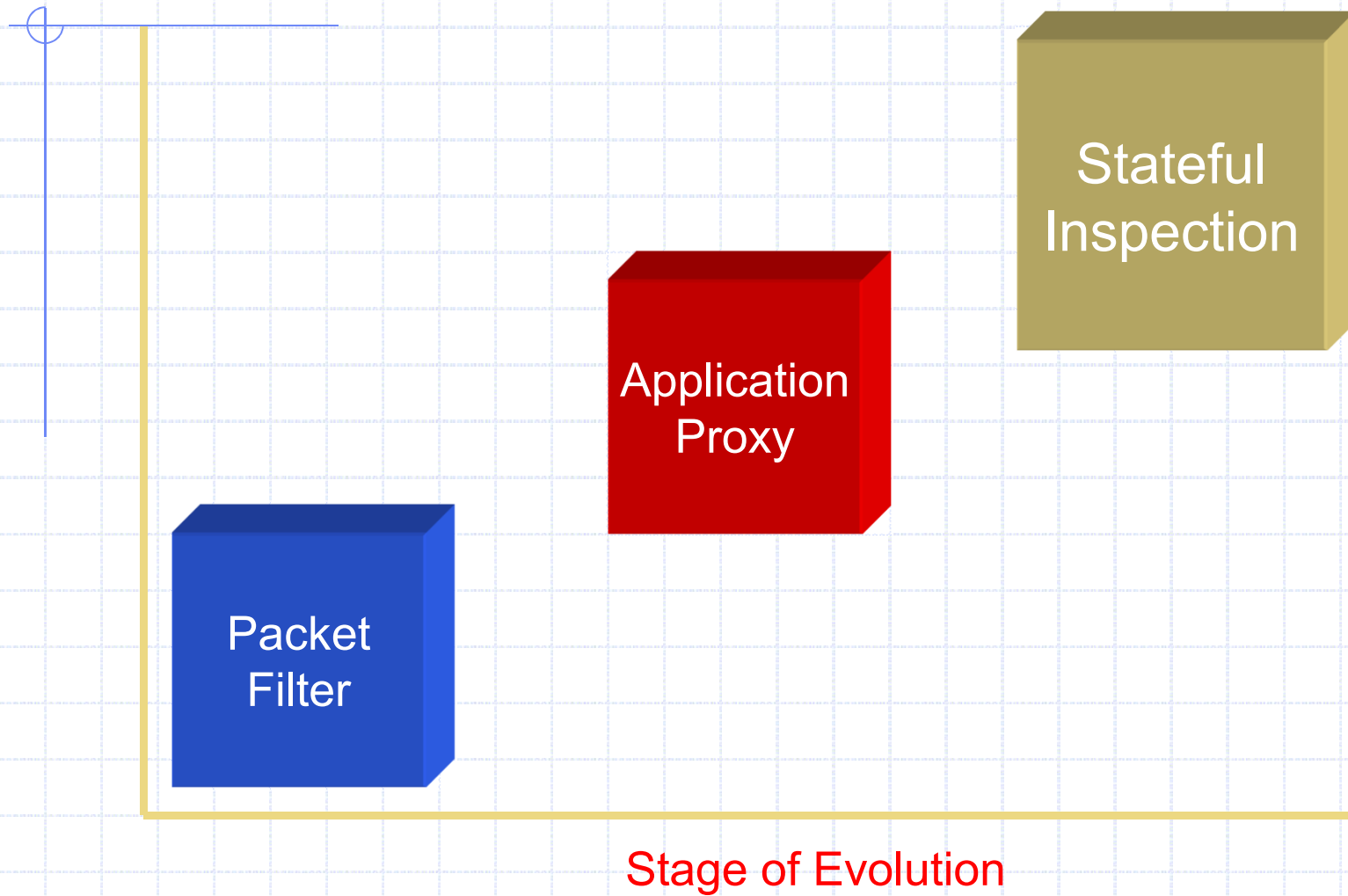
Packet Filter

◆ Packets examined at the network layer

◆ Useful "first line" of defense - commonly deployed on routers

◆ Simple accept or reject decision model

◆ No awareness of higher protocol layers

Applications	Applications	Applications
Presentations	Presentations	Presentations
Sessions	Sessions	Sessions
Transport	Transport	Transport
Network	Network	Network
Data Link	Data Link	Data Link
Physical	Physical	Physical

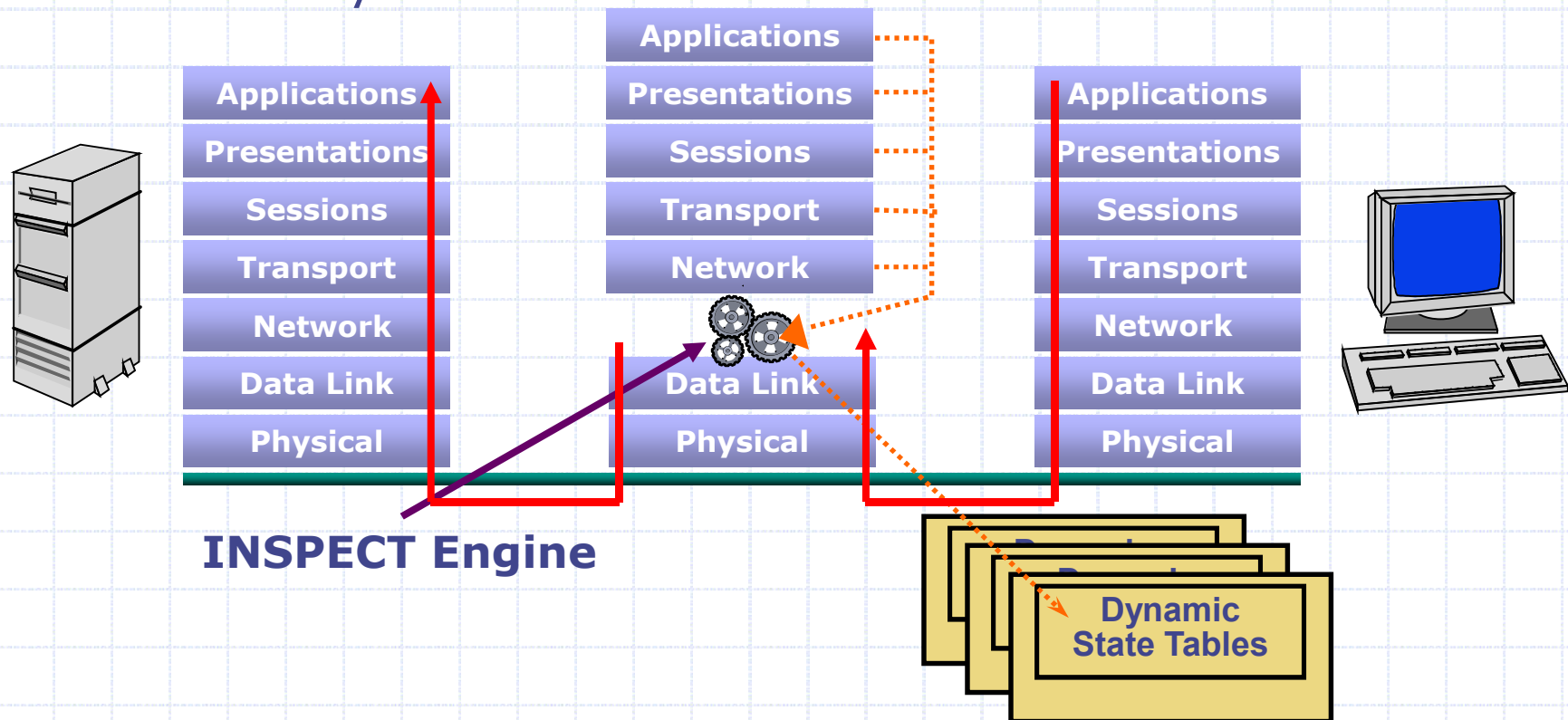# Application Gateway or Proxy

◆ Packets examined at the application layer

◆ Application/Content filtering possible - prevent FTP "put" commands, for example

◆ Modest performance

◆ Scalability limited

Applications
Presentations
Sessions
Transport
Network
Data Link
Physical

Applications
Presentations
Sessions
Transport
Network
Data Link
Physical

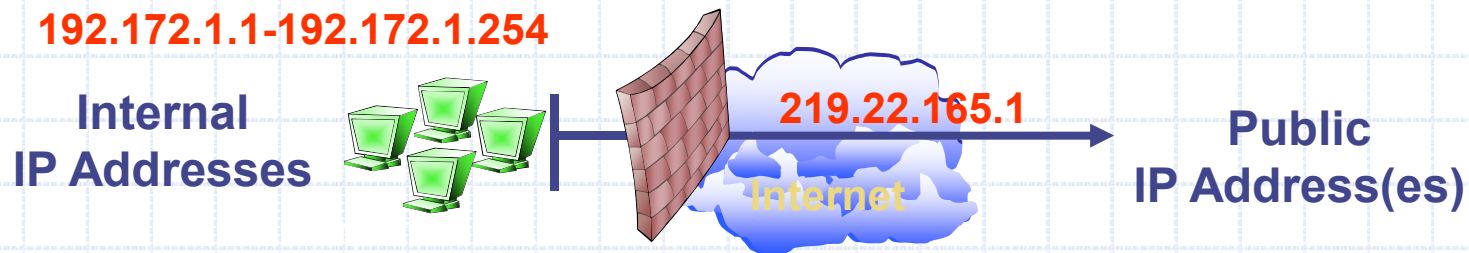| Applications |
|---|
| Presentations |
| Sessions |
| Transport |
| Network |
| Data Link |
| Physical |
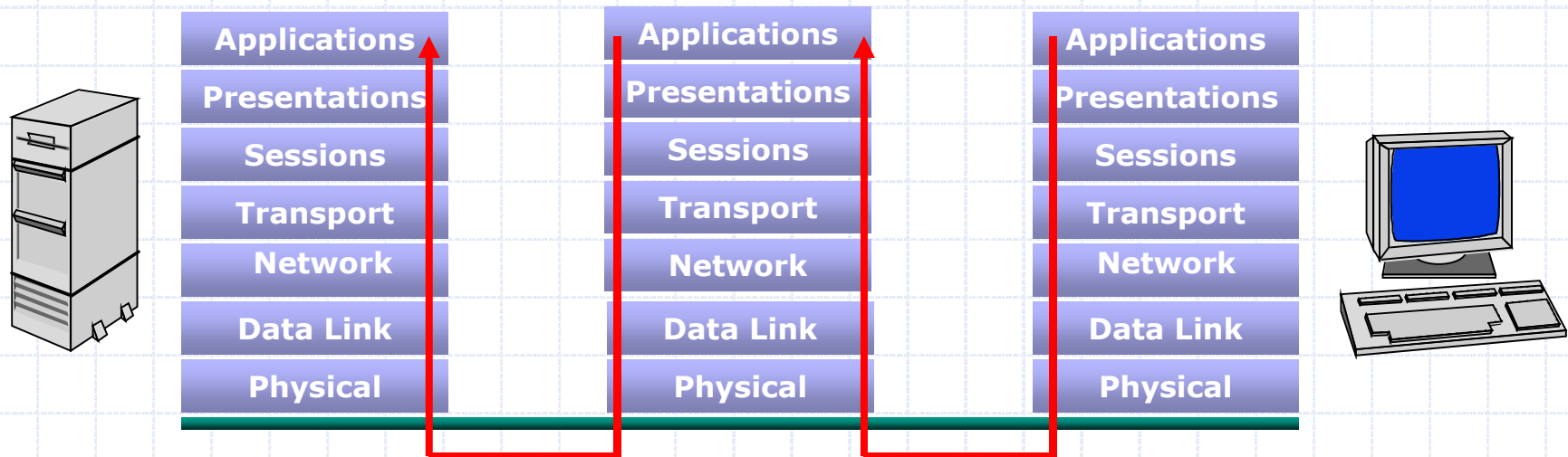
Stateful Inspection

◆ Packets Inspected between data link layer and network layer in the OS kernel

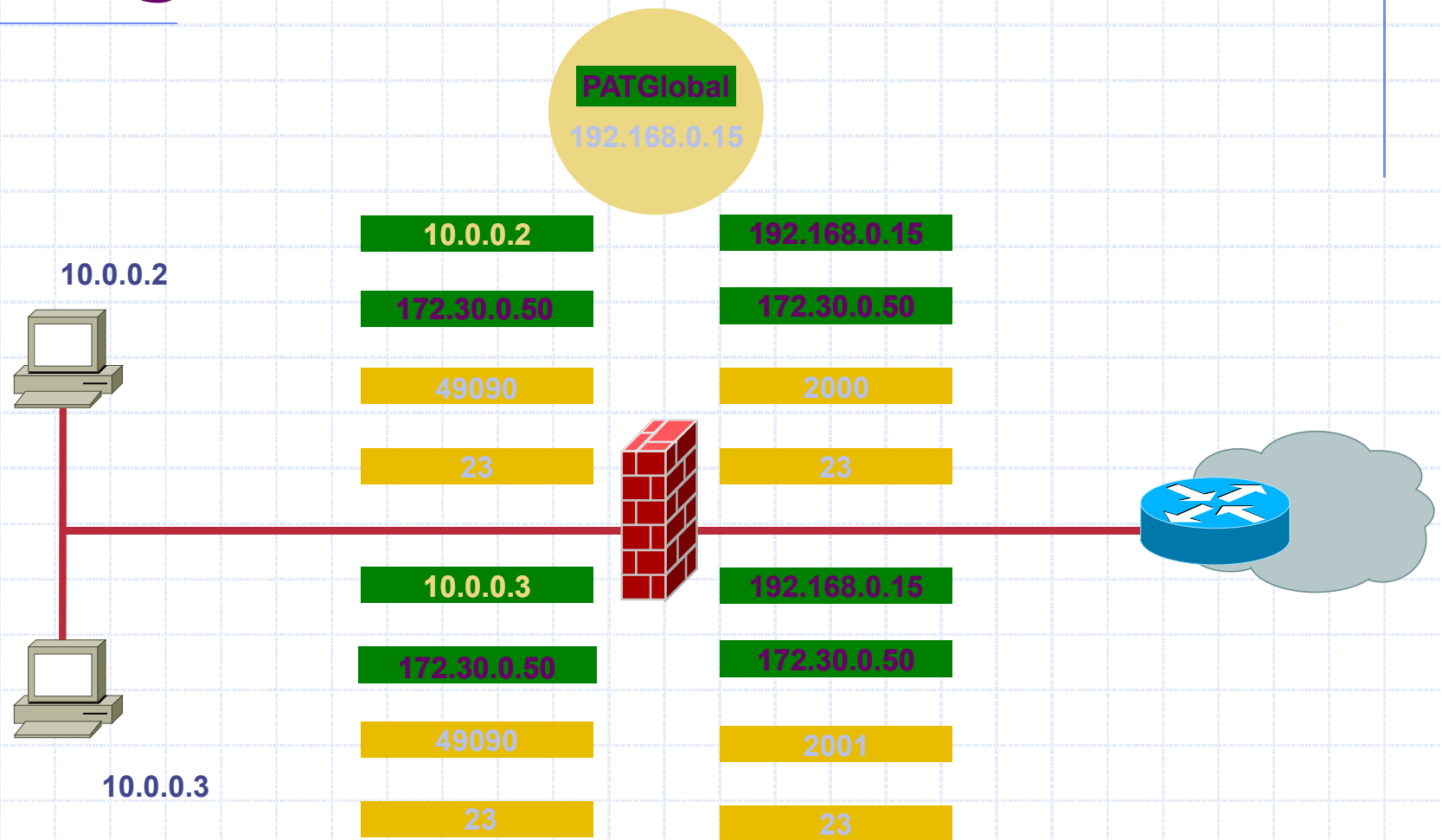◆ State tables are created to maintain connection context

◆ Invented by Check Point

Applications	
Presentations	
Sessions	
Transport	
Network	

Applications	
Presentations	
Sessions	
Transport	
Network	
Data Link	
Physical	

Applications	
Presentations	
Sessions	
Transport	
Network	
Data Link	
Physical	

INSPECT Engine

Dynamic State Tables

Network Address Translation (NAT)

192.172.1.1-192.172.1.254

**Internal
IP Addresses**

219.22.165.1

Internet

**Public
IP Address(es)**

◆ Converts a network's illegal IP addresses to legal or public IP addresses

- Hides the true addresses of individual hosts, protecting them from attack
- Allows more devices to be connected to the network

Port Address Translation— Hiding

PATGlobal
192.168.0.15

10.0.0.2	192.168.0.15
172.30.0.50	172.30.0.50
49090	2000
23	23

10.0.0.2

10.0.0.3	192.168.0.15
172.30.0.50	172.30.0.50
49090	2001
23	23

10.0.0.3

Personal Firewalls

- Need arises from always on connections
- Your PC is not protected enough by your OS
- Intrusion detection facilities
- Different levels of security
  - Templates

Firewall Deployment

◆ Corporate Network Gateway

- Protect internal network from attack
- Most common deployment point

Internet

Corporate Network Gateway

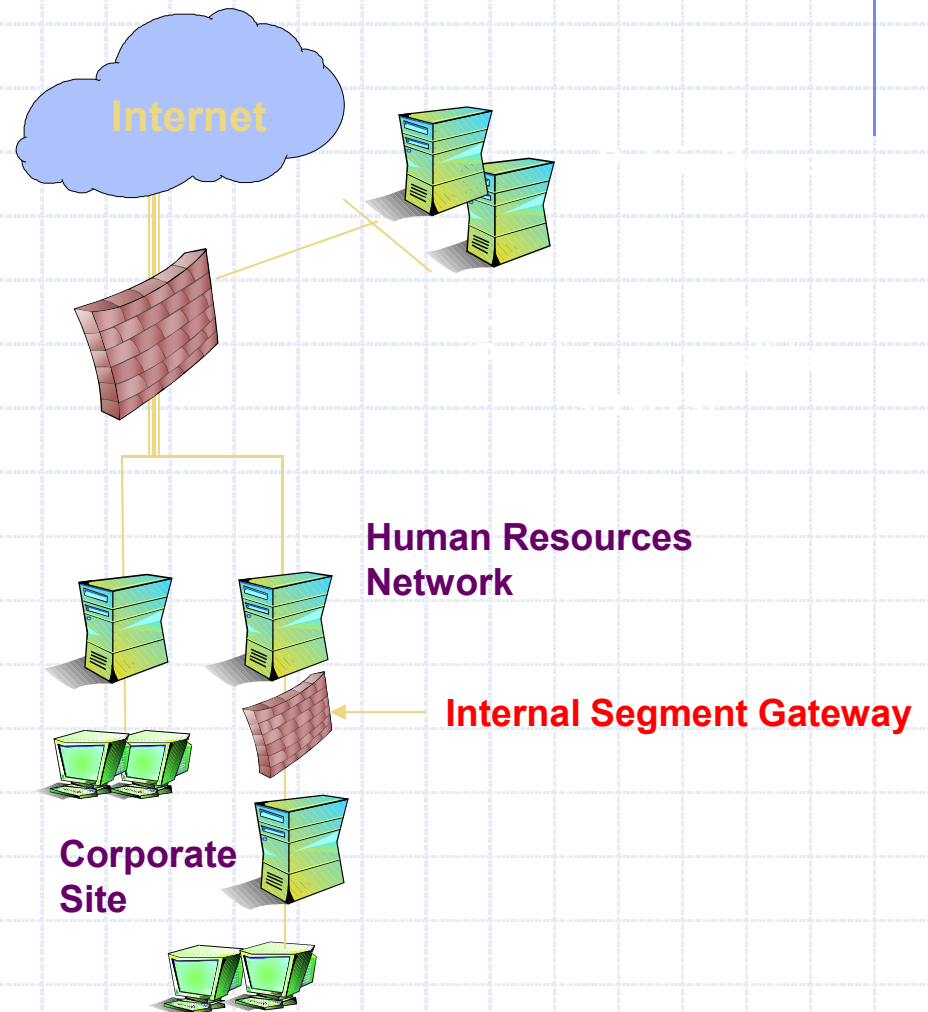**Human Resources Network**
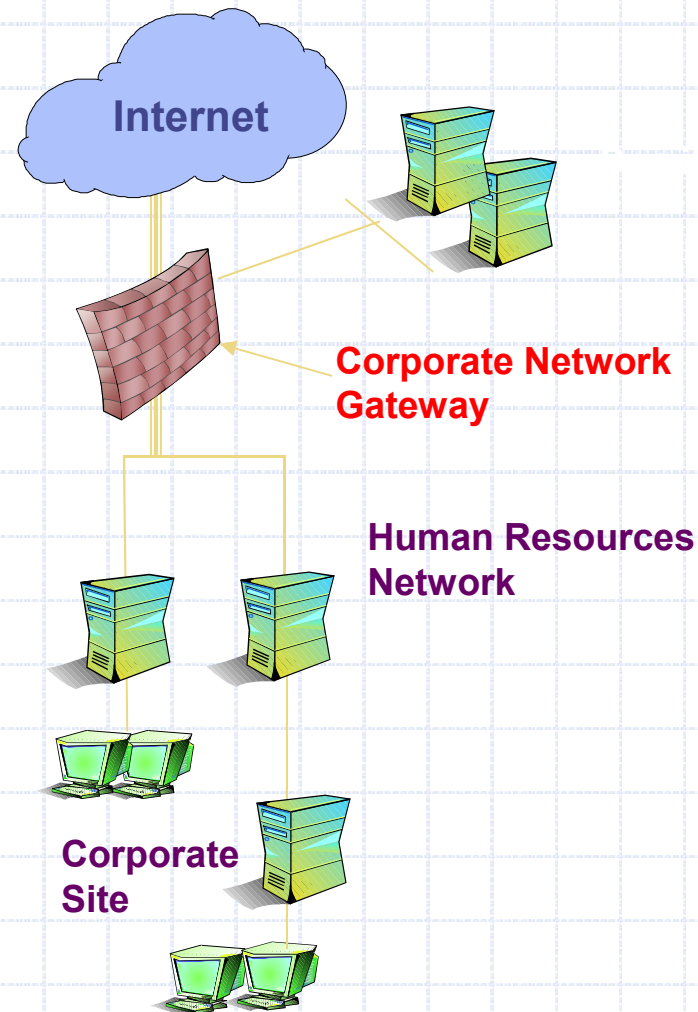
Corporate Site

Firewall Deployment

◆ Corporate Network Gateway

◆ Internal Segment Gateway

  ▪ Protect sensitive segments (Finance, HR, Product Development)

  ▪ Provide second layer of defense

  ▪ Ensure protection against internal attacks and misuse

Internet

Human Resources Network

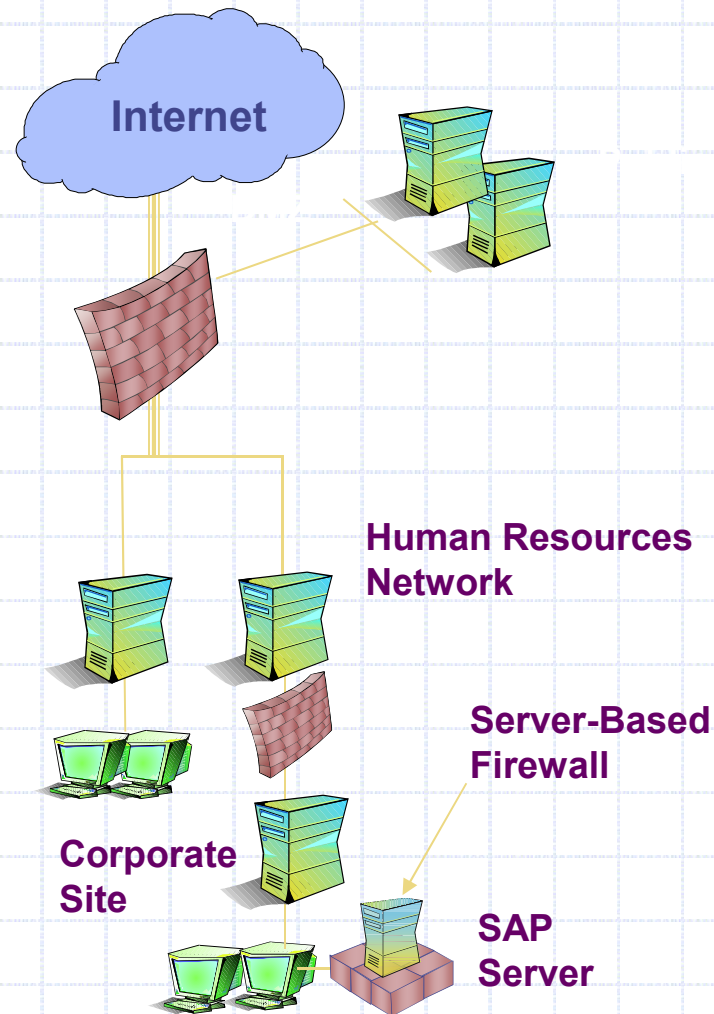Internal Segment Gateway

Corporate Site

Firewall Deployment

◆ Corporate Network Gateway

◆ Internal Segment Gateway

◆ Server-Based Firewall

  ▪ Protect individual application servers

  ▪ Files protect

Internet

Human Resources Network

Server-Based Firewall

Corporate Site

SAP Server

Firewall Deployment

◆ Hardware appliance based firewall
   - Single platform, software pre-installed
   - Can be used to support small organizations or branch offices with little IT support

◆ Software based firewall
   - Flexible platform deployment options
   - Can scale as organization grows

Summary

◆ Firewalls foundation of an enterprise security policy

◆ Stateful Inspection is the leading firewall technology