

# Information Security Education : UCF Firewall Teaching Lab

## *Summer Workshop on Distributed Computing, Networking and Security with Applications*

Instructor :      Joohan Lee  
                              jlee@cs.ucf.edu  
                              CSB 227, 823-6095  
                              <http://www.cs.ucf.edu/~jlee>

School of Computer Science  
University of Central Florida



# Introduction



## ■ Internet age

- Evolution of information systems
- Inevitable to provide an access to the Internet to/from any size of organizations
- Persistent security concerns

## ■ Firewall

- An effective means of protecting a local system or network of systems from network-based threats while at the same time affording access to the outside world via wide area networks and the Internet
  - Isolate the private network resources
  - Allow users to access the public resources
  - Log accesses (logging access history)

# Designing Goal of a Firewall

- All traffic must pass through the firewall
  - Inside to outside and vice versa
- Only authorized traffic will be allowed to pass
  - Defined by local security policy
- Firewall itself is immune to penetration
  - Use of a trusted system, a secure operating system



# Four General Techniques to Control Access and Enforce the Security Policy

- **Service Control**
  - Type of services: IP address, TCP port number, Proxy
- **Direction Control**
  - Direction of the service
- **User Control**
  - Who can access what types of service
- **Behavior Control**
  - Controls how particular services are used



# What is a Firewall?

- A single **choke point** of control and monitoring
- Interconnects networks with differing trust
- Imposes restrictions on network services
  - Only authorized traffic is allowed
- Auditing and controlling access
  - Can implement alarms for abnormal behavior
- Is itself immune to penetration
- Provides **perimeter defence**



# Firewall Limitations

- Cannot protect from attacks bypassing it
  - [eg] sneaker net, utility modems, trusted organizations, trusted services (eg SSL/SSH)
  - What if the web server behind the firewall is vulnerable?
- Cannot protect against internal threats
  - [eg] disgruntled employee
- Cannot protect against transfer of all virus infected programs or files
  - Because of huge range of O/S and file types

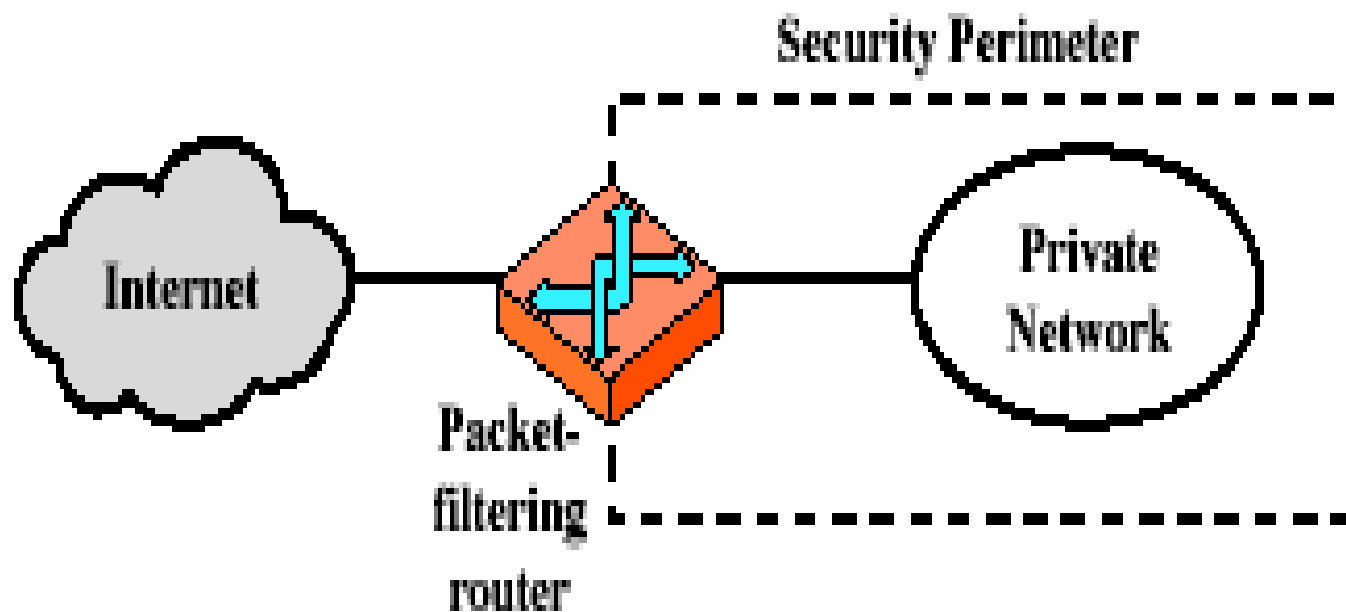


# Types of Firewalls

- Packet-Filtering Router
- Application-Level Gateway
- Circuit-Level Gateway



# Firewalls – Packet Filters



(a) Packet-filtering router

# Firewalls – Packet Filters

- Simplest of components
- Foundation of any firewall system
- Examine each IP packet (no context) and permit or deny according to rules
- Hence restrict access to services (ports)
- Possible default policies
  - That not expressly permitted is prohibited
    - Cyberguard firewall takes this default policy
  - That not expressly prohibited is permitted



# Firewalls – Packet Filters

Table 20.1 Packet-Filtering Examples

**A**

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

**B**

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

**C**

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

**D**

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

**E**

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers



# Attacks on Packet Filters

- IP address spoofing
  - Fake source address to be trusted
- Source routing attacks
  - attacker sets a route other than default
- Tiny fragment attacks
  - Split header info over several tiny packets
    - checks the first packet and lets the remaining packets pass through

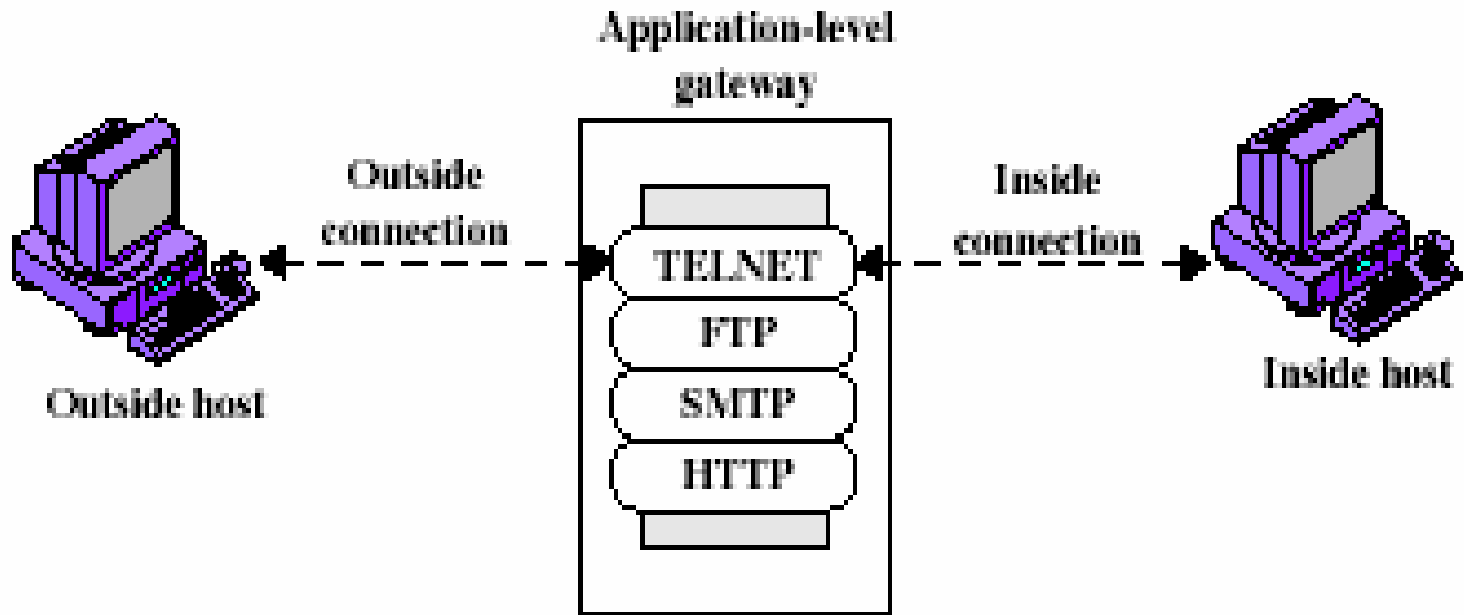


# Firewalls – Stateful Packet Filters

- Examine each IP packet in context
  - Keeps tracks of client-server sessions
  - Checks each packet validly belongs to one



# Firewalls - Application Level Gateway (or Proxy)



(b) Application-level gateway

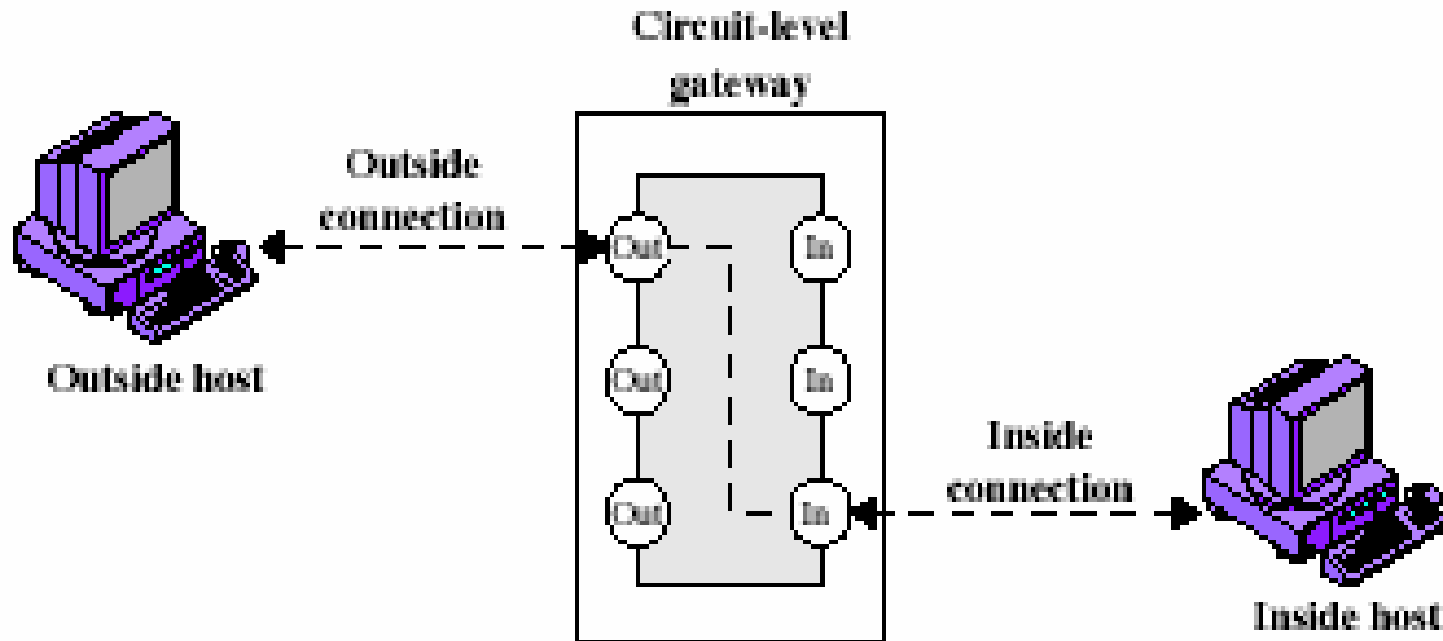


# Firewalls - Application Level Gateway (or Proxy)

- Use an application specific gateway / proxy
- Has full access to protocol
  - User requests service from proxy
  - Proxy validates request as legal
  - Then actions request and returns result to user
- Need separate proxies for each service
- Advantages
  - Tend to be more secure than packet filters
  - Easy to log and audit all incoming traffic at the application level
- Disadvantages
  - Additional processing overhead on each connection



# Firewalls - Circuit Level Gateway



(c) Circuit-level gateway

# Firewalls - Circuit Level Gateway

- Relays two TCP connections
- Imposes security by limiting which such connections are allowed
- Once created usually relays traffic without examining contents
- Typically used when trust internal users by allowing general outbound connections
  - Overhead of examining incoming application data for forbidden functions but does not incur overhead on outgoing data

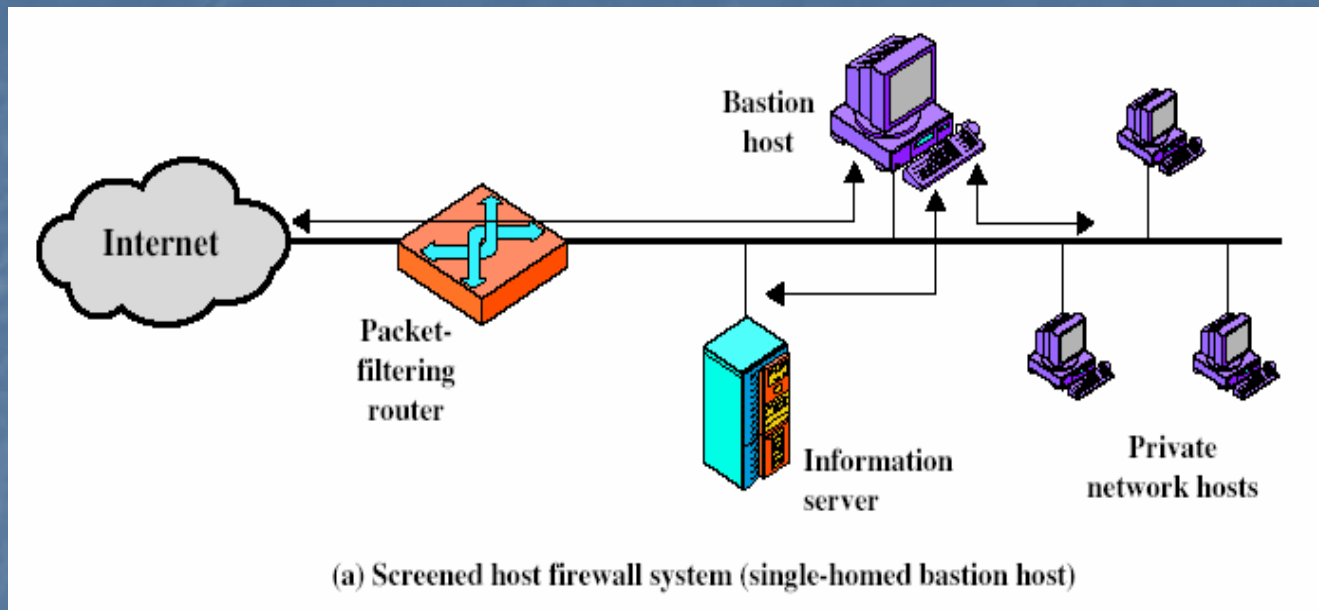


# Bastion Host

- A system identified by the firewall administrator as a critical strong point in the network's security
- Characteristics
  - Runs secure operating systems
  - Potentially exposed to "hostile" elements
  - Only the essential services are installed
    - DNS, FTP, SMTP, and user authentication
  - May support 2 or more net connections
  - May be trusted to enforce trusted separation between network connections
  - Runs circuit / application level gateways



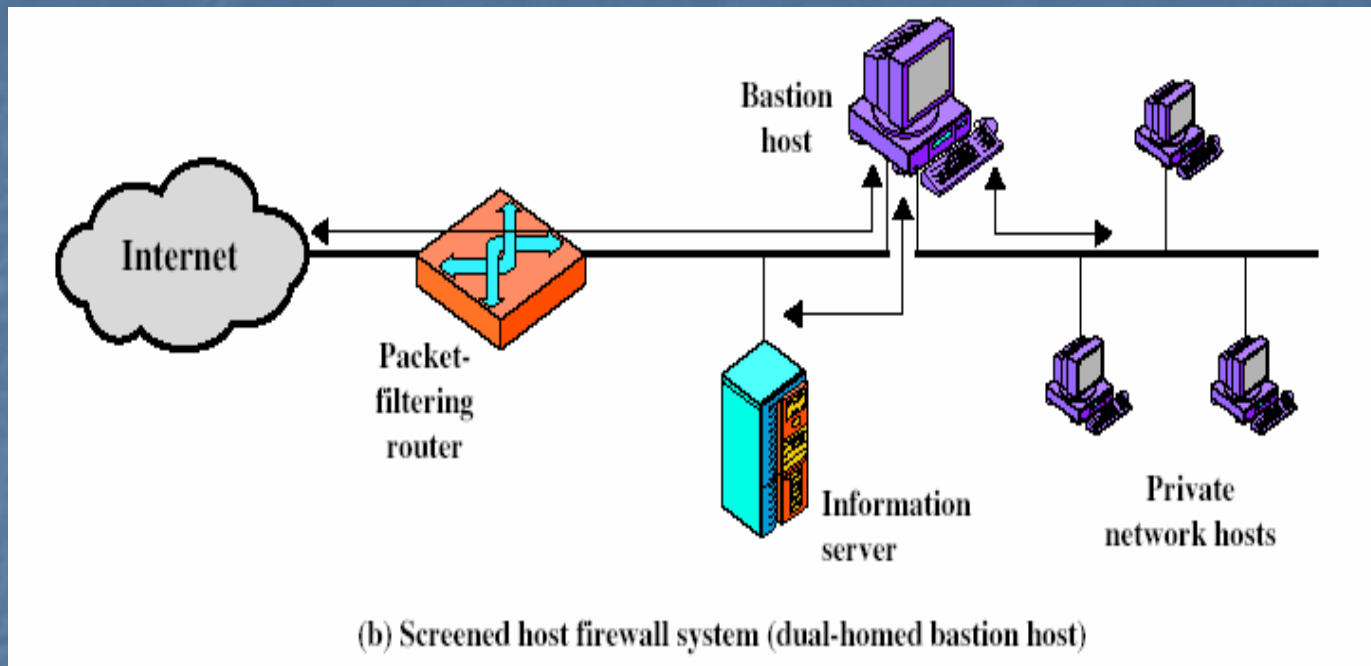
# Firewall Configurations



- For traffic from the external network, only IP packets destined for the bastion host are allowed in
- For traffic from the internal network, only IP packets from the bastion host are allowed out
- Bastion hosts performs
  - authentication, and proxy functions
- Both packet-level and application level filtering → better security

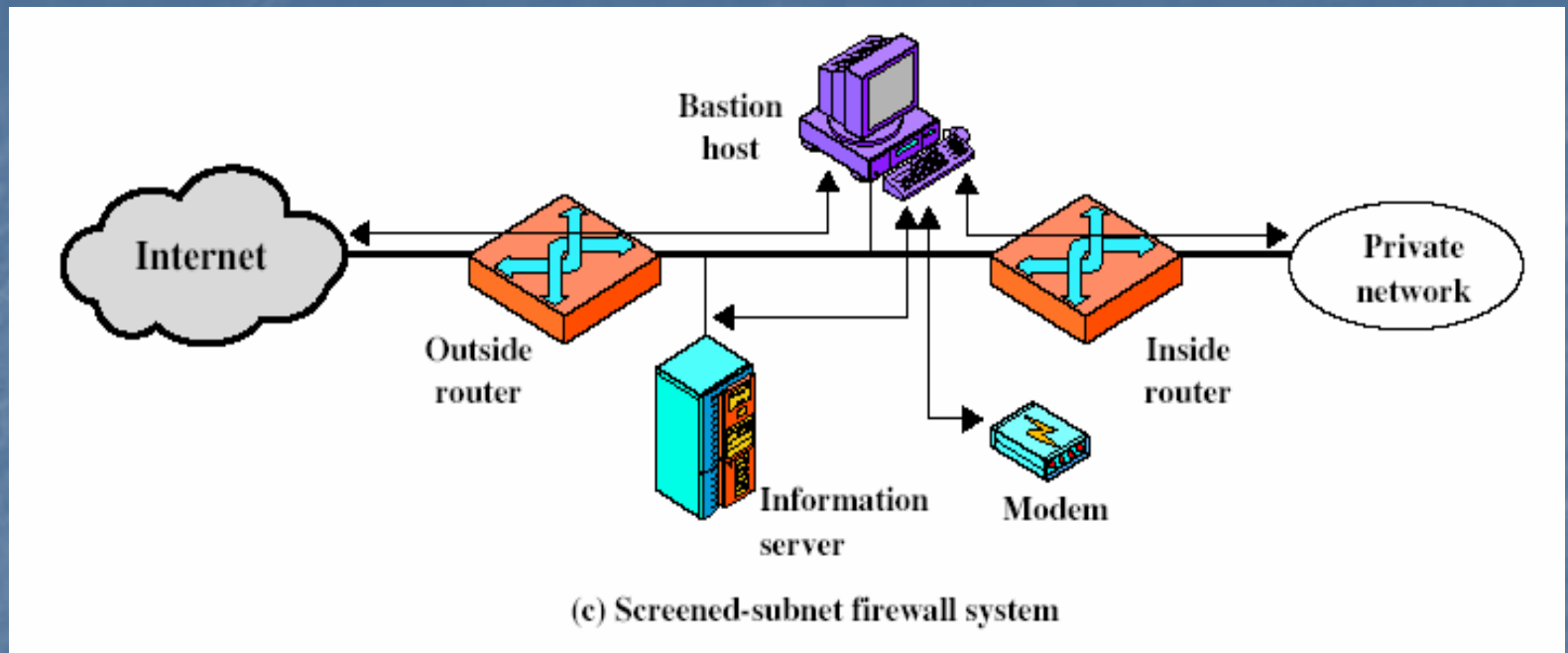


# Firewall Configurations



- Security breach in (a) → once the firewall is compromised traffic can directly flow into the private network
- Physically prevents such a security breach

# Firewall Configurations



- The most secure configuration
- Two firewalls (packet filtering routers) are used
- Three levels of defense
- Inside private networks invisible to and isolated from the Internet

# UCF Firewall Teaching Lab



# Lab Objective

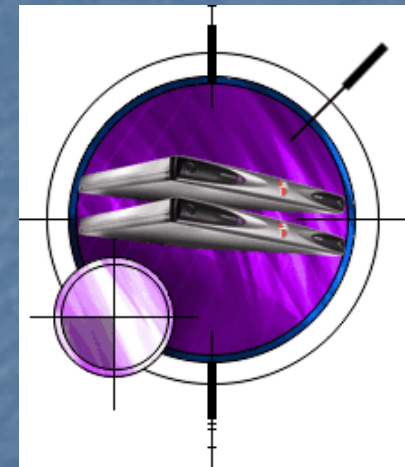
- Students should be able to do:
  - Install the firewalls and set up the network
  - Set up the IP addresses
  - Translate the security policy into a set of packet filtering rules
  - Add a symbolic host and network
  - Check system statistics using reports
  - Configure dynamic gateway and static routes
  - Add a packet filtering rule with options
  - Configure a default gateway and static routes
  - Add and configure a SmartProxy
  - Configure dynamic and static Network Address Translation (NAT)



# Development of Firewall Lab



- In collaboration with the Cyberguard
  - Set up the teaching lab for the undergraduate security education
  - Participated in Firewall Security Administration course offered by Cyberguard
  - Developed the teaching materials to help the students understand the concept of Firewalls
  - Have the hands on experience on setting up the networks and configuring the firewalls to implement the various security policies
  - Provide an simulated wide area networking environment



# Basic Configuration



192.168.10.10

**Firewall 1**

10.0.10.1

10.0.10.110

**PC**

192.168.20.20

**Firewall 2**

10.0.20.1

10.0.20.110

**PC**

192.168.30.30

**Firewall 3**

10.0.30.1

10.0.30.110

**PC**

192.168.40.40

**Firewall 4**

10.0.40.1

10.0.40.110

**PC**



# IP addresses

- How to find out my network configuration (Red Hat Linux)
  - IP address
    - /etc/sysconfig/network-scripts/ifcfg-eth0
      - Ethernet interface configuration
    - /etc/hosts
      - hostnames info
    - /etc/sysconfig/network
      - routing info. including default gateway
  - Useful commands
    - ping
    - netstat -nr
    - traceroute
    - nslookup, dig



# Secure Operating System

- Multilevel Security
  - There is no absolute root in the OS
  - Depending on your level, you will have different privileges
  - Different levels
    - SYS\_PRIVATE
    - SYS\_PUBLIC
    - Root
    - Network
  - How to change the level
    - /sbin/tfadmin newlvl SYS\_PRIVATE
    - root
    - newlvl network
  - Unixware specific OS command options
    - ps -efz
    - ls -alx

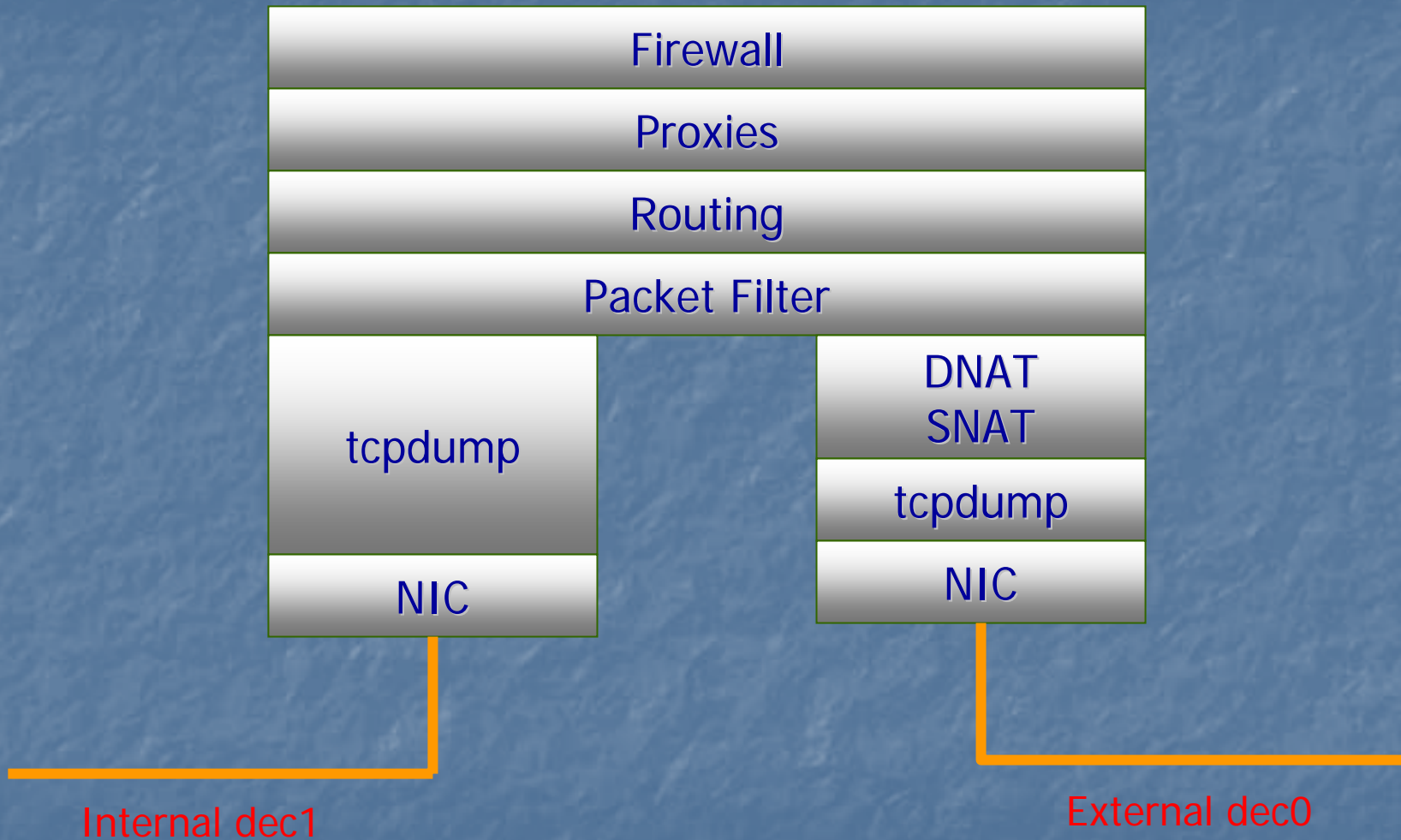


# Packet Filtering

- Order of packet filtering rules
  - Top down: Rules at the top will be applied first even though they may conflict with those at the bottom
  - Remember that the default rule is **"Deny every packet"** at the bottom
- Inserting packet filtering rules
  - Shouldn't use **"allow all traffics from everyone to everyone"**
  - Try to use specific service names and host names or IP addresses
  - What if there are so many types of services and computers to manage?
    - use **grouping**



# Firewall Block Diagram



# Grouping

- The symbolic names allow a group of related rules to be collapsed into one rule, greatly simplifying firewall administration
- This simplification increases security by reducing human error
- Names can be assigned to IP addresses, networks, and services. Once names are assigned, these names can be used in policy statements (packet filtering rules) to make the policy more meaningful to a human reader

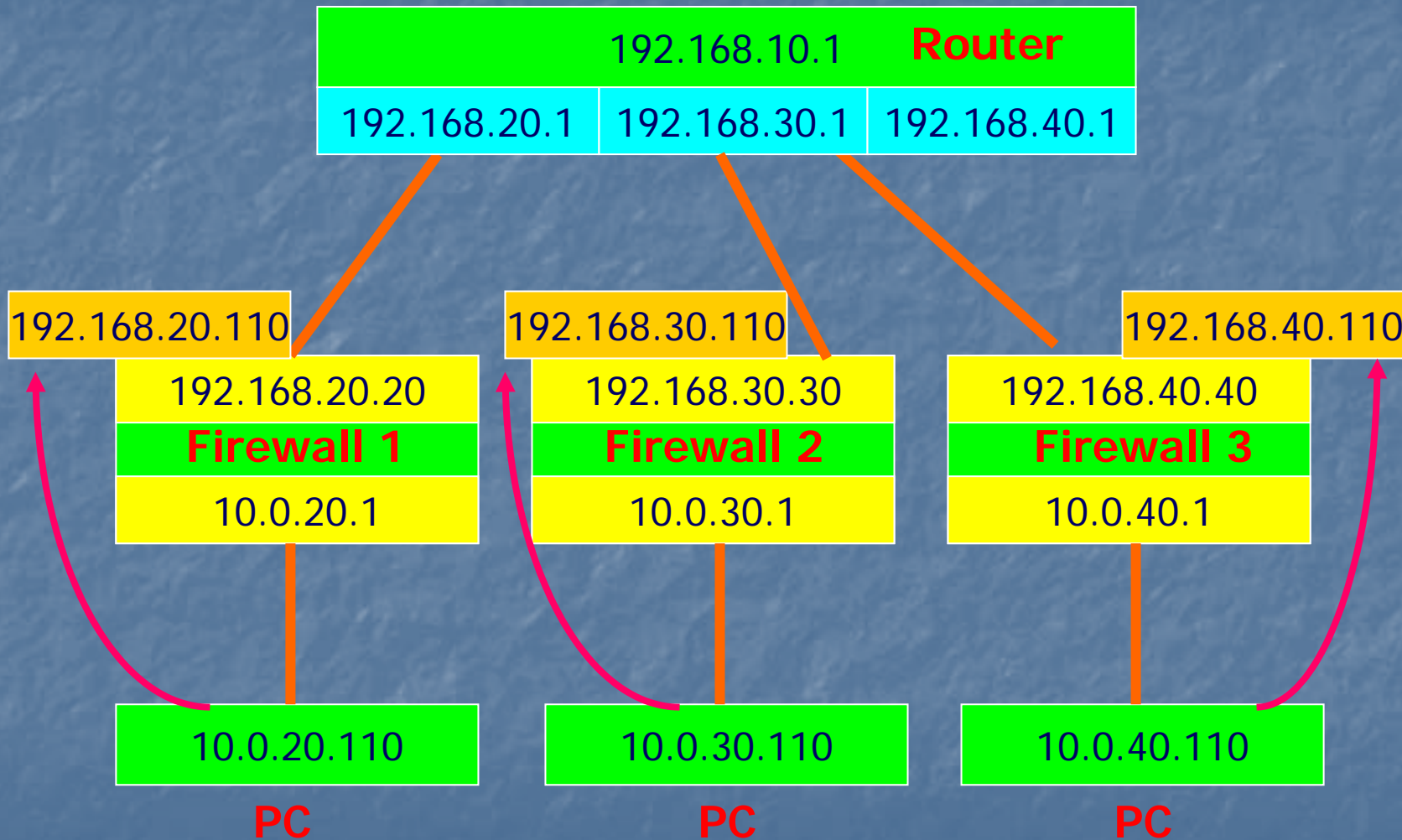


# Network Address Translation

- Without NAT, each inside computer would be assigned a real IP address and every message passing out through the firewall would retain its real source IP address in the header fields
- **Problem**
  - Anyone tapping the communications channel can discover the real IP addresses of the client computers and use this information to probe your internal network looking for weakness
- **Solution**
  - **Static NAT** : Use the firewall as the active interface to limit IP address visibility. One IP address on the inside is mapped to one unique external IP address that is different from the firewall's IP address
  - **Dynamic NAT**: All internal hosts appear on the outside network as originating from a single IP address. The firewall acts as the man in the middle and translates all traffic from one IP address to another



# Dynamic/Static NAT



# Network Address Translation

- What property of TCP/UDP communication allows NAT to work?
  - The concepts of ports. Ports can be tracked and manipulated by the firewall to convert one established host IP address to a different IP address with a new port number. Only the firewall has the key to the port to port mapping that it uses



# Users and Proxy (Application Level Firewall)

- In this lab, we create a new user and setup the appropriate FTP proxy for this user
- We can also setup Web proxy for a particular user
- Remember that proxy is per service based
- That's why Proxy is also called an application level firewall



# Alerts, Activities, and Archives

- The tools available to monitor, audit, and send alerts based on network activity
- Monitoring activity is important so that you can detect and respond to threats and critical conditions
- You can configure the firewall to recognize suspicious and critical events and customize your response to these events
- By default, the system generates binary logs and saves them in the `/var/audit/directory`
- If configured, the `auditlogd` process will produce the ASCII logs from the binary and save them in the `/var/audit_logs` directory



# Alerts, Activities, and Archives

