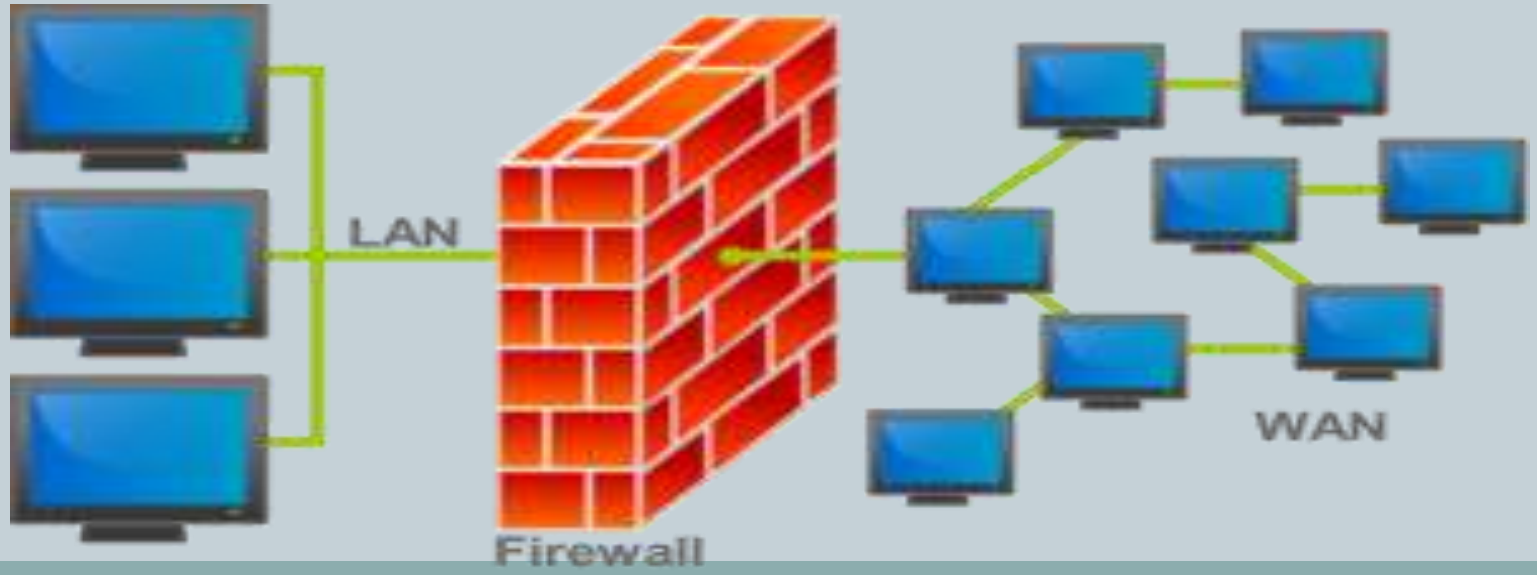
Presentation :’Firewalls’

PRESENTERS :-
GAGANDEEP SINGH
KARANDEEP VOHRA
PUNEETPAL SINGH

Table of Contents

Introduction

- Is hardware, software, or a combination of both
- used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer.

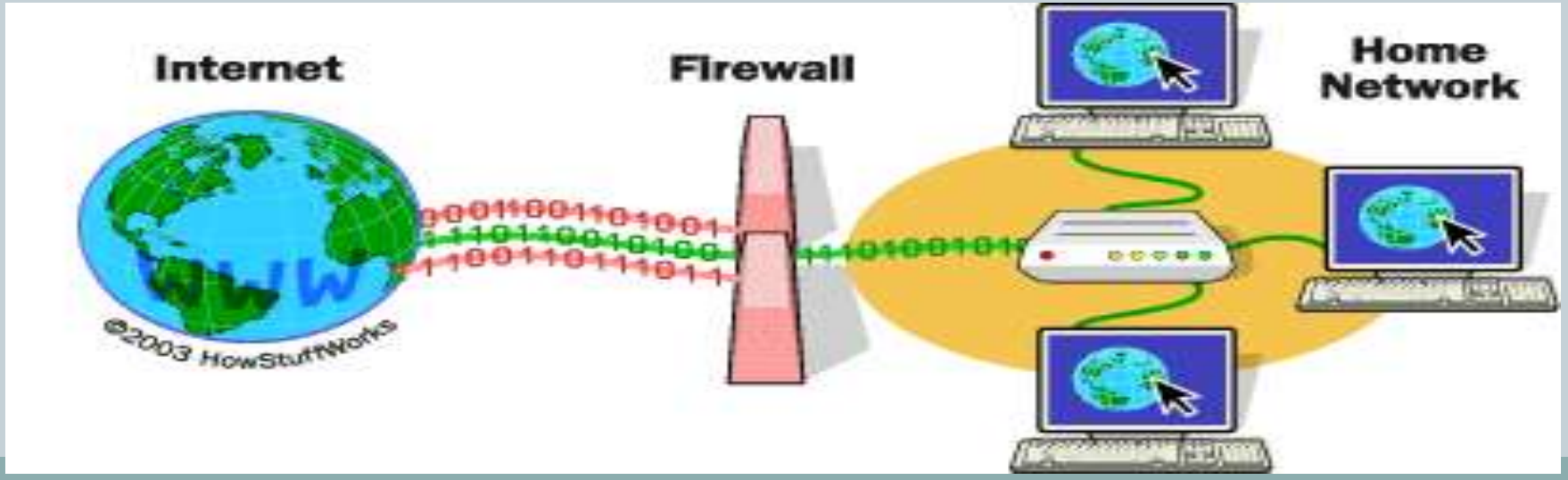


Hardware vs. Software Firewalls

- Hardware Firewalls
  - Protect an entire network
  - Implemented on the router level
  - Usually more expensive, harder to configure
- Software Firewalls
  - Protect a single computer
  - Usually less expensive, easier to configure

How does a software firewall work?

- Inspects each individual “packet” of data as it arrives at either side of the firewall
- Determines whether it should be allowed to pass through or if it should be blocked



Firewall Rules

- Allow – traffic that flows automatically because it has been deemed
- Block – traffic that is blocked because it has been deemed dangerous to your computer
- Ask – asks the user whether or not the traffic is allowed to pass through

What Can a Firewall Do?

- Focus for security decisions
  - Stop hackers from accessing your computer
- Can enforce security policy
  - Protects your personal information
- Limits your exposure
  - Blocks “pop up” ads and certain cookies
- Can log Internet activity efficiently
  - Determines which programs can access the Internet

What Can't a Firewall Do?

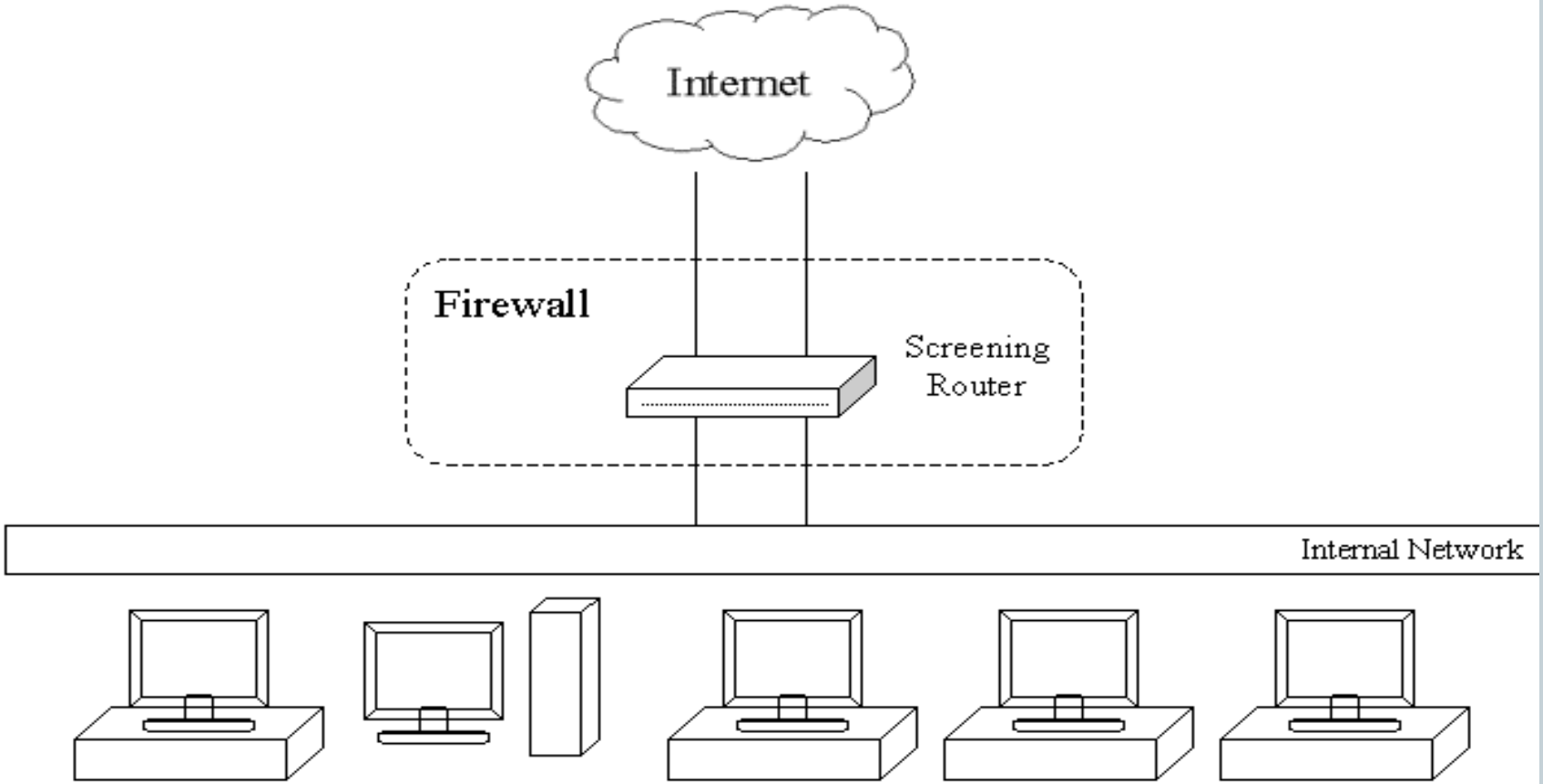
- Can't protect you against malicious insiders
- Can't protect you against connections that don't go through it
- Can't protect against completely new threats
- Can't protect against viruses

Types of Firewalls

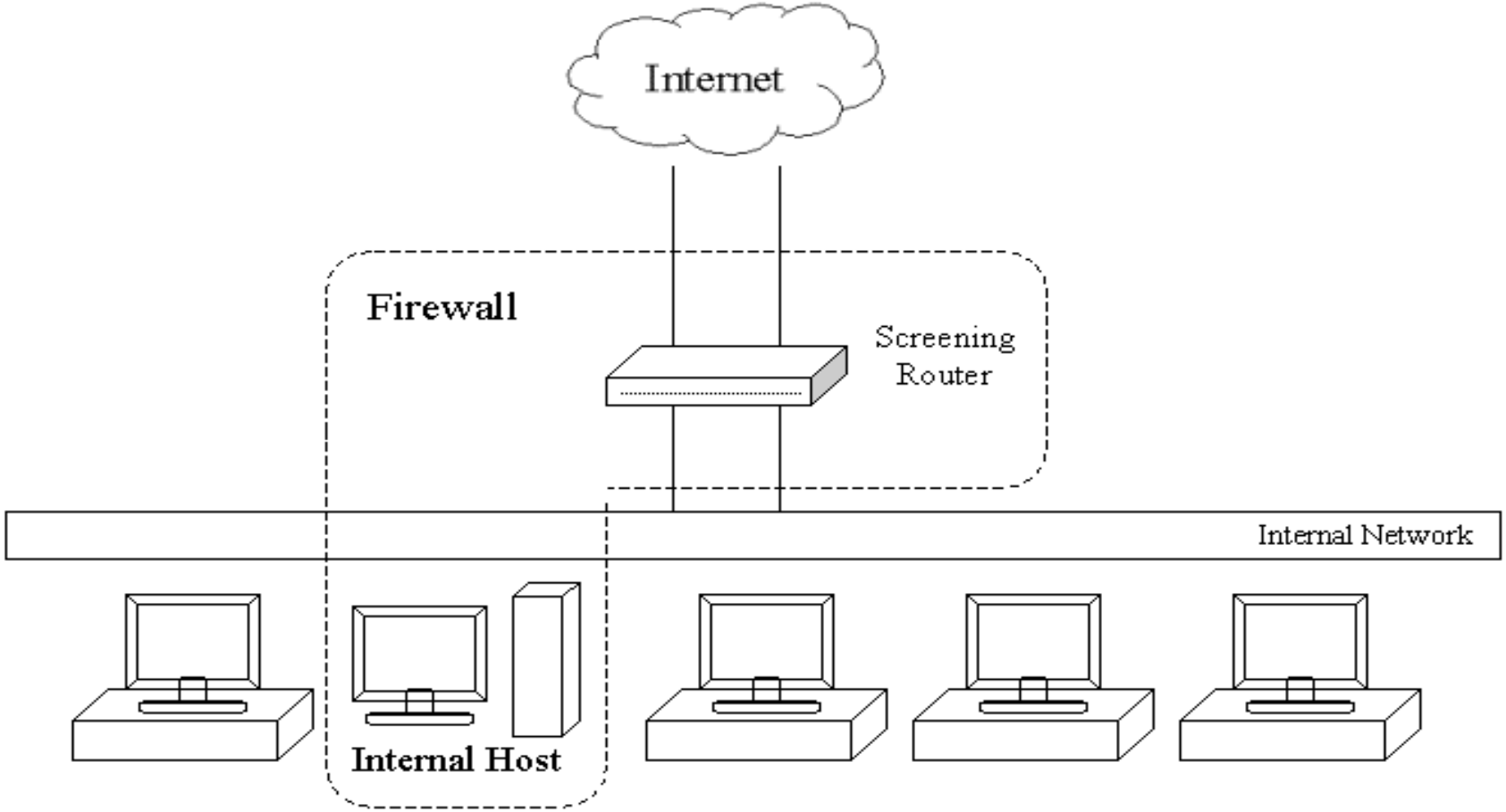
- Packet Filtering Firewall
- Application level Gateway
- Circuit level gateway

Architectures for Firewall

- Single-Box Architecture



Screened Host Architecture



Making The Firewall Fit

- IP address
- Domain names
- Protocols
- Ports

What It Protects You From

- Remote login
- SMTP session hijacking
- Operating system bugs
- Spam
- E-mail bombs
- Source routing

Security Strategies implemented

- Default Deny
  - Prohibit all communication that is not expressly permitted
- Default Permit
  - Permit all communication that is not explicitly prohibited
- Least Privilege
  - reduces the authorization level at which various actions are performed
- Defense in Depth
  - security approach whereby each system on the network is secured to the greatest possible degree
- Choke Point
  - forces attackers to use a narrow channel to bypass the network

Testing a Firewall Configuration

- A faster and easier method is available with the Linux firewall
- implementation
- Allows you to manually generate tests
- Suppose our local network is 172.16.1.0
- And we allow only TCP connections

Example

- **# ipchains -C forward -p tcp -s 172.16.1.0 1025 -d 44.136.8.2 80 -i eth0 accepted**

  source Destination

- # **ipchains -C forward -p tcp -s 172.16.2.0 1025 -d 44.136.8.2 80 -i eth0** denied

  Wrong

- **# ipchains -C forward -p udp -s 172.16.1.0 1025 -d 44.136.8.2 80 -i eth0 denied**

  Wrong

- **# ipchains -C forward -p tcp -s 172.16.1.0 1025 -d 44.136.8.2 23 -i eth0 denied**

  Wrong

REFRENCES

- www.howstuffworks.com
- www.securityfocus.com
- www.firewall.com

Conclusion

TESTING A FIREWALL CONFIGURATION

THANKU