Firewall Simulation

COMP620

Firewall Simulation

- The simulation allows participants to configure their own simulated firewalls using Cisco-like syntax.
- Participants can take benign or malicious actions against other players to score points.
- The interactive and competitive nature of the simulation helps students learn about firewalls while having fun.

Enter FireSim configuration

Instructions Network Configuration Diagram

```
access-list 111 permit tcp any host 152.8.1.1 eq 443
access-list 112 permit tcp any host 152.8.1.1 eq 80
```

Check Configuration

Select	Name	Score
●	Fred	99
	Mary	101

Take Action	View the home page of their website
Take Action	Retrieve an IP address from their Domain Name Server
Take Action	Send regular email.
Take Action	Copy a file from their FTP server
Take Action	Access email via POP from the Internet.
Take Action	Access email via IMAP4 from the Internet.
Take Action	Employees access www.wasteoftime.com.
Take Action	VPN access to the network
Take Action	Petya ransomware access to system

You were denied access to Fred's Domain Name Server. +1 point
You successfully accessed Fred's web server. No change in score.
Firewall Configuration Updated
You must select a player to act upon
Start
Firewall Configuration Updated
Messages both internal and external
will appear here

Simulation Process

- When you first start, you must enter your name and the Group Identifier given by your instructor
- Configure your firewall to allow needed services while preventing attacks
- When the instructor starts the simulation, you can take actions against other players
- Reconfigure your firewall whenever necessary to correct problems
- New tasks will appear that may require you to reconfigure your firewall

Help Needed

- I need some assistance in configuring the Apache web server

Computers Needed in Class

- I hope to run a firewall simulation event in class on Friday
- We can do the simulation here or in a computer lab

Can you bring a laptop to class on Friday?

A. Yes

B. No

Configuration Syntax

access-list number {**permit** | **deny**}
[protocol]
{**any** | ipaddr mask | **host** ipaddr}
{**any** | ipaddr mask | **host** ipaddr}
[operator port | **established**] [**log**]

- The entire access-list command must be written on one line.

Address Formats

- You can specify a source or destination IP address in three different formats:
- **any** – all addresses match
- **host** *12.34.56.78* – This address matches one specific computer with the given address
- *IPaddress mask* – This address is compared to the given IP address ignoring the bits that are one in the mask.

Example

- This permits any computer on the Internet to connect to the computer whose IP address is 152.8.1.1 using the TCP protocol and port 443.

```
access-list 111 permit tcp any host 152.8.1.1 eq 443
```

Example

- This prevents any UDP traffic from reaching computers in 152.8.100.X subdomain

```
access-list 112 deny udp any
            152.8.100.0  0.0.0.255
```

- Note: access-list statements must be written on one line.

Order is Important

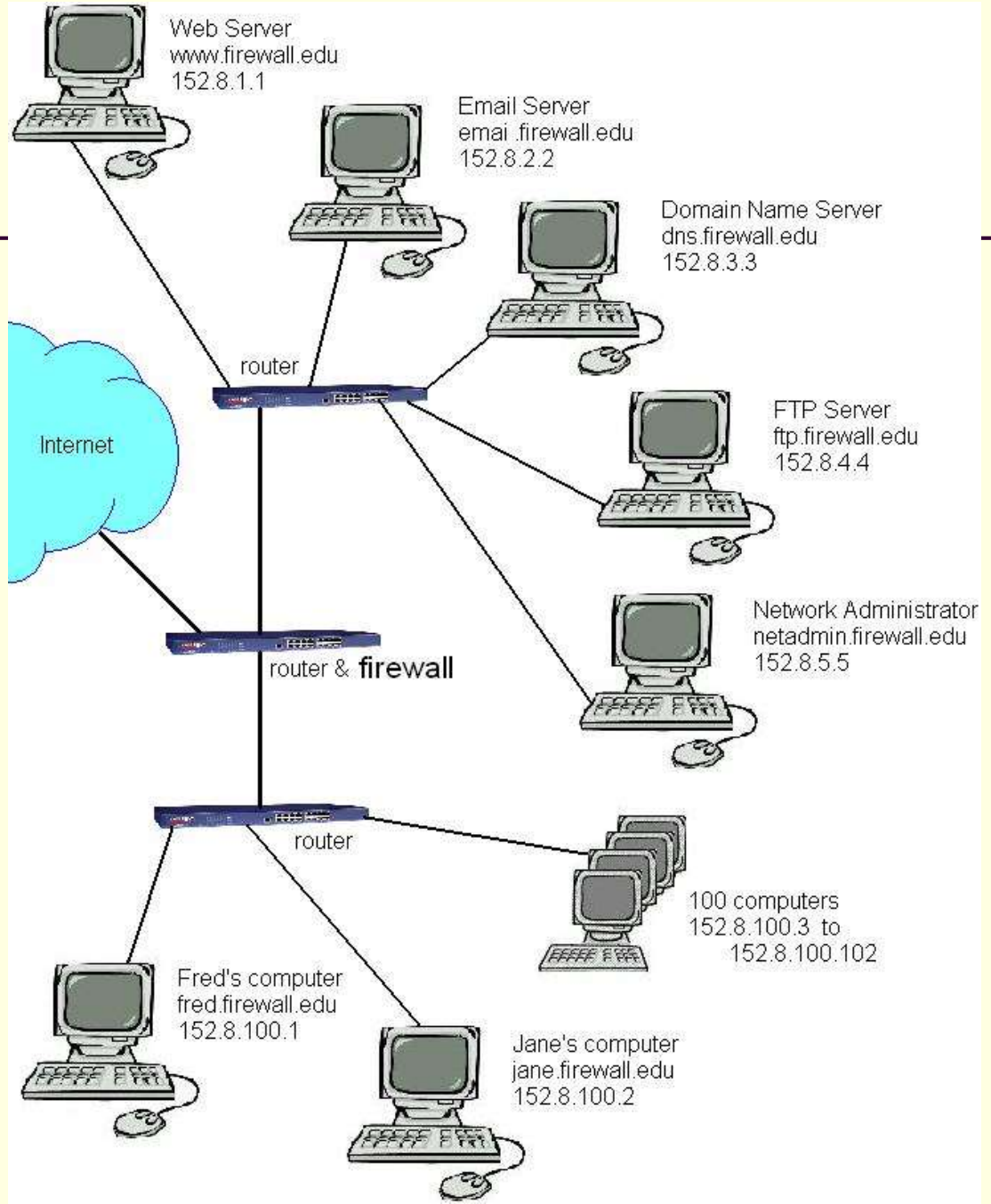
- When a packet arrives at your firewall, it will be compared with each access-list statement in the order they appear
- The number after "access-list" is required but ignored
- The first statement that applies to that packet determines if it is permitted or denied
- For incoming traffic, there is an implicit deny everything at the end of the access-lists
- For outgoing traffic, there is an implicit permit everything at the end of the access-lists

Firewall Configuration

- The firewall configuration window should contain all of your **`access-list`** commands
- You can edit your firewall configuration at any time. Click on "Check Configuration" to update your firewall
- If errors are detected in the configuration, no change is made to your configuration

Your Simulated Network

- There is a link on the webpage to a diagram of the simulated network showing the computers and their IP addresses.
- Your domain has the Internet address of 152.8.0.0/16


Web Server
www.firewall.edu
152.8.1.1
Email Server
emai .firewall.edu
152.8.2.2
Domain Name Server
dns.firewall.edu
152.8.3.3
router
Internet
FTP Server
ftp.firewall.edu
152.8.4.4
Network Administrator
netadmin.firewall.edu
152.8.5.5
router & firewall
router
100 computers
152.8.100.3 to
152.8.100.102
Fred's computer
fred.firewall.edu
152.8.100.1
Jane's computer
jane.firewall.edu
152.8.100.2

Coming and Going

- The access-list commands specify source and destination addresses.
- If the source address starts with 152.8, then the traffic is going out from your network to the Internet.
- If the source is any other address, then the traffic is coming into your network.

Timing

- Your instructor can add firewall requirements at any time
- 45 seconds after a new firewall requirement, you can attack another player (or be attacked)
- After successfully attacking another player, you cannot perform the same attack on that player for another 45 seconds.

Needed Services

- Access by the public to your web site
- Email from other email servers using SMTP
- Domain Name Server access

Useful Port Numbers

21	FTP
23	Telnet
25	Simple Mail Transport Protocol
53	Domain Name Servers
80	HTTP
110	POP3 client email
123	Network Time Protocol
137-139	Microsoft NETBIOS
143	IMAP4 client email
161	Simple Network Maintenance Protocol
443	HTTPS
445	Windows File Sharing
1863	MSN Instant messaging
3389	Windows Remote Desktop Protocol
5190	AOL instant messenger