



# Lab 8: Firewall

*ITCS461: Computer and Communication Security*

Mahidol University



## Table of Contents

1 Without Firewall

2 With Firewall

3 With 2 Firewalls



## Part I

### Without Firewall



## Without Firewall Overview

The **Firewall Visualization Tool**<sup>1</sup> is used to help demonstrate the effects of various firewall rules and configurations on innocent and malicious traffic.

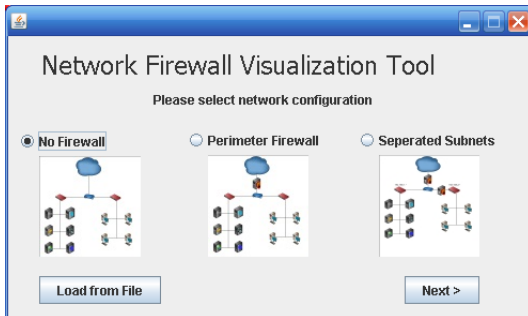
---

<sup>1</sup> Parks Masters, David Musielewicz, Taylor Verett, Justin Warner, and Robert Winchester, "Firewall Visualization Tool Version: 1.0", Computer Security Instructor Manual (by W. Stallings and L. Brown), Pearson, 2012

## Without Firewall

### Network Overview

1. Start the firewall visualization program by double click on “Firewall Visualization Tool.jar”.  
You should see a screen similar to the one below:

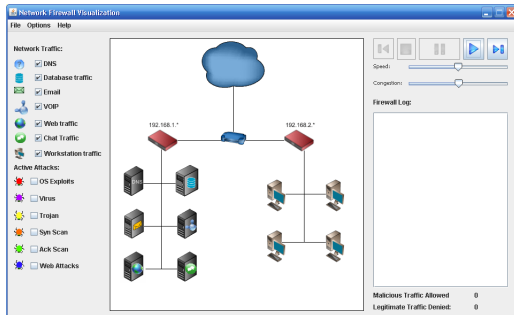



2. Choose “No Firewall” and click **next**. The following screen will be appeared.

## Without Firewall

### Network Overview

Overview of a network without firewall





- Click the  button to start the traffic simulation. Note that the traffic flows both from the “cloud” or internet to/from the client machines. By default, all types of network traffic are generated without malicious traffic flowing to the machines.



## Without Firewall

### Network Overview

- Click on the “OS Exploit” option and wait for awhile. Eventually, you’ll see a similar red colored bug  flow from the internet into the local area network and land on a machine, infecting the machine. Once a machine is infected, it is marked as such with the “international No” emblem or . We’ll see later if configuring a firewall will help prevent such infections.
- Try how to **select** or **deselect** legitimate/malicious traffic, then observe the simulation results. The 2 slide bars on the right hand side can help you **speed up/slow down** the traffic and also **increase/decrease** traffic congestion. Practice until you are sure that you can command the visualization tool, then go to PART II. There is no question for this part.



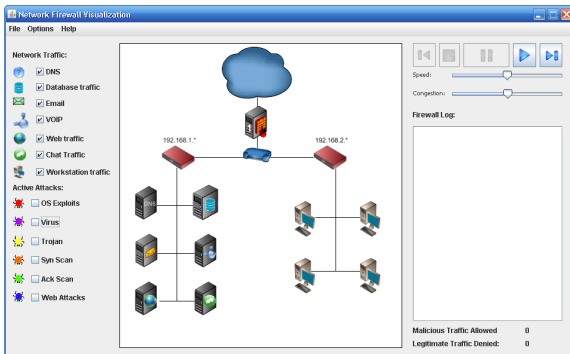
## Part II

### With Firewall



## With Firewall

1. Start a new session by clicking File -> New in the upper window of the tool.
2. This time, choose “Perimeter Firewall” (the option in the middle). The window that comes up will look like this:



You now have a firewall located between the Internet (represented by a cloud symbol) and your network router (represented by a blue box). Click the play button and watch what happens.



## With Firewall

### Question 1

#### Question 1:

- Observe the traffic flowing from the Internet into your system or from your network to the Internet. Is your network connected to the Internet? \_\_\_\_\_ (Y/N)
- Explain why or why not:

---

---

Add some **active attacks** by clicking on several different options.

- Are these attacks able to get into your network? \_\_\_\_\_ (Y/N)
- Do you feel your system is secure? \_\_\_\_\_ (Y/N)
- What's wrong with this scenario?

---

---

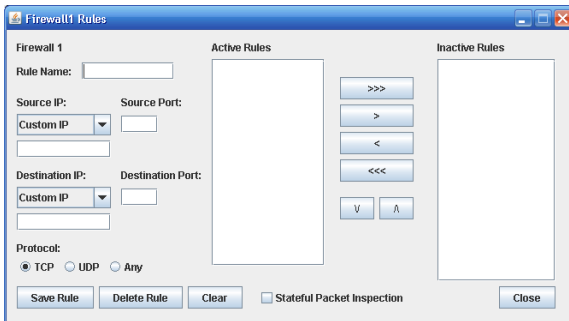
## With Firewall

### Configuring Firewall

Next, we will configure your firewall to allow traffic to flow in and out of your network.

1. Select menu “Options”
2. Choose “Define Firewall1 Rules”

You should see a screen similar to the one below:



The screenshot shows a window titled "Firewall1 Rules". On the left, under "Firewall 1", there are fields for "Rule Name:", "Source IP:" (with a dropdown menu set to "Custom IP"), "Source Port:", "Destination IP:" (also with a "Custom IP" dropdown), "Destination Port:", and "Protocol:" (with radio buttons for TCP, UDP, and Any, where TCP is selected). At the bottom left are buttons for "Save Rule", "Delete Rule", and "Clear". A checkbox for "Stateful Packet Inspection" is located at the bottom center. On the right, there are two large empty boxes labeled "Active Rules" and "Inactive Rules". Between these boxes are five buttons: ">>>", ">", "<", "<<<", and two buttons with up and down arrow symbols. A "Close" button is at the bottom right.

**Note:** Firewall rules defined in this tool applies “drop policy”, such that it denies traffic by default, unless a rule specifies which traffic is allowed.



## With Firewall

### Configuring Firewall (Cont'd)

Assuming the traffics that we want to use in our network are :


Type	Machine's IP Address	Port	Protocol
DNS	192.168.1.5	53	UDP
Database	192.168.1.233	3306	TCP
Email	192.168.1.136	25	TCP
VOIP	192.168.1.74	38287	TCP
Web	192.168.1.114	80	TCP
Chat	192.168.1.68	5222	TCP
Workstation Traffic	Simply turns on traffic which will originate from the workstations.		



## With Firewall

### Setting Firewall Rules for DNS

Example: To define a rule to allow only DNS traffic to go out.

1. In Firewall1 Rule setup window, try setting the following firewall rule:
  - Rule Name: **DNS out**
  - Source IP: **DNS** (IP and Port will be automatically filled)
  - Source Port: **53**
  - Destination IP: **Any** (IP : \*.\*.\* and Port: \* will be automatically filled)
  - Protocol: **Any**
2. Click **"Save Rule"**.
3. You should now see the rule **DNS out** in your **Active Rules** box.
4. Click **"close"** and you should be back to your Network Firewall Visualization Tool window.
5. Click the play button  and watch what happens. You may need to move the speed bar to the right for increasing the traffic speed.
6. Observe how traffic now flows through the firewall. If the traffic does not flow as expected, correct the rule and try again.
7. Add some active attacks and watch if they flow through the firewall.

*Note: For convenient observing, remove all traffic except **DNS** and **Workstation** traffic.*



## With Firewall

### Setting Firewall Rules for Email

**Question 2:** What is firewall rule which allows only **Email** traffic to go out ?

- Source IP : \_\_\_\_\_ Port : \_\_\_\_\_
- Destination IP : \_\_\_\_\_ Port : \_\_\_\_\_
- Protocol : \_\_\_\_\_

(Create firewall rule named, “**Email out**”, similar to DNS out, try until you get success, copy IP, Port and Protocol from Firewall1 Rule window to your answer.)

**Question 3:** What is firewall rule which allows only **Email** traffic to come in ?

- Source IP : \_\_\_\_\_ Port : \_\_\_\_\_
- Destination IP : \_\_\_\_\_ Port : \_\_\_\_\_
- Protocol : \_\_\_\_\_

(Move “**Email out**” rule to **Inactive Rules** box. Then create new firewall rule named, “**Email in**”, similar to Email out, but define source IP as any and destination IP as Email, try until you get success, copy IP, Port and Protocol from Firewall1 Rule window to your answer.)



## With Firewall

### Question 4

**Question 4:** What is a set of firewall rules which allows only **Email** traffic to come in and go out ?

The 1st Rule :

- Source IP : \_\_\_\_\_ Port : \_\_\_\_\_
- Destination IP : \_\_\_\_\_ Port : \_\_\_\_\_
- Protocol : \_\_\_\_\_

The 2nd Rule :

- Source IP : \_\_\_\_\_ Port : \_\_\_\_\_
- Destination IP : \_\_\_\_\_ Port : \_\_\_\_\_
- Protocol : \_\_\_\_\_

(Combine, “**Email in**” and “**Email out**” rules into **Active Rules** box, try to play until you get success, copy IP, Port and Protocol from Firewall1 Rule window to your answer.)



## With Firewall Questions

### Question 5:

- Change a sequence of Email in and Email out rules. After the change, does the traffic still flow? \_\_\_\_\_ (Y/N)
- Why?

---

### Question 6:

- What is a rule which allows all inbound traffics?
- What is a rule which allows all outbound traffics?
- What is a rule which blocks all traffics?

---

---

---





## With Firewall

Setting Web, DB and VOIP

Create a minimum set of rules which allows **Web** to come in, **DB** traffic to go out, and **VOIP** to come in and out.

**Question 7:** How many rules do we need? Write down all of them.

Source IP	Port	Destination IP	Port	Protocol
-----------	------	----------------	------	----------

---

---



## Part III

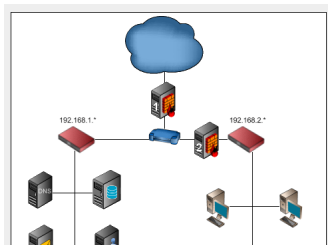
### With 2 Firewalls

## With 2 Firewalls

Setting Web, DB and VOIP

In some situation, we need to have separate network zones for our machines that we will apply different policy to them. In this case, we will setup 2 firewalls so that we can apply different sets of traffic rules.

1. Go to menu **File -> New**
2. Select Separated Subnets (the last option to select firewall)



Now you would have see that there are 2 firewalls - one placed between the Internet and the main router, another one placed in between the router and network 192.168.2.\* .



## With 2 Firewalls

### Question 8

**Question 8:** What is a set of firewall rules such that **Firewall 1** allows only DNS, Chat and Email to come in and out, **Firewall 2** allows only Chat and Email to come in and out.

	Source IP	Port	Destination IP	Port	Protocol
Firewall 1	<hr/>				
	<hr/>				
Firewall 2	<hr/>				
	<hr/>				