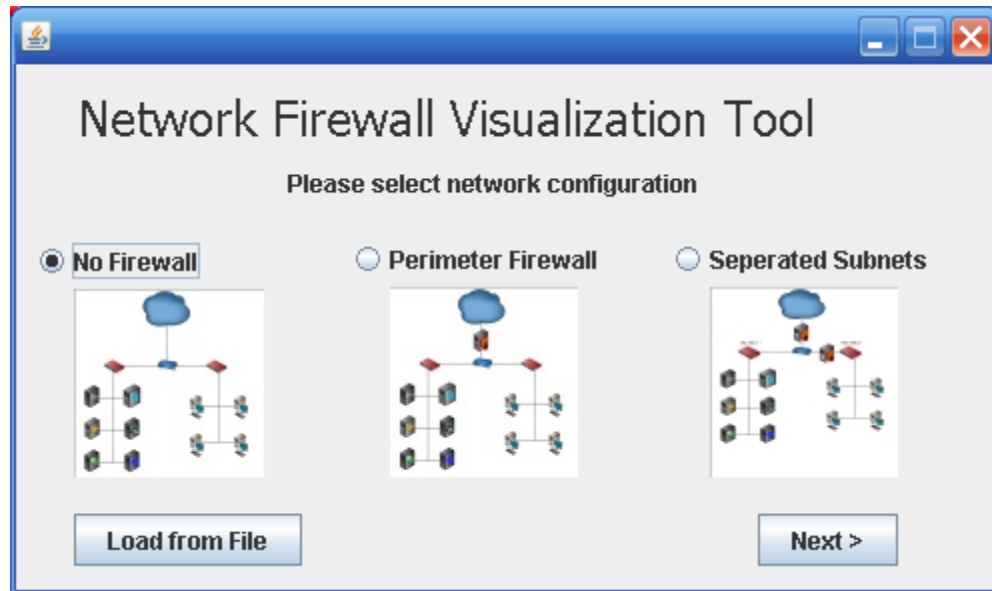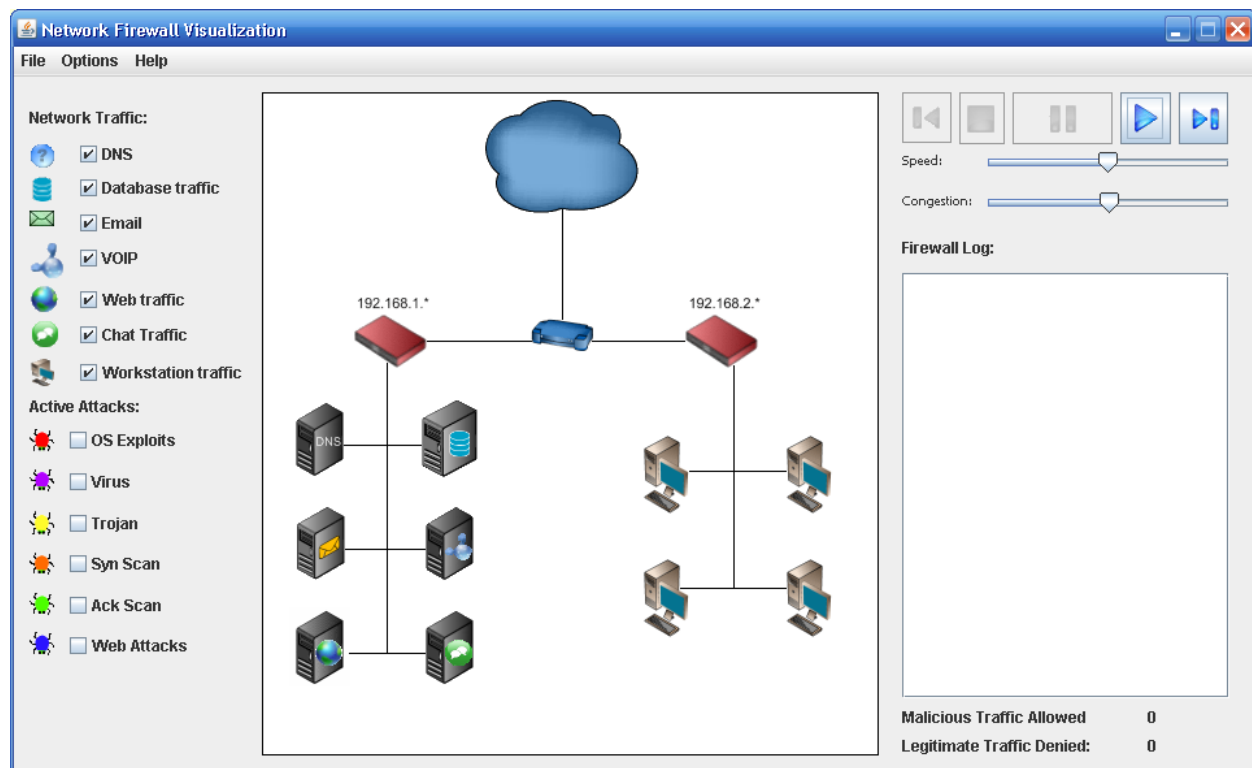# Firewall Exercise

BACKGROUND:

1. Start the Firewall program from the Tools menu of the class web site. You should see a screen similar to the one below:


Choose "no firewall" and click next. The following screen will appear:

Click the ▶ button. Note that the traffic flows both from the "cloud" or internet to the client machines. By default, there is no malicious traffic flowing to the machines. Click on the *OS Exploit* option. 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 ⊘. Let's see how configuring a firewall will help prevent such infections.

FIREWALL Configuration.

1. Start a new session by clicking File -> New in the upper window of the tool. This time, choose the Parameter firewall. The window that comes up will look like this:
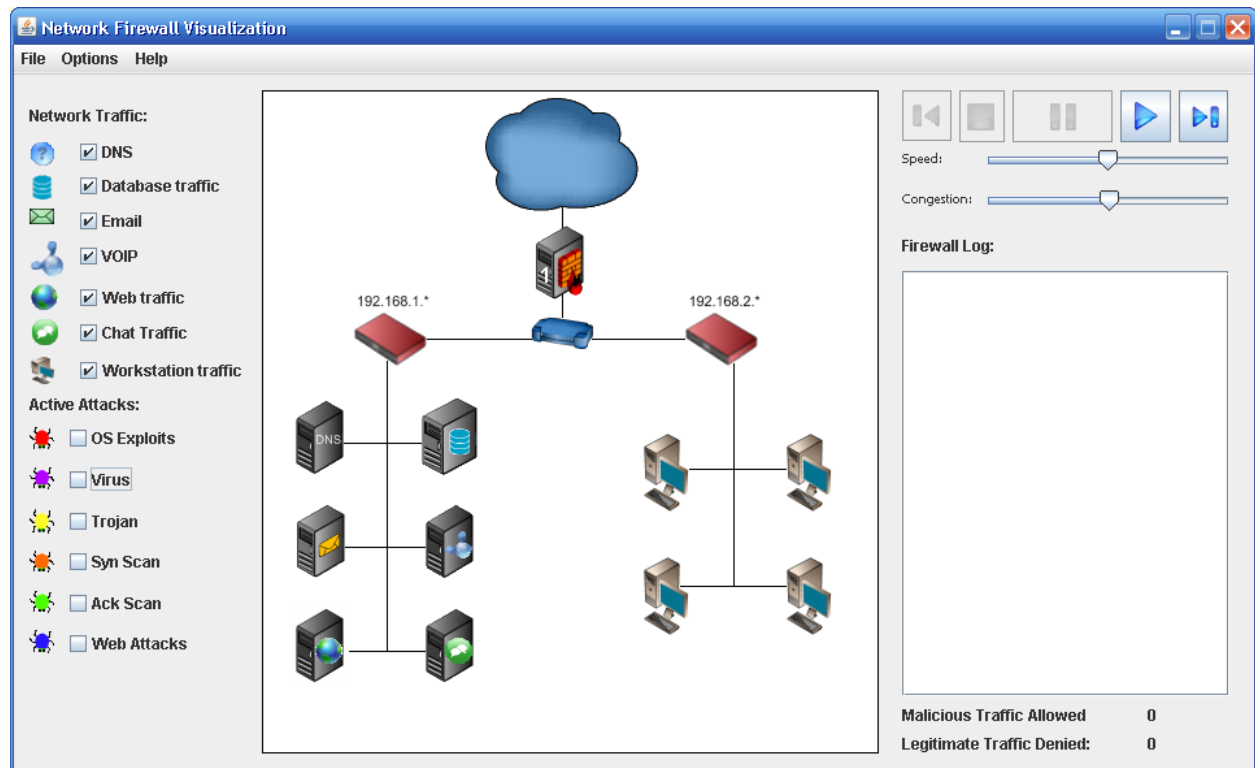
You now have a firewall between the internet (represented by a cloud) and your network router. Click the play button and watch what happens. **Do you see traffic flowing from the internet into your system or from your network to the internet? Explain why or why not:**

No, everything passed through FW1 is being legitimate traffic denied from both internet into system or from network to the internet.

2. Add some active attacks by clicking on several different options. **Are these attacks able to get to your network? Do you feel your system is secure? What's wrong with this scenario?**

No, none of these attacks be able to get to my network. The system is isolated from the internet with its network. It is secure if no malicious virus inside. But nothing can get through the perimeter firewall, even the regular communication with the internet. It does

not match the purpose for network, and nothing being detected as virus blocked on the firewall logs.

3. Configure your firewall to allow traffic to flow in and out of your network. Do this by choosing the 'options' tab at the top of the tool and define firewall rules. You should see a screen similar to the one below:
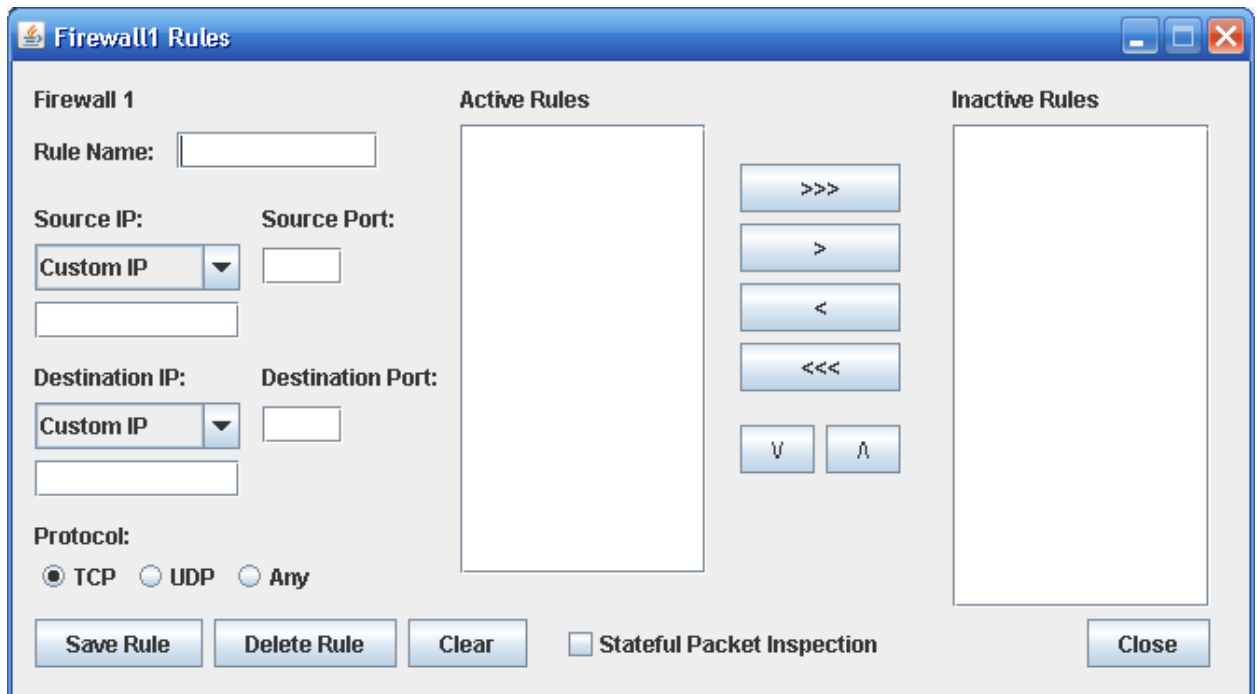
Name your firewall rule (typically with a name that focuses on a given subject or attack). The "Source IP" option and port refer to how you want the firewall to recognize a given source IP/Port combination and respond. The Destination is similar but focusing on a destination rule. The goal of any good firewall configuration is to identify legitimate traffic while restricting malicious traffic. Try setting the following firewall rule:

    Rule Name: DNS Rule
    Source IP: DNS, Source Port: 53
    Destination IP: Any, Destination port *
    Protocol: Any.

Click "Save Rule". You should now see the rule in your Active Rules box. Click "close" and you should be back to your Network Firewall Visualization Tool window. Click the play button and watch what happens. You may need to move the speed bar to the right

for a higher speed of traffic. **What traffic now flows through the firewall?** Add some active attacks and watch if they flow through the firewall. **Would you claim your rule is now sufficient to allow traffic to flow for a typical network? Why or why not? Do any of the active attacks now work against machines behind the firewall?**

Only DNS can pass through the firewall from network to internet.

No, the rule is not sufficient as it will only allow specific kind of network of traffic pass through with specific rules. User has to set up all possible rules to allow network traffic pass through or it will be denied. Only Malicious traffic allowed, and legitimate traffic denied close to 0 will be the most sufficient. I didn't see any active attacks work against machines behind the firewall, they all blocked by the firewall.

4. Come up with a series of rules which seems to protect the network from all attacks. Be sure to watch the legitimate traffic denied and malicious traffic permitted in the lower right hand portion of the screen. That should tell you how well your rules are working. **How many rules did you have to write to secure your network? Were you able to completely secure the network? What types of rules did you create?**
I have to set up every rule for every possible item in both ways. For possible network traffic I have to set up 17 rules to allow them pass through the firewall. It is hard to completely secure the network as you don't know all the possible network traffic items like how many workstations will you have. You have to block web, chat, and email from any to block the malwares. Firewall rules only allow the ruled item pass through one way of the firewall and block all the malicious traffic outside as they didn't assign in the rule with source ip and destination. I create the DNS rule, Database rule, VOIP rule, Workstation rule, etc.

5. Download the WorkstationDatabase scenario from the tools page of the web site and save it to your desktop. Choose File -> new to restart the program and click "load from file" button, pointing the program to the file you downloaded.

This scenario was configured so that workstations can pass through *firewall2* and gain access to the database. *Firewall1* has an ***allow all*** traffic rule set so all information is passed through to the network and from the network to the servers. Write rules to prevent active attacks from passing through *firewall 1* and attacking the database. **Which active attacks are you able to prevent by restricting access on the firewall?**

For firewall1, I inactive all in and all out rule but set up rules which allow any to database, and database to any.