Department of Informatics
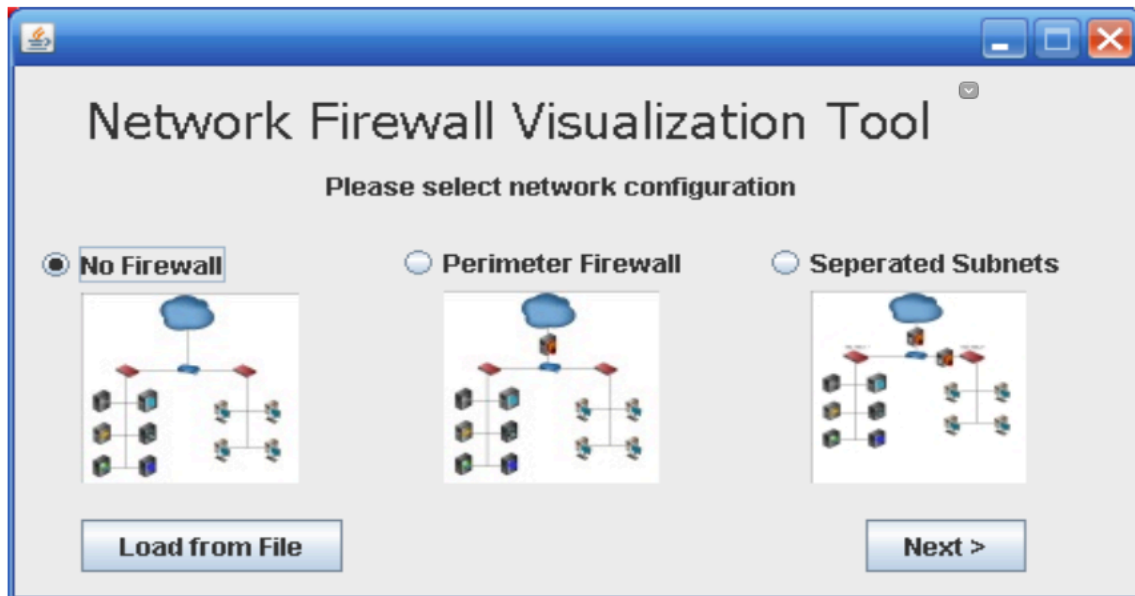
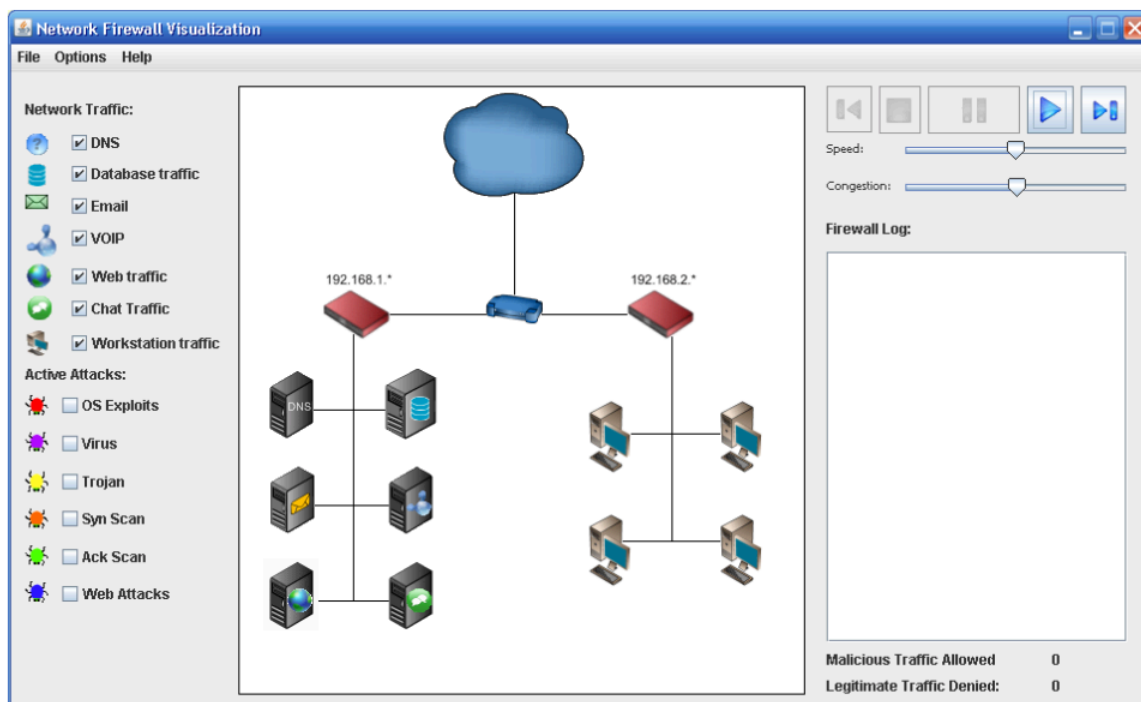# FIREWALL SIMULATION

Network Security

Diego Sempreboni

INTRODUCTION

1. Start the Firewall program FirewallVisualizationTool.jar.
   - You should see a screen similar to the one below:

   - Choose "No firewall" and click "Next". The following screen will appear:

- Click the "play" 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.
- Let us see how configuring a firewall will help prevent such infections.

2. Start a new session by clicking "File -> New" in the upper windows of the tool. This time, choose the Parameter firewall. The window that comes up will look like this:
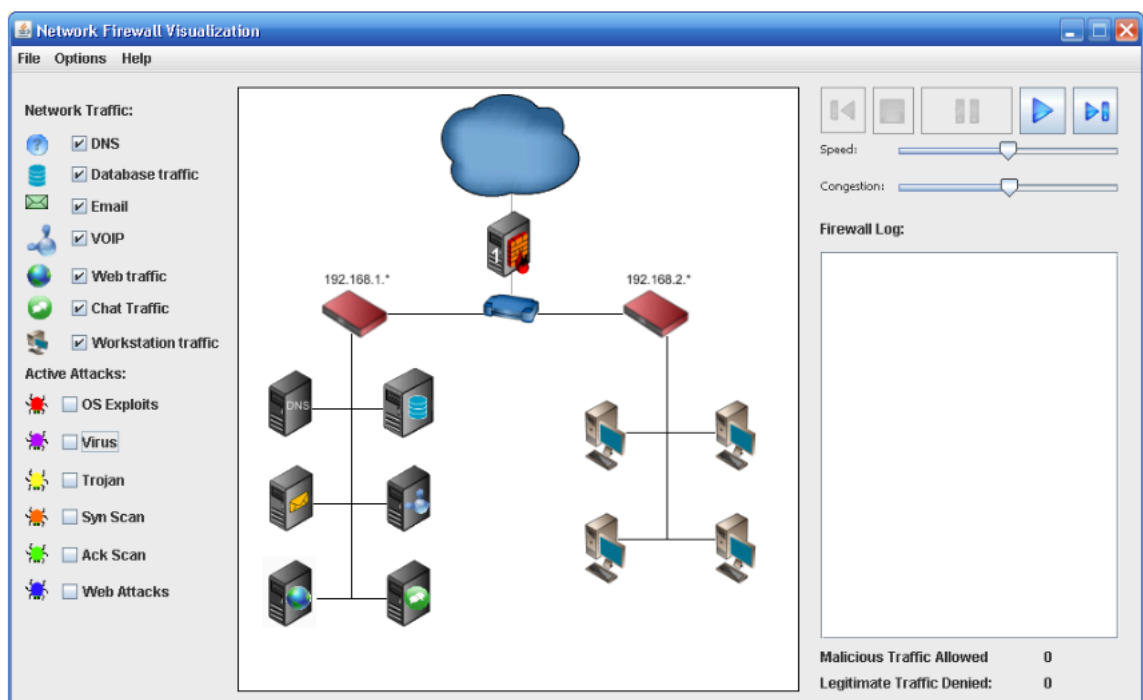
You now have a firewall between the internet (represented by a cloud) and your network router.

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:

3. 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 is wrong with this scenario?
4. 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 tool and define firewall rules.
   - You should see a screen like below:
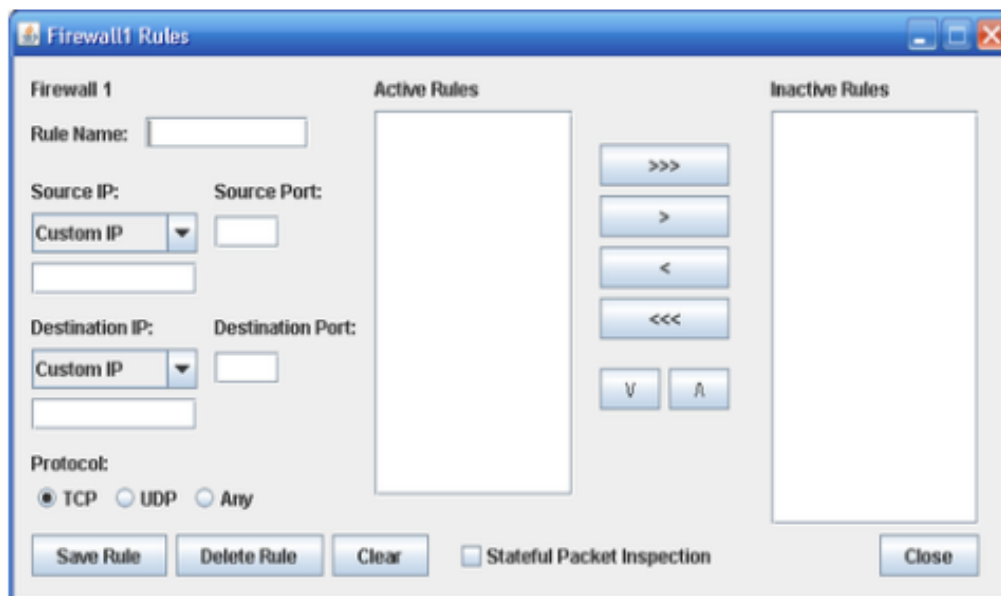
- Name your firewall rule (typically with a name that focuses on a given subject or attack).
   - The "Source IP" option and port refer to how you want the firewall to recognize a given source IP/Port combination and respond.
   - The Destination is similar but focusing on a destination rule.
   - The 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 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?

5. 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?

6. Use the WorkstationDatabase scenario in the file `FirewallWorkstationDataFile.dat` (choose "File -> New" to restart the program and click the "load from file" button, pointing the program to the file .dat).
   - 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 "Firewall1" and attacking the database.
   - Which active attacks are you able to prevent by restricting access on the firewall?

7. If you have time, have a look at the paper Firewallpaper.pdf (thanks are due to the authors of that paper and to Kevin Curran).
8. Also have a look at http://jekor.com/gressgraph/.