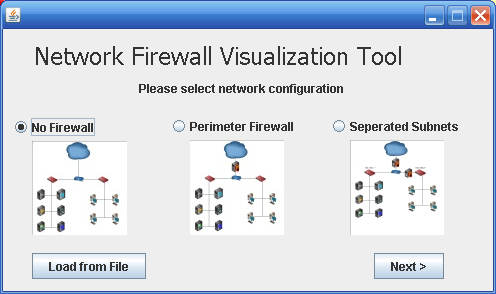
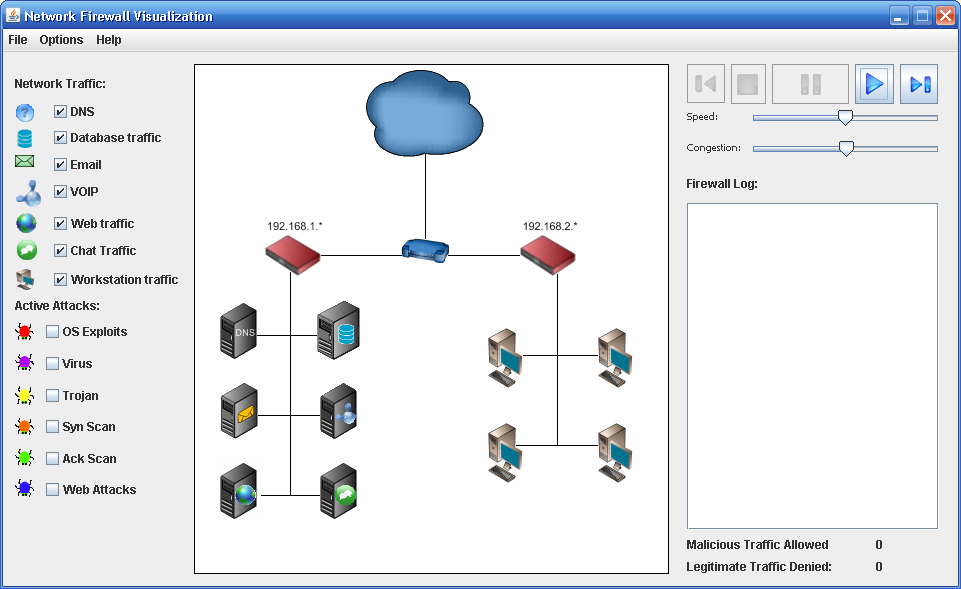
Firewall Exercise

1. Start the Firewall Visualization Tool program. You should see a screen similar to the one below:



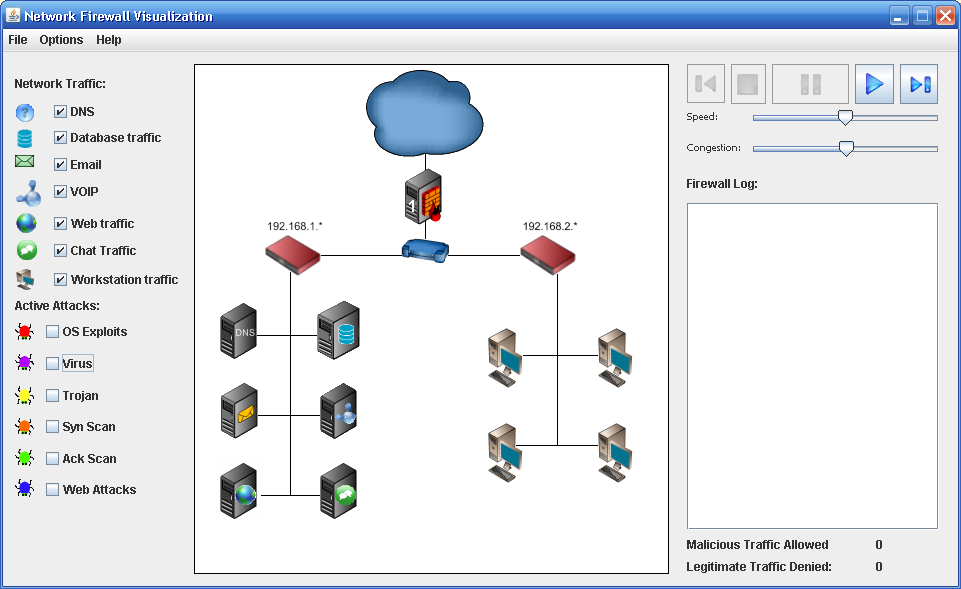
Choose “no firewall” and click next. The following screen will appear:



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:



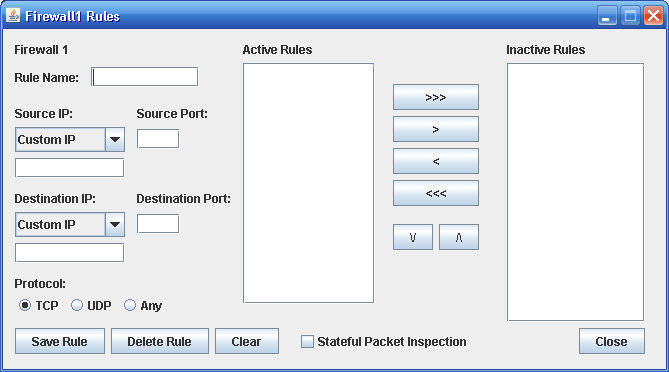
You now have a firewall between the internet (represented by a cloud) and your network router. Click the play button and watch what happens.

**Questions:**

1. **Do you see traffic flowing from the internet into your system or from your network to the internet?** No
2. **Explain why or why not:** The firewall does not have any rules that allow anything to pass through it.
3. Add some active attacks by clicking on several different options.

**Questions:**

1. **Are these attacks able to get to your network?** No they are not
2. **Do you feel your system is secure?** The system is very secure from any external attacks, but not internal attacks.
3. **What is wrong with this scenario?** Nothing is allowed to pass from the internet into the network or out to the internet. The only thing that can happen is traffic internally.
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 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.

**Questions:**

1. **What traffic now flows through the firewall?**

The DNS can go from the internal network to the internet, but cannot come in from the internet.

1. **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?**

Not yet

1. **Why or why not?**

Nothing besides DNS can go out from the internal network, so it will need to allow other things to come in and go out.

1. **Do any of the active attacks now work against machines behind the firewall?**

No active attacks have been let through the firewall.

1. 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.

**Save the simulation (File->Save Simulation) to YourUserNameFirewallData4.dat File and submit it with this word file when the questions are completed.**

**Questions:**

1. **How many rules did you have to write to secure your network?** 12 rules
2. **Were you able to completely secure the network?** Very few of the malicious traffics were able to get through, but it was not completely secured.
3. **What types of rules did you create?** I created rules that allowed each of the different types in from the cloud, plus each of the types allowed to go anywhere.
4. Choose File -> new to restart the program and click “load from file” button, pointing the program to Firewall Workstation Data 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 *firewall 1* and attacking the database.

**Save the simulation to YourUserNameFirewallData5.dat File and submit it with this word file when the questions are completed.**

**Questions:**

* 1. **Which active attacks are you able to prevent by restricting access on the firewall?**

OS Exploits, Virus and Trojan

* 1. **Think back to the class discussion on malicious software attacks and distributed denial of service attacks.**

**Using the information from that class, why do you think that these types of attacks are not able to be prevented through the firewall?**

Those are harder to block because the source IP can be the same as a good traffic type.

* 1. **How might you prevent these attacks from taking place?**

You could set up to make sure that the router that the internet is coming through checks to see if the IP for the incoming types, making sure that it is coming from the same location that it says it is from.