

CSC3064 Practical 3 Firewalls

This practical explores the configuration and implementation of firewalls using a Network Firewall Visualization Tool¹. Within the tutorial, there are some short questions for you to answer. Make a note of your answers and we will discuss them in class next week.

The Network Firewall Virtualization Tool is hosted on a Linux virtual machine (VM1 used in Practical 1).

1. From the Windows Desktop, open the folder C:/Vbox/CSC3064/
2. Double-click on the xubuntu1 VM to launch it in virtualbox. Select Import.
3. Start the xubuntu1 VM. Username: xub, Password: CSC3064_2018

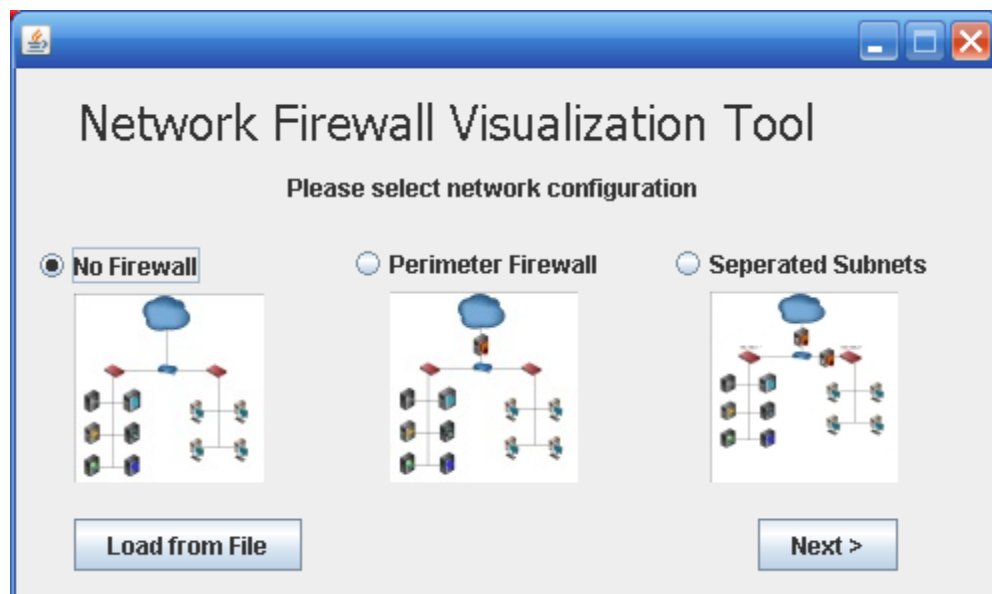
Step 1: Start the Firewall program as follows:

On VM1, open the command prompt and enter the following commands:

```
cd ~/Desktop/CSC3064_Practicals/Practical2
```

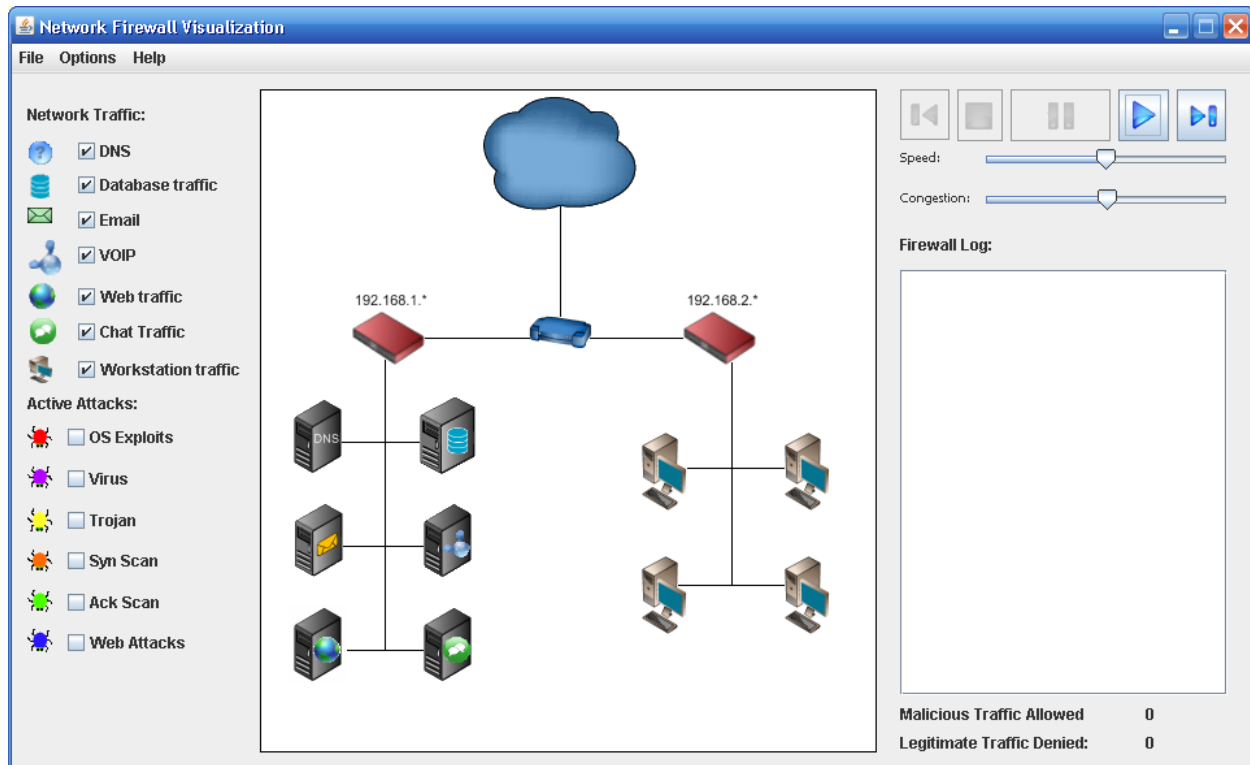
```
sudo java -jar Firewall\ Visualization\ Tool.jar
```



You should see a screen similar to the one below:



¹ The Network Firewall Visualization Simulator is provided from Pearson's Instructor Resource Centre for William Stallings Network Security Essentials. The tool was developed at U.S. Air Force Academy.

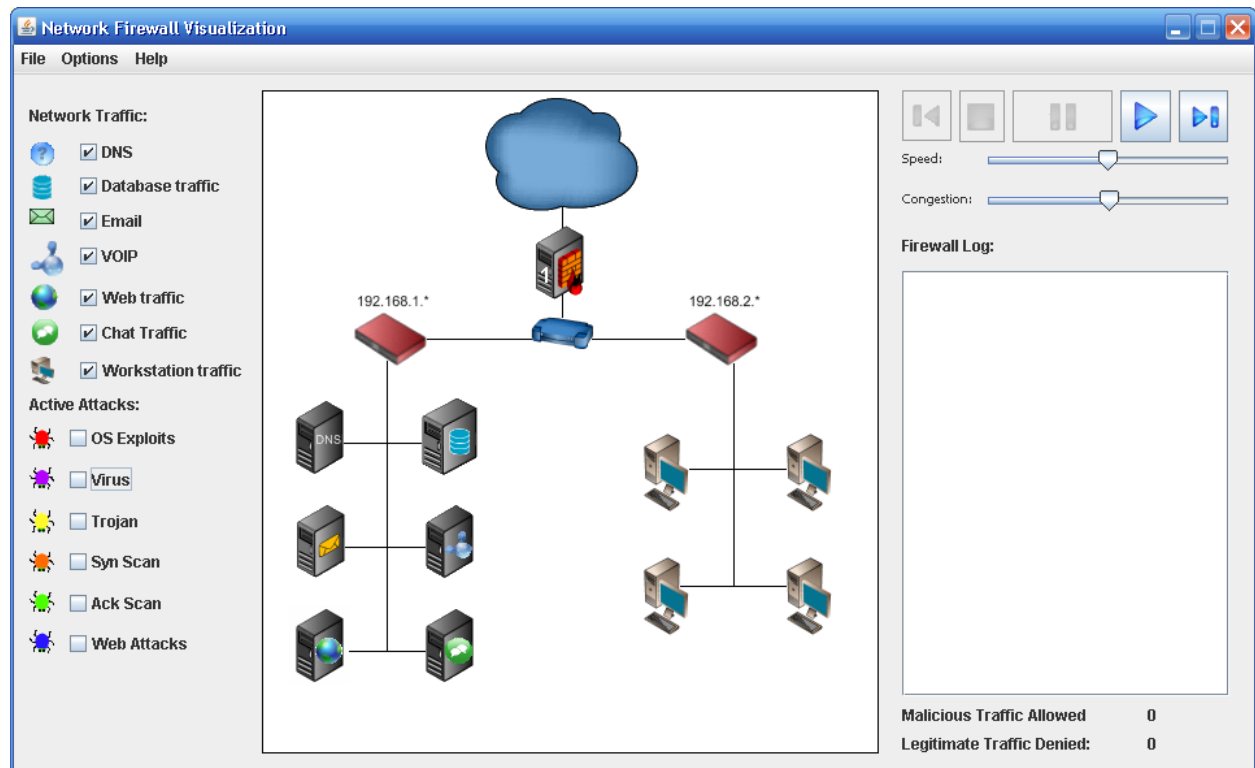
Step 2: Choose “no firewall” and click next. The following screen will appear:



Step 3: 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:

Step 4: Start a new session by clicking File -> New in the upper window of the tool. This time, choose the “Perimeter 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.**

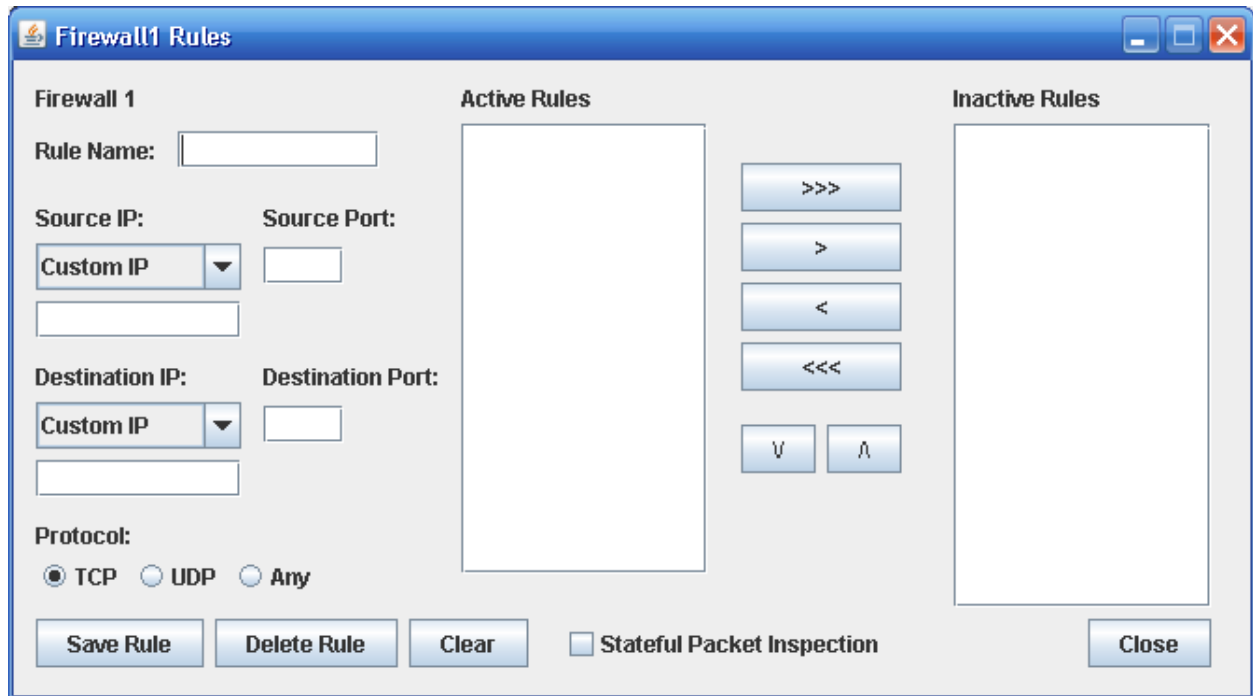
Step 5: Add some active attacks by clicking on several different options. **Are these attacks able to get to your network? Do you feel your system is secure? What's wrong with this scenario?**

Now answer questions 1 and 2.

Lab3 Q1: Is traffic flowing from the internet into your system?

Lab3 Q2: Do you feel your system is secure?

Step 6: 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 on the next page:



Step 7: 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?**

Now answer questions 3 and 4.

Lab3 Q3: What traffic flows through the firewall after adding your DNS Rule?

Lab3 Q4: Which active attacks (e.g. OS Exploits, Virus etc.) now work against machines behind the firewall?

Step 8: Come up with a series of rules, which seem 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?**

Now answer questions 5-9.

- Lab3 Q5: How many rules did you have to write to secure your network?
- Lab3 Q6: What firewall rule(s) did you create to allow chat traffic on the network?
- Lab3 Q7: Which active attacks now work against machines behind the firewall?
- Lab3 Q8: What does the stateful packet inspection flag on this firewall do?
- Lab3 Q9: Is this the behaviour you expect from stateful packet inspection? Briefly explain.

Optional Exercise:

1. Choose File -> new to restart the program and click "load from file" button.
2. Select Files of Type: All Files
3. Navigate to the Workstation Database Scenario file
(/home/xub/Desktop/CSC3064_Practicals/Practical2/Firewall\ Workstation\ Data\ File.dat) and open it.
4. 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?**