

Module Fifteen:

Firewall Configuration

Grading

Note: You will need to have a partner for this lab to exchange keys with.

Total points: 32

☐ [2 points] Your submission is labeled as “cyb404_module15_lab00_[nauid]_[lastname]_[firstname].pdf.” For example, if I were in Group 1, to submit a file, it would be labeled as cyb404_module15_lab00_mv668_vigil-hayes_morgan.pdf. FAILURE TO COMPLY WITH THIS STEP CAN LEAD TO A ZERO GRADE.

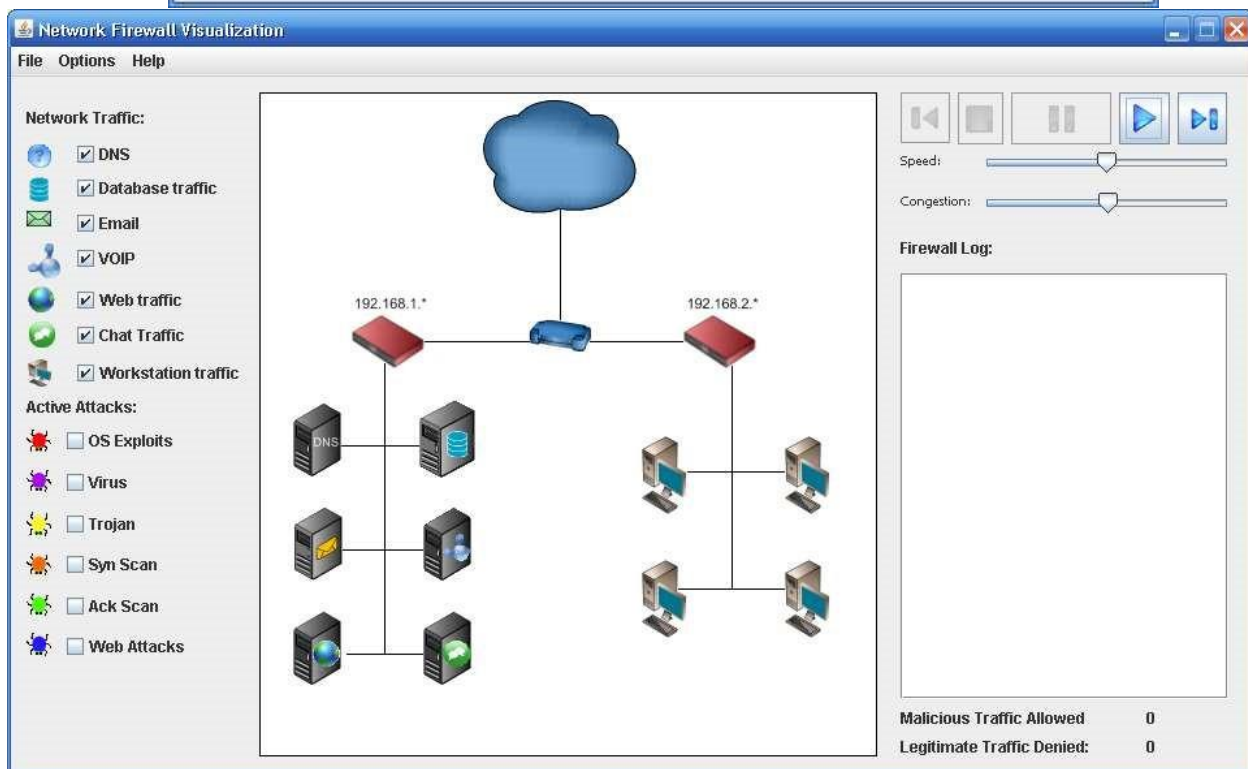
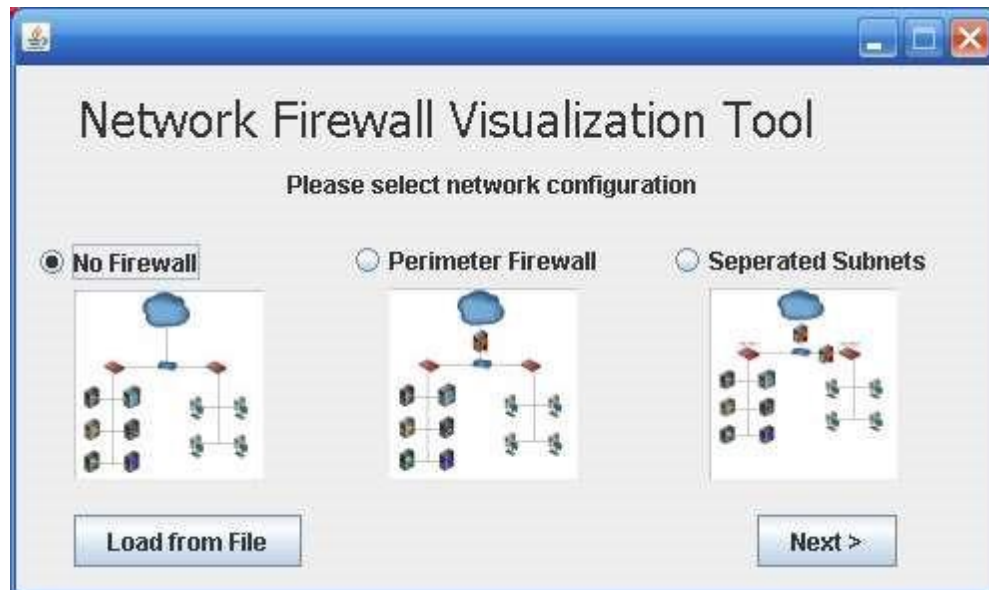
☐ [30 points] You thoughtfully reflect and respond to Q00-Q05 with at least 150 words per response.


Part 1: Exploring Firewall Rules

First, you may need to install the Java Development Kit (JDK) if you do not already have it installed. Download and install from this page: <https://www.oracle.com/java/technologies/javase-jdk15-downloads.html>

1. Start the Firewall program from the attached JAR file. 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

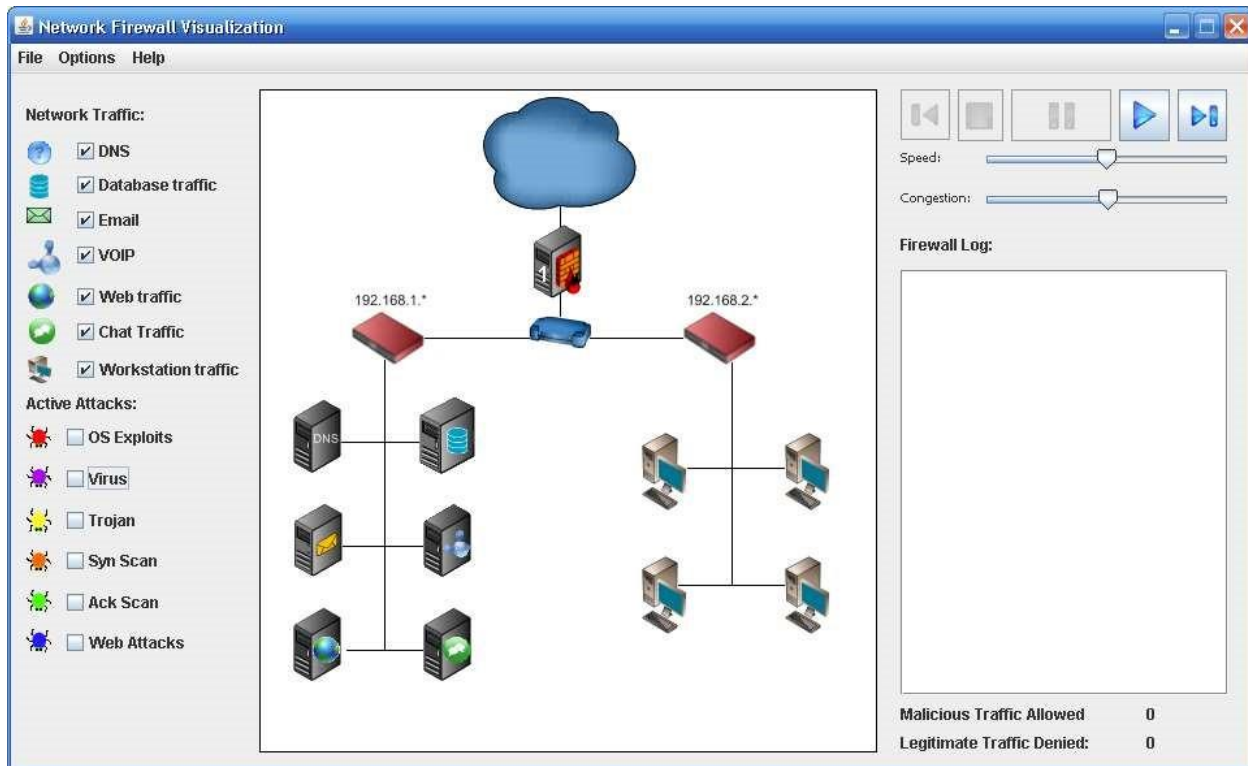
machine is infected, it is marked as such with the “international No” emblem



or . Let’s see how configuring a firewall will help prevent such infections.

FIREWALL Configuration.

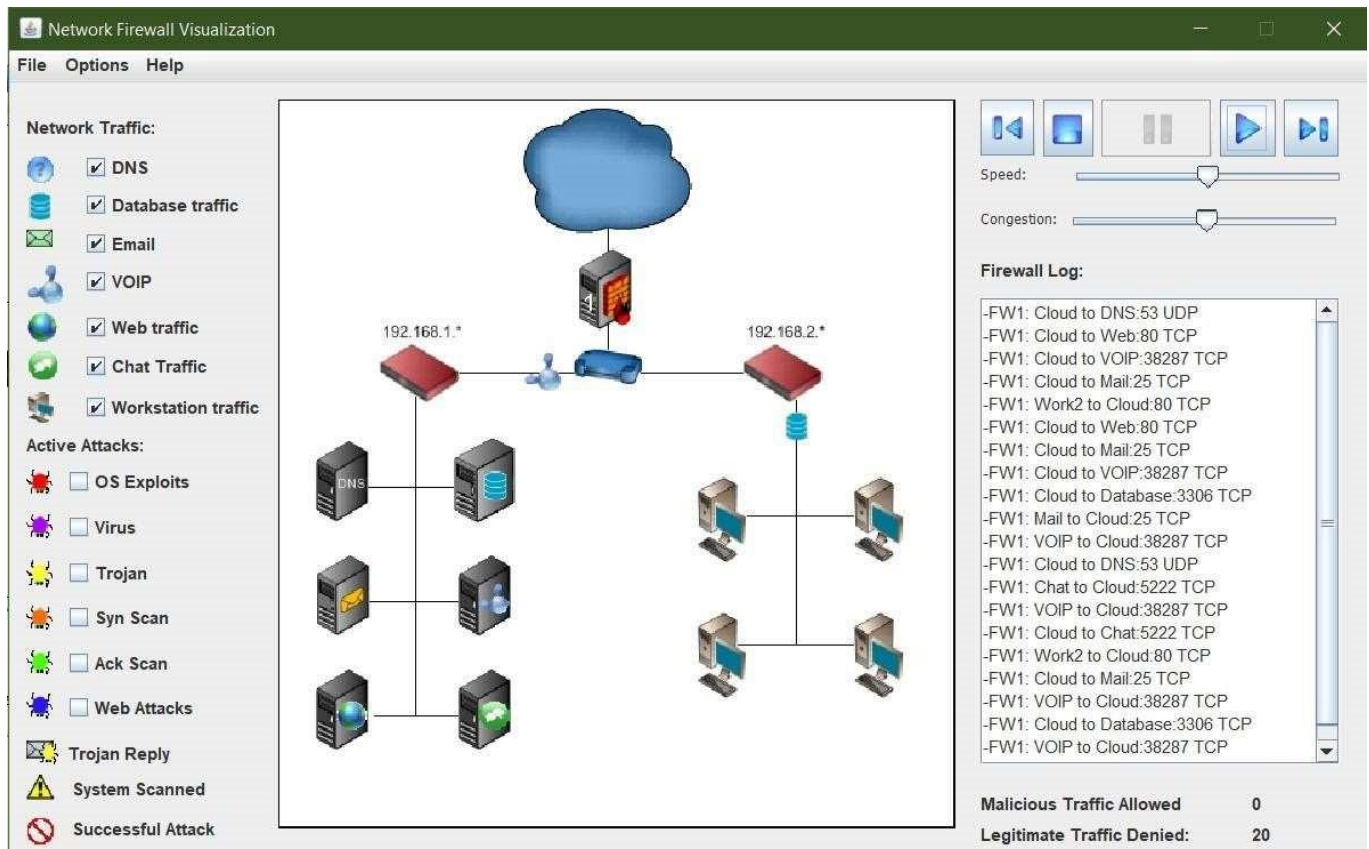
1. Start a new session by clicking File -> New in the upper window of the tool. This time, choose the Parameter firewall. The window that comes up will look like this:



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

Q00. Do you see traffic flowing from the internet into your system or from your network to the internet? Explain why or why not:

Yes. On the firewall log page, I can see the network flowing from the internet to the system, as well as what legitimate traffic is being refused. The firewall log shows blocked packets organized by source, destination, port, and protocol. All transport or media connection packets, as well as their port numbers and IP addresses, are included in the traffic stream. The traffic flow is a sequence of packets that move from source to destination, and the traffic flow only goes through the test packet headers, not the content.



Q01. 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?

Even though these attacks are impossible to reach my network when my firewall is switched on, I do not feel safe, because closing the firewall degrades the system's security and exposes your PCs to the attack, according to me. The attack will be able to infiltrate and abuse your system if I set up the firewall and create rules to allow traffic from any network and port. However, allowing various attacks via the peripheral firewall does not allow the attack to get past my firewall; my firewall claims to accept traffic but does not. Because we haven't established any firewall rules to decide which services and ports to allow, we don't have access to the server.

Optim Hlp

Network Traffic:

☒ DNS

@ VOIP

@ ChatTraffic

☒ Workstation traffic

Active Attacks:

☒ OS Exploits

☒ Virus

☒ Trojan

☒ Syn Scan

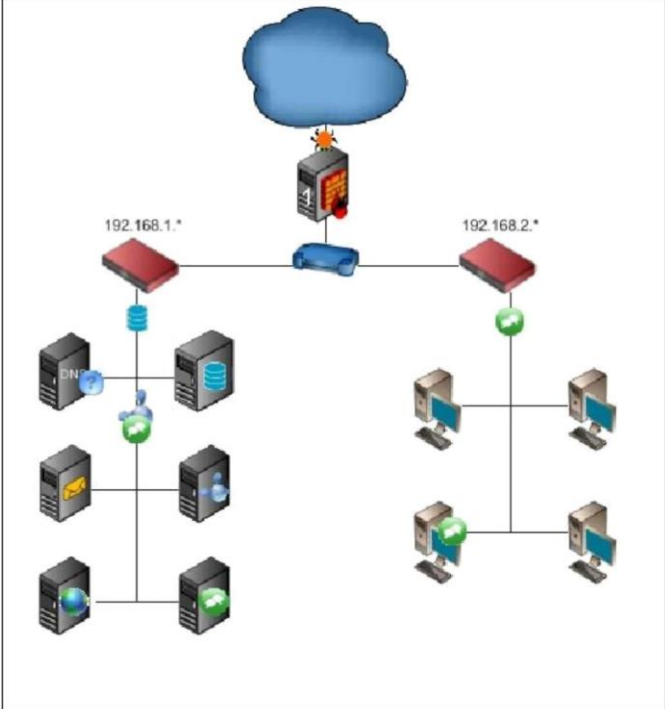
☒ Ack Scan

☒ Web Attacks

Trojan Reply

System Scanned

Successful Attaslt



Speed:

Firewall Log:

- FW J: Cbcxl to Mail:0 TCP
- FW1: Cbud to Chat:5222 TCP
- FW J: Clocxl to DNS:53 UDP
- FW1: Cbud to DNS:0 TCP
- FW J: Cbcxl to Work3:12345 TCP
- FW1: Cbud to Web:80 TCP
- FW J: Work4 to Cbud:80 TCP
- FW1: Cbud to Chat:31337 TCP
- FW J: Cbcxl to Chat:5222 TCP
- FW1: Cbud to Web:80 TCP
- FWJ: Cbcxl to VOIP:38287 TCP
- FW1: VOIP to Cbud:38287 TCP
- FW J: Mail to Cloud:25 TCP
- FW1: Cbud to VOIP:38287 TCP
- FWJ: Cbcxl to VOIP:3J337 TCP
- FW1: Cbud to Work3:12345 TCP
- FW J: Database to Cbud:3306 TCP
- FW1: Cbud to Ma1:445 TCP
- FW1: Database to Cbud:3306 TCP

Malicious Traffic Alloaad 0

Lagltkrate Trafflo Danled: 66

2. 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:

Firewall1 Rules

Firewall 1

Rule Name:

Source IP: Source Port:

Custom IP

Destination IP: Destination Port:

Custom IP

Protocol:

☒ TCP ☐ UDP ☐ Any

Save Rule Delete Rule Clear ☐ Stateful Packet Inspection Close

Active Rules

Inactive Rules

- 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 focuses 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.

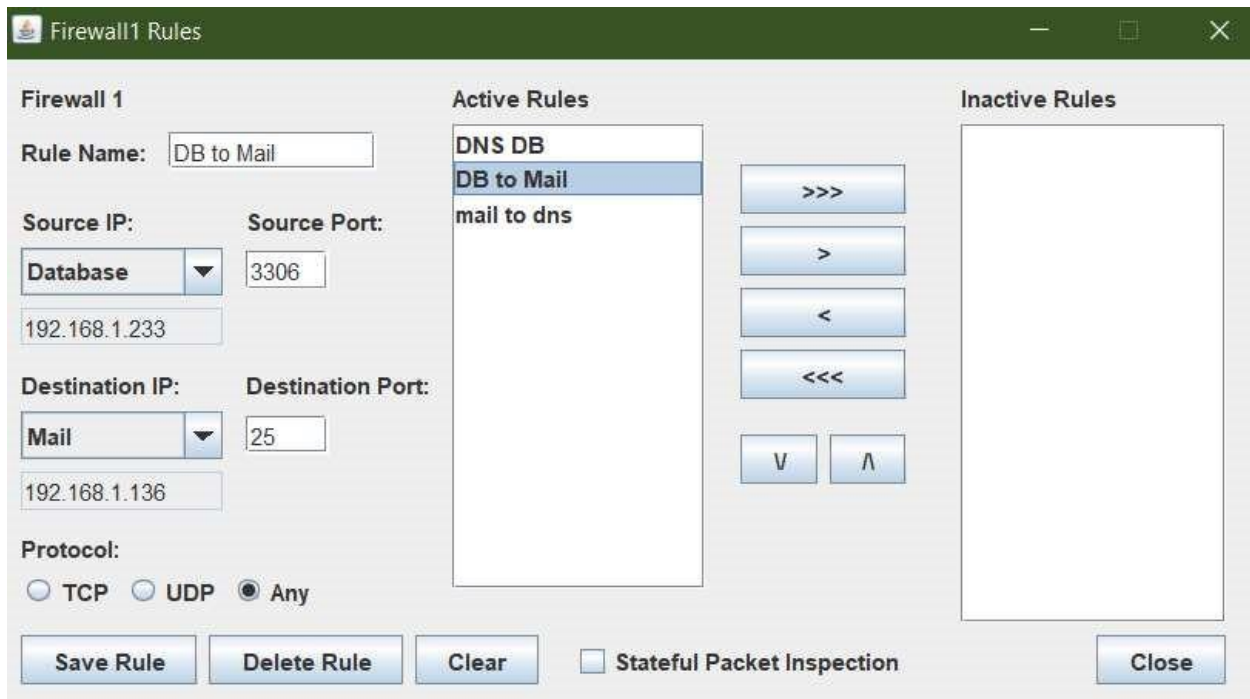
Q02. Would you claim your rule is now sufficient to allow traffic to flow for a typical network? Why or why not? Do any of the active attacks now work against machines behind the firewall?

Yes! This rule is sufficient to allow traffic to flow in a normal network. We're going to whitelist the connection on the firewall, and we'll have to change our firewall rules to enable active assaults to get through. As a result, if the rules are poorly specified and fail to meet the criteria, our connection will be denied permanently. As a consequence, we put up a rule that permits traffic to get past the firewall in order for traffic to transit over the network. Active assaults against machines protected by firewalls are similarly ineffectual. Only communication from the originating DNS IP is whitelisted on port 53, and it utilizes whatever port is available. If the firewall rule did not meet the packet rules, the packet was denied.

Q03. 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?

To secure my network, the following are the rules below:-

- 1) The source IP for the DNS to DB rules is the DNS, and packets are routed from DNS on port 53 to the database on port 3306. DNS, on the other hand, is primarily intended for TCP and UDP tracking. The UDP protocol, on the other hand, is mostly utilized by DNS.



- 2) The next method I use to secure the network is to utilize the database as the source IP on port 3306, which is trusted for TCP transmission, and mail on port 25 as the destination.
SMTP protocol used to send or receive mail from recipients on the Internet
- 3) The IP address in this rule source is web, and it is using port 80, which is a web-based communication port. Finally, there are compensating rules in place to avoid network attacks. I created these rules for various ports since the port determines whether a request is made from the incoming server and if the destination is permitted in or not. It will allow the incoming request if it comes from the source port and IP that I specified in the operating rules; else, it will refuse all incoming requests. The request always includes the port number.

Firewall1 Rules

Firewall 1

Rule Name:

Source IP: Source Port:

Destination IP: Destination Port:

Protocol:
☐ TCP ☐ UDP ☒ Any

Active Rules

DNS DB
DB to Mail
mail to dns

Inactive Rules

>>>
>
<
<<<
V Λ

Save Rule Delete Rule Clear ☐ Stateful Packet Inspection Close

Firewall1 Rules

Firewall 1

Rule Name:

Source IP: Source Port:

Destination IP: Destination Port:

Protocol:
☐ TCP ☐ UDP ☒ Any

Active Rules

dns
Web_to_data

Inactive Rules

>>>
>
<
<<<
V Λ

Save Rule Delete Rule Clear ☐ Stateful Packet Inspection Close

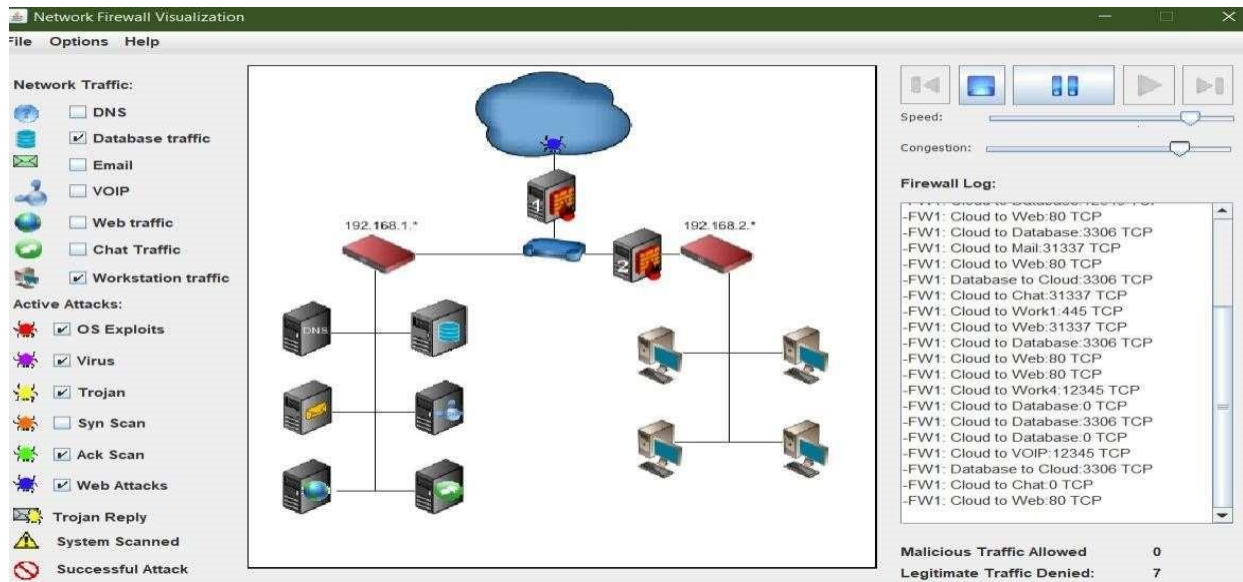
Part 2: Installing firewalls

Download the Firewall Workstation Data File.dat scenario from BbLearn 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.

Q04. Which active attacks are you able to prevent by restricting access on the firewall?

We need to set up the firewall such that it can block traffic from the Internet while also prohibiting direct access from the Internet service, which might expose it to a number of active assaults. To protect our database, I created a firewall rule that only permits access from the client to the database on port 3306. 3306 is a TCP port that employs the control protocol, which is one of the most important protocols in TCP/IP networks. I can protect myself from operating system exploits, malware, Trojan horses, ACK scanning, and web assaults. It is possible to build a connection between two servers and exchange data streams. TCP guarantees that packets are sent appropriately while creating firewalls, and the main differentiator between TCP and UDP is 3306. However, if UDP port 3306 is configured, inbound packets may be missed. or copy in such a way that the UDP port lacks the same level of safety and security as TCP. I reran the attack after setting my rules, and I was able to observe that all of the continuing attacks continued even after the rules were set to everything, and it was no longer able to abuse my system. In this scenario, I was able to thwart OS exploits, Trojans, validation scans, online assaults, and infections.



The **Firewall1 Rules** window shows the configuration for rule **wrk_to_data**. The **Rule Name** is `wrk_to_data. The Source IP is Workstation 1 (192.168.2.100) and the Source Port is 3306. The Destination IP is Database (192.168.1.233) and the Destination Port is 3306. The Protocol is set to TCP. The Active Rules list contains Any_to_database and wrk_to_data. The Inactive Rules list contains All In and All Out. Navigation buttons include >>>, >, <, <<<, V, and Λ. At the bottom, there are buttons for Save Rule, Delete Rule, Clear, a checkbox for Stateful Packet Inspection, and a Close button.`

Q05. 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? How might you prevent these attacks from taking place?

A malicious software attack is a type of attack that leverages or exploits a person's computer system using multiple attack vectors such as computer viruses, social engineering assaults, phishing, and other methods. A DoS attack includes flooding a server with fictitious requests in order to render a service or network unusable. There are a number of strategies for preventing this sort of attack, and a strong firewall can assist to some extent. Firewalls safeguard unknown and external traffic networks that aren't detected by the ruleset, preventing malware attackers from reaching your machine over the internet using established rules. It may also be used to guard against DoS attacks by specifying which traffic must be permitted, capturing data from specified ports, and addressing it such that only the data needed gets through. Firewalls, on the other hand, are powerless in the face of social engineering or human error attacks.