III. THE NETWORK FIREWALL VISUALIZATION TOOL

Five senior students recently created the Network Firewall Visualization Tool under the mentorship of a faculty member during their capstone course. This capstone course is taught during two sequential terms in which students work on projects identified by either faculty members or industry representatives. The goal of the capstone course is to permit teams of students to perform real world system engineering functions including formal design review meetings, schedules with strict milestones and detailed system analysis with the customer being the organization or person who has requested the project.

The need for the Network Firewall Visualization Tool was identified by CS department faculty members who teach network topics to various class levels. The goal of the tool is to give students the opportunity to experiment with creating firewall rules to identify and stop network attacks. Accomplishing this task using actual firewall equipment would be expensive and difficult to maintain and monitor in a lab environment.

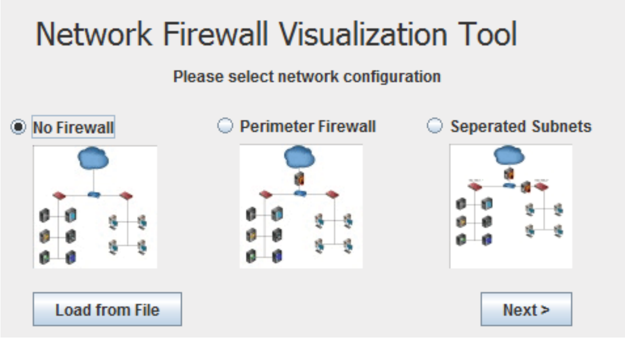
The Network Firewall Visualization Tool is a Java based program designed to run on individual laptops. At our institution, students are required to purchase laptops as freshmen and to bring them to their classrooms to perform tasks associated with the individual classes such as note taking and programming.

The Network Firewall Visualization Tool represents three distinct networking environments: a network with no firewall, a network with a single firewall, and a network with two different firewall configurations. The tool is further separated into several major components:

Network Selection
Traffic Definition
Simulation Control
Simulation Report
Simulation
Rule Creation
User Help

With the exception of the network layout, each component can be dynamically modified at any time during the scenario and the simulation will automatically update its course of action. For example, after defining traffic type and beginning the simulation, rules may be changed or new attacks may be added. The simulation will update automatically to reflect these changes. Furthermore, the current network setup including network selection, traffic, and rules can be saved to a file at any time for use in a later demonstration.

A screenshot of the network selection dialog is shown in Figure 1: Network Selection Dialog Box. By default, our tool provides three standard network layouts common in traditional network security: no firewall, perimeter firewall, and a two firewall setup with a DMZ. As seen in Figure 1, the user has the ability to select which layout they would like to use or to load prebuilt scenarios from a file. This allows faculty members to create scenarios which can be loaded shared with the class. Additionally, students who have problems understanding a given scenario can save that scenario and share it with the instructor to allow the instructor to provide an analysis and feedback of the student's specific situation.

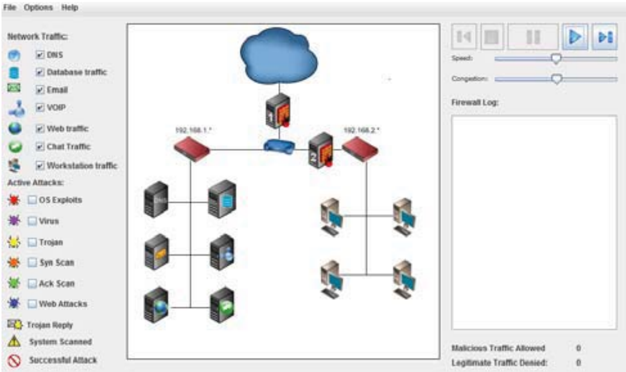

Network Firewall Visualization Tool
Please select network configuration
Load from File
Next >

● No Firewall ○ Perimeter Firewall ○ Seperated Subnets

Figure 1: Network Selection Dialog Box

After selecting a network or loading a scenario, the user enters the primary simulation screen as seen in Figure 2 – Main Simulation Window. The user may select options on the left to define the traffic present in a given scenario. Options allow enabling all of the represented services such as chat traffic, VOIP traffic, or DNS queries. When traffic is generated, it is visually reflected in the tool.

Some common attacks were included to test overarching concepts such as trojans (which exploit systems by removing information) or viruses (which propagate traffic which is hard to stop with packet filtering). As in real life scenarios, some of the attacks can not be stopped by a firewall, while others may be more easily controlled in such firewall scenarios.



Network Traffic:
☑ DNS
☑ Database traffic
☑ Email
☑ VOIP
☑ Web traffic
☑ Chat Traffic
☑ Workstation traffic

Active Attacks:
☐ OS Exploits
☐ Virus
☐ Trojan
☐ Syn Scan
☐ Ack Scan
☐ Web Attacks

Malicious Traffic Allowed 0
Legitimate Traffic Denied: 0

Figure 2: Main Simulation Window

The user can control the simulation using the buttons and slide bars in the upper right hand corner of the main window. These controls allow users to start, stop, pause or navigate through the scenario using buttons similar to the common DVD player (See Figure 2).

During simulation usage, students can measure their success with the firewall or debug a rule set using the log window on the right side of the main screen. This log screen will display blocked packets by source, destination, port and protocol. The counters at the bottom right indicate the number of malicious packets allowed through the firewall and the number of legitimate packets that were blocked. Ideally, a rule set would minimize both of these numbers. The goal of this tracking is to allow students to grasp the concept of the balance between security and usability while demonstrating that it is possible to secure a system to the point that it denies both legitimate and malicious traffic.

Figure 3: Firewall Simulation with Active Traffic illustrates the active usage of the system. Network packets are listed in the legend on the left as symbols (an envelope for e-mail packet, disk platter for database traffic, and so on). As traffic flows along the network, the symbol associated with a given packet moves from the Internet cloud to a given computer, or between computers depending on the type of traffic. For example, mail traffic may flow into the system from the Internet, or from a workstation to the mail server. As active attacks take place, small color coded 'bugs' travel across the network

to different machines as shown in Figure 4: Tool Icon Breakdown. The color coded symbols identify the type of attack being perpetrated against the network (i.e. red bugs symbolize an operating system exploit, etc.). Successful infection of a machine is identified through the use of the 'international no' symbol. Furthermore, once a machine is infected, that infection can spread to other workstations or servers, just as in a real life situation. By following traffic down the network, it is possible for the user to identify where the traffic flows and which systems are vulnerable to attack. As packets continue through the system, firewall logs are kept similar logs kept in active firewall systems. These logs are scrollable through the Firewall Log window.

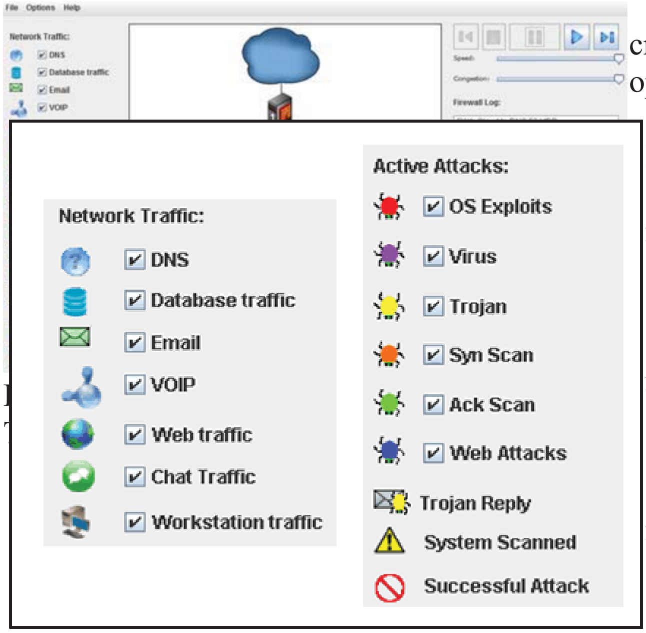


Figure 4: Tool Icon Breakdown

Users configure the tool by creating rules. To do so, the user opens up the firewall rules dialog for a given firewall as seen in Figure 5: Firewall Rule Dialog. Within this dialog, there are two boxes on the right which contain activated rules and inactive rules. New rules are created by first clicking on the "clear" button and inputting all of the required information (Name, Source IP, Source Port, Destination IP, Destination Port and Protocol). Once created, a user can move individual rules to the inactive side for debugging without having to delete and recreate the rule for later analysis. Rules are applied in the order in which they are placed in the active box. To simplify the configuration of the rules, users can use the drop-down boxes to select which service they desire for the source or destination and to use the auto-complete feature for the IP Address and Port information. The user can then save the rule by selecting the "save rule" button. If a rule needs to be modified or viewed, the user can click on the desired rule and the information will be updated in the correct fields. Finally, the user can make the firewall stateful by checking that option to prevent ACK Scans from passing through the firewall by reviewing the data within the packets to see if they are harmful to the network.

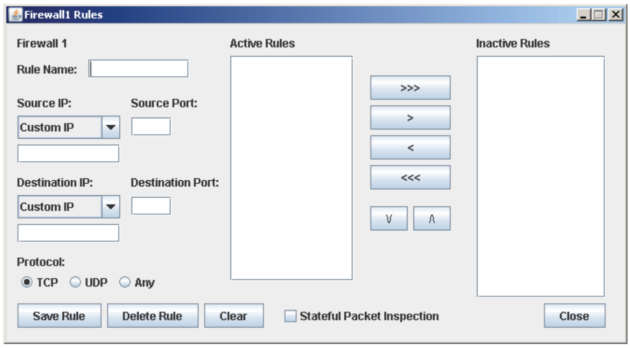
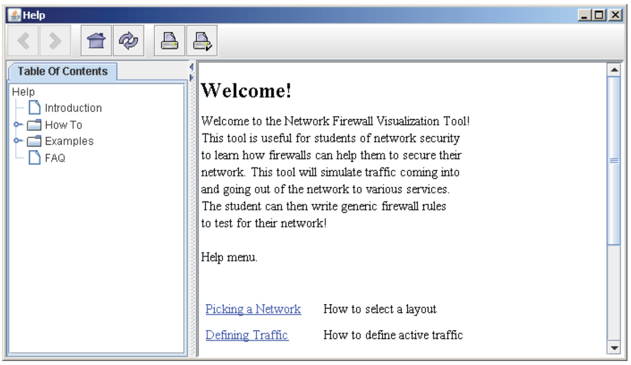


Figure 5: Firewall Rule Dialog

For help with all of these functions and concepts, the user can refer to the help documentation as illustrated in Figure 6: Help Dialog. The help pages are laid out to assist the user through each step of creating a scenario. Should the user want to skip to a specific area of the Help function, they can use the Table of Contents provided on the left hand side of the window. This help function was designed to mimic standard Microsoft Windows help functions.



Welcome!

Welcome to the Network Firewall Visualization Tool!
This tool is useful for students of network security
to learn how firewalls can help them to secure their
network. This tool will simulate traffic coming into
and going out of the network to various services.
The student can then write generic firewall rules
to test for their network!

Help menu.

Picking a Network How to select a layout

Defining Traffic How to define active traffic

Figure 6: Help Dialog

IV. TOOL USAGE

Our experience using visualization tools in the classroom suggests that students benefit from a formal guided path through the program. We have accomplished this by using exercises which not only guide the student through the use of the tools but also ask specific questions that force the student to draw conclusions based not only on what the tool shows them but their interaction with it. For example, in one exercise, a student is asked to create a rule with the following format:

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

Once the rule has been created, the student will begin the scenario by clicking the play button. As the traffic begins traversing through the simulation, students are then asked questions such as:

- What traffic now flows 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?

Without such formal guidance on the tool usage, we suspect the students will focus on the game-like aspect of the tool instead of focusing on understanding the rationale behind an attack being presented.

Such specific questioning of students also provides the opportunity to assess student understanding of a given scenario. At the end of the lab session, students submit answers to the formal questions for assessment by instructors. Such assessments allow instructors to understand exactly how well students are grasping a given topics.

By focusing on multiple attack types such as SYN, web attack, and ACK, the student is forced to ascertain why a given rule would stop one type of attack while permitting others. An example of this would be the SYN attack. In a SYN or TCP SYN Flood attack, a series of valid requests for a service is generated yet no connection to that service is created [10]. This would be something that is not typically solved using a firewall solution but instead by ensuring that the computer does not permit substantial hanging service requests. The simulation actually permits these SYN attacks to go through the firewall regardless of what students do to restrict this. By treating these attacks as they would be in the wild, students are forced to understand the details of the