12-2005

Studying the Performance of a Firewall in Network Courses

José M. Garrido
Kennesaw State University, jgarrido@kennesaw.edu

STUDYING THE PERFORMANCE OF A FIREWALL IN NETWORK COURSES*

José M. Garrido
Department of Computer Science and Information Systems
Kennesaw State University
Kennesaw, GA 30144
jgarrido@kennesaw.edu

ABSTRACT

This paper presents a simple simulation model of a firewall to derive several performance metrics and briefly argues on the importance and value of modeling and simulation in courses that study various aspects of perimeter defense in network security.

The simulation model mentioned previously is part of an effort by faculty of our department to develop a multi-disciplinary repository of computational models that includes object-oriented discrete-event simulation models. One of the goals of this repository is to build resources that help educate students of computer science, software engineering, and information technology, in modeling and information security.

This and other network simulation models are implemented in Java with the PsimJ simulation package. Other models have been implemented in C++ using the Psim3 package. The source code for the models, the downloadable simulation package, and more detailed description can be found on the Psim Web page.

Keywords: Simulation models, firewalls, networks, Java, education, performance.

INTRODUCTION

Modeling and simulation has shown to be very useful in the study of networks. In addition to studying the dynamic behavior of traffic through a network, such as

---

transmission, propagation, and queuing delays, estimates of various performance metrics can be derived to help identify traffic bottlenecks and other conditions in the network.

Simulation is one of the most powerful analysis approaches available to people responsible for the planning, design and/or operation of large and complex systems. Simulation modeling can not only deal with complex and large problems, it is a safe approach because it may be too difficult, dangerous, and/or expensive to experiment with the real system under observation. The testing of ideas (and mistakes) is carried out abstractly and under our own control, causing no danger and disruption to the real system. In information security, this advantage is even more important.

In the last few years, object-oriented modeling and simulation has become widely used. Real-world entities in a system are modeled as objects. Several books present a good introduction and more advanced principles in simulation modeling, [1] and [2] are two examples.

Several sources provide a good introduction and justification of the use of simulation in information security education, one such reference is Saunders [3]. He argues that individuals at different levels of the organization must respond in different ways to crisis and to planning of information defenses. Saunders lists several areas in information security in which simulation modeling can be utilized.

Seo and Cho in [4] discuss models and simulation of Intrusion Detection Systems (IDS). In the description of system modeled, several IDS agents are placed in a network then the simulation is run. Detection is assessed under various conditions.

Other important features of these simulation models in information security are:

- The simulation models allow promotion of better understanding of information security issues.
- Students have direct control of information security issues to be modeled, and in what level of abstraction.
- These models help students understand the various configurations possible for a firewall.
- Students apply object-oriented modeling with information security issues.
- Students are reinforced in their ability to specify, design, code in java, and test object-oriented software.
- The simulation package, PsimJ and several simulation models in Java are freely available from the Psim Web page.
- Analysis of intrusions and attacks.

Several excellent books explain the general concepts and principles of network activity, protocols, and security. Two such books in computer networking are Keshav [5] and Kurose and Ross [6]. An example of a book in network security is Kaufman [7].

Most of the commercial software tools available for simulation modeling are aimed at large-scale network design. Therefore, they are expensive and relatively difficult to learn and use. We take the approach that these tools are mainly useful for network professionals and for large network systems. The simulations models discussed in this paper are more general and are useful for educational purposes in academic settings. The students can add any relevant aspects they find necessary to a model. From point of views

of object-oriented modeling and the software development, the construction of these models also includes significant educational value.

Models in professional practice are also used to carry out risk assessment and cost benefit analysis of network security.

STUDYING PERIMETER DEFENSE USING OBJECT-ORIENTED SIMULATION

Several object-oriented discrete-event simulation models have been developed by faculty and students of the Department of Computer Science and Information Systems (CSIS) at Kennesaw State University. These models are mainly for general education in information security and for studying network activity and perimeter defense. These models include probabilistic routing for large networks, Ethernet model for studying performance, client-server database system, and several models of firewalls for studying non-trusted traffic and intrusion detection. Most of these models are freely available from the Psim Web page.

Animation of a model is an important aspect of simulations for illustration purposes, but more important is the trace and the performance estimates produced by the simulation runs. The trace shows the dynamic behavior of a model through time and illustrates the sequence of events that occur during a simulation run. Some of these events and the corresponding time occurrences for the firewall models are: generation of trusted and non-trusted packets, the firewall start processing of the various types of packets, the sequence of how the rules are applied by the firewall processor. The performance estimates are the values of relevant metrics computed by the simulation runs.

The main points that are illustrated by the firewall simulation models are, first, packet filtering; the various rules that are applied by the firewall when inspecting the packets. A more detailed analysis of simulation runs of the models would show the types of rules that are relevant and the ordering of these rules.

Second, the performance issues involved are important for practical considerations of this type of system protection. These models compute several performance metrics, the most important being: the number of packets dropped the number of packets inspected by the firewall, the average total delay for the packets, the average utilization of the firewall processor, and the average number of packets in the firewall queue.

Third, all activity of the firewall should be logged in an appropriate database. This important for auditing information protection effectiveness and help determine the type of traffic in the network and the vulnerability of the network system. We are currently enhancing a simulation model to include this facility.

The models for network security help validate the security specifications, help assess the vulnerabilities in network systems and the limitations of these types of perimeter protection for network systems. These models also emphasize the level of integrity and availability possible on network systems.

A SIMPLE SIMULATION MODEL OF A FIREWALL

A simple object-oriented simulation model implemented in Java and using the PsimJ simulation packet is briefly described here. This model is implemented as a Java console application; another version of the model includes a GUI and a simple animation developed by one of our students. Additional similar models have been developed recently.

The simulation model for the firewall includes the simple functionality of a Network Address Translation (NAT) router and a firewall. The model represents several entities that communicate via the Internet. Incoming traffic is represented by packets generated by an entity, InternetClient, located on an external network; the other end is an entity in the local network, LANServer. Traffic in the other direction is represented by an entity located in the local network (corporate LAN), LANClient, which attempts to send packets to another entity, located on an external network and is called the InternetServer. A Firewall is included mainly to protect the entities on the local network by blocking some traffic from the Internet and by blocking some traffic from the local network to the external network. Different packets are generated and transferred from one entity to the other but have to pass through the firewall. This simple model is illustrated in Figure 1. A client in an external network attempts to access a server in the local network. In a similar manner a client in the local network attempts to access a client in the external network.

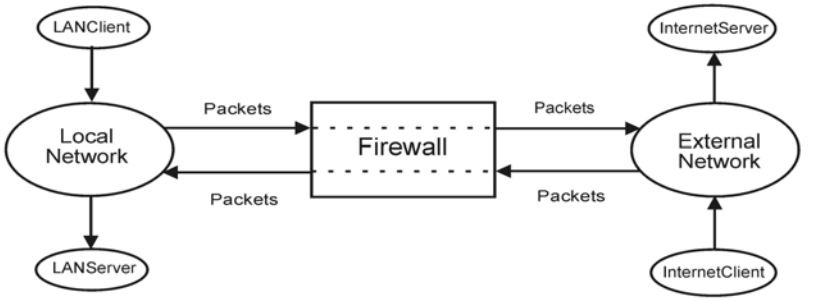

Figure1. Simple network topology represented in the model.

Figure 2 shows the graphical user interface (GUI) used to set up the most common workload and system parameters. When a entity from the local network sends a packet to the Internet, the firewall strips the source IP address from the packet and replaces it with the routers own Internet Valid IP. With TCP packets, the firewall/NAT router strips out the source port number (the port the destination will send the response on) with a random number it chooses. In addition, it adds the original source IP and port to a list that will associate them with the new port chosen by the router. Then the packet is sent on its way to the destination.

The entity on the Internet will receive this modified packet and will process the data and generally will generate a response packet. This response will be sent back to the source IP and port listed in the original packet. When this response is received by the firewall, it will look up who the original sender's IP and port is. Next, the firewall will replace the IP and Port in the destination section of the response packet, with the original sender credentials. And finally, it will send the modified response packet back to the original sender on the private local network.

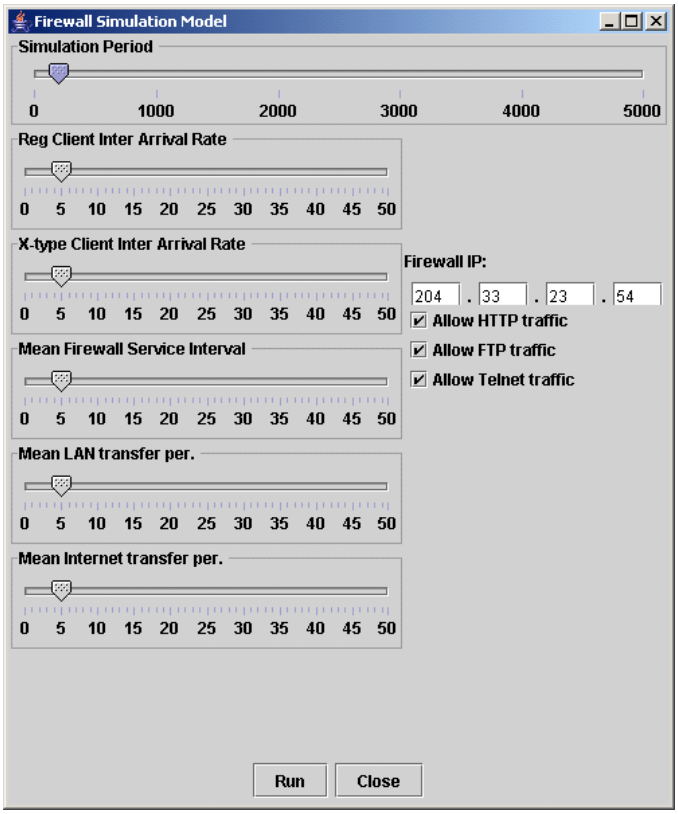

Figure 2. The main GUI of the firewall model.

Three types of packets are generated depending on the protocol indicated on the header of the packet: HTTP, Telnet, and FTP. Packets that indicate Telnet or FTP are blocked (dropped) by the firewall. Packets are generated at some specified rate, following an exponential probability distribution. Each packet spends some specific processing period at the firewall and at the server.

The simulation model uses several classes for active objects: FirewallTest, Firewall, LANclient, and InternetServer. The classes for the passive objects are: HTTPpacket, TelnetPacket, and FTPPacket.

The workload on the simulation run is defined by the following parameters:

1. Simulation period
2. Average packet generation rate
3. Average firewall processing period
4. Average server processing period

The other parameters are the IP addresses of: the local client machine, the firewall, and the server. The output of a simulation run has two parts: the trace and the summary statistics. The trace is the sequence of events ordered by time of occurrence. The summary statistics shows some performance metrics and other useful information. The following listing shows a small part of the out of a simulation run; only the last part is shown. The only performance metric shown is the total number of packets that were processed and the total number of packets that were blocked.

Client: FTP Packet15 created. Source 172.16.12.35:16344 Dest 66.235.137.4:21
Client: Firewall queue full? false
Client: Passed Packet15 to Firewall at 1541690.4068246891
Client: Dropped packet notification received from Firewall for Packet14 at 1541690.4068246891
Client: create a new packet at 1541690.4068246891
Firewall: Telnet protocol not open for routing. Packet dropped at 1541698.857580426.
Client: FTP Packet16 created. Source 172.16.12.35:28902 Dest 66.235.137.4:21
Client: Firewall queue full? false
Client: Passed Packet16 to Firewall at 3083386.513097668
Client: Dropped packet notification received from Firewall for Packet15 at 3083386.513097668
Client: create a new packet at 3083386.513097668
Firewall: Telnet protocol not open for routing. Packet dropped at 3083394.6079012966.
Simulation closing at: 4000000.25
End Simulation of Firewall Simulator, clock: 4000000.25
Total number of HTTP packets created: 48

Total number of Regular packets created: 48

Total number of packets serviced: 41

Total number of packets dropped: 12

CONCLUSION

Using simulation modeling provides a valuable and powerful approach that can be used to help teach different aspects of perimeter defense in network security. In this paper a simple model represents the basic behavior of a firewall setup to protect entities in a local network. Some of the performance metrics that are gathered from simulation runs are throughput, response time, and CPU utilization of the firewall. These metrics can also show under which conditions a bottleneck exits in the network.

The model discussed in one of several models that are under development in our department for the study of network security and that will be included in the corresponding courses. These models use object-oriented modeling, a good and

well-established approach to simulation that is used to study a wide variety of systems from small and simple to large and complex systems.

The Web page with free access to several of the simulation models mentioned is: http//science.kennesaw.edu/~jgarrido/psim.html

REFERENCES

[1] J. Banks, J. S. Carson, and B. Nelson. *Discrete-Event System Simulation*. Sec.Ed. Prentice Hall, Englewood Cliffs, NJ. 1996.

[1] J. M. Garrido. *Object-Oriented Discrete-Event Simulation with Java: A Practical Introduction*. Kluwer/Plenum Pub. NY 2001.

[2] J.H. Saunders. "Simulation Approaches in Information Security Education". *Proceedings of the Sixth national Colloquium for information Systems Security education*. Redmond. Washington. June 4-6, 2002.

[3] S. H. Seo and H. T. Cho. "Simulation of Network Security with Collaboration among IDS Models". *Australian Joint Conference on Artificial Intelligence*. Tasmania. September 4-6, 2001.

[4] S. Keshav. *An Engineering Approach to Computer Networking*. Addison-Wesley. Reading, Mass. 1997.

[5] J. F. Kurose and K. W. Ross. *Computer Networking*. Third Ed. Addison-Wesley/Pearson. 2005.

[7] C. Kaufman, R. Perlman, and M. Speciner. *Network Security*. Sec. Ed. Prentice Hall. Upper Saddle River, NJ. 2002.