Chapter 13
Firewall Rulebase Management: Tools and Techniques

Michael J. Chapple
University of Notre Dame, USA

Aaron Striegel
University of Notre Dame, USA

Charles R. Crowell
University of Notre Dame, USA

ABSTRACT

The network firewall serves as one of the foundational network components for modern day computer security. A key challenge with respect to firewalls is the on-going maintenance of the rules of the various firewall devices, namely how does one keep the firewall at maximum security effectiveness in the face of changing security threats and enterprise application needs? To that end, this chapter focuses on contributions in two key areas with respect to the practice of firewall rulebase management. First, the chapter presents a general model for the auditing and analysis of installed firewalls that ensures compliance with security policy requirements and technical specifications. Second, the chapter provides insight for the proactive identification of rules that possess a high likelihood of becoming orphaned in the future based upon their similarity to previously orphaned firewall rules.

INTRODUCTION

The introduction of the modern computer network has revolutionized how computing is used in the workplace. Whether it is through simple sharing files via common storage locations or accessing a wealth of information through both external Internet sources and internal intranet sources, the modern network has become a necessity for nearly all companies to deploy. Technology and application growth seem to continue unbounded raising the question of what the next technology will be after smart phones, Twitter, or social networking. Unfortunately, the very act of communication that opens up such a wealth of information serves as a double-edged sword, both allowing helpful, requested information to flow but also offering

DOI: 10.4018/978-1-60960-573-5.ch013

a new opportunity for malicious individuals to attack the digital enterprise environment.

In the enterprise security environment, the *firewall* serves as the front-line security device effectively delineating the perimeter between various zones of security control within the network of an organization. These *zones of control* can range from guarding sensitive data repositories such as a large database of personnel information to separating individual departments from one another to simply protecting the internal network from outside attacks originating in the Internet. Moreover, firewalls have become nearly ubiquitous with deployment levels approaching nearly 97% within modern enterprises (Richardson, 2007).

While other security tools such as virus scanners also enjoy similar deployment rates, the firewall is the de facto tool for enforcing network security. Analogous to the gate officer of old, firewalls operate as the network "traffic cop," determining which connections can start and stop and to whom communications can go or from whom they can be received. Due to the current and growing significance of firewalls in computer security for the enterprise, this chapter has the following goals.

- **Overview of firewalls and networking**: We begin with a brief overview of computer networks and describe the core approaches on how firewalls and the network interact. Particularly, we focus on the rules or logic of the firewall, i.e. how does the device decide what traffic may pass and how do the rules governing that activity emerge from company policy and / or history?
- **Discussion of rulebase management:** We continue with a discussion of the current state of affairs with respect to firewall rulebase management. Given that the enterprise and its applications are ever changing, what is the current state of the industry and most organizations with respect to keeping their firewall rule sets in peak running condition. What are the most common approaches to this task?
- **An important but neglected aspect of rulebase management:** We conclude the chapter with a case study regarding the notion of orphaned rules. We discuss why orphaned rules offer an excellent case study regarding the importance of proper organizational security leadership and we describe specific tools we have created to address this matter.

Overview of Firewalls and Networking

The foundation of the modern computer network rests on multiple layers of technology described by what is called the "Open System Interconnection" (OSI) model. This model involves several key layers including the *physical layer* (how devices are connected and communicate at the lowest level), the *network layer* (how to find a particular device), the *transport layer* (how data is split up for sending), and the *application layer* (the actual executable programs used). At the lowest physical layer, devices are typically connected to the network via wires through Ethernet (IEEE 802.3) or wirelessly through WiFi (IEEE 802.11). Switches connect computers in the wired case while access points (APs) implement wireless connectivity in the wireless case.

Conversely, the highest application layer represents the applications that are using the network. Common applications would include web browsers (Firefox, Internet Explorer, Safari), e-mail clients (Outlook, Thunderbird), and various communication-centric applications (Skype, Instant Messenger, etc.). Similarly, file sharing such as a roaming profile or network drive could also be viewed through the lens of the application layer. Communications across the network take place between a pair of applications in that