Chapter XIII
Design and Implementation of a Distributed Firewall

Dalila Boughaci
LRIA-USTHB, Algeria

Brahim Oubeka
LRIA-USTHB, Algeria

Abdelkader Aissiou
LRIA-USTHB, Algeria

Habiba Drias
LRIA-USTHB, Algeria

Belaid Benhamou
Technopôle de Château-Gombert, France

ABSTRACT

This chapter presents the design and the implementation of a decentralized firewall. The latter uses autonomous agents to coordinately control the traffic on the network. The proposed framework includes a set of controllers’ agents that ensure the packets filtering services, a proxy agent that plays a role of a proxy server and an identifier agent which is responsible for user authentication. The decentralization of the different agents’ activities is managed by an administrator agent which is a core point for launching the most important operations of the access control. A prototype has been designed and implemented. Furthermore, the authors hope that the underlying framework will inform researchers of a possible way to implement a decentralized firewall to improve the current solution, and will help readers understand the need for techniques and tools such as firewalls that are useful to protect their network traffic.

INTRODUCTION

A firewall is a software program or a hardware device operating as packet filters or an application level gateway. It permits to analyze the network traffic and allow or disallow the transfer of data on base of certain rules.

In a central firewall solution, all traffic from internal corporate network to the Internet and vice versa has to pass through the firewall. However, an increasing bandwidth causes problems to that solution.
Also, bottlenecks and potential vulnerabilities for the whole network communication may be caused by the central solution.

To improve the classical solution, some approaches have been proposed. Among them, we cite: the smart data servers to manage distributed personnel firewalls with a central tool proposed in Haffner, Roth, Heuer, Engel, and Meinel (2001). In Bellovin (1999) and Ioannidis, Keromytis, Bellovin, and Smith (2000), the authors propose a distributed firewall where IPsec is used to distribute credentials that express parts of the overall network policy. A prototype using KeyNote (Blaze, Feigenbaum, and Keromytis, 1999) trust management system is implemented in (Ioannidis et al., 2000). Al-Shaer and Hamed (2004) and Al-Shaer, Hamed, Boutaba, and Hasan (2005) propose a set of techniques to automatically discover policy anomalies in centralized and distributed firewalls, and recently, Wang, Behera, Wong, Helmer, Honavar, Miller, and Lutz (2006), Boughaci, Drias, Bendib, Bouznit, and Benhamou, (2006a), and Boughaci, Oubeka, Aissioui, and Benhamou (2006b) use agents to implement some security tools.

In the following, we will provide a possible way to implement a decentralized firewall by the use of autonomous agents.

The implementation of firewalls with agent technology is one of the new paradigms for the access control for computer systems. In this chapter, an agent-based firewall is proposed. It uses autonomous agents to coordinate the traffic on the network. The proposed system allows controllers and proxy agents to collaborate to provide a complete system permitting the distribution of the access control and the automation of the complex administration tasks. A prototype has been designed and implemented.

The utilization of agents in the domain of computer network security for the access control is justified by the fact that the cooperative work offered by agents can help firewalls to decrease the congestion by distributing the access control on different intelligent entities (agents) and automating the complex administration tasks.

The chapter is organized as follows. The following section gives some background on both firewalls and software agents. The third section describes our proposed firewall. Some implementation details are given in the fourth section. Finally, the fifth section concludes and gives some future works.

**BACKGROUND**

This section is intended to give the reader a basic understanding of traditional firewalls and software agents.

**Firewall**

A firewall is a security tool used to protect a computer network from unauthorized access. It may be a hardware device, a software program, or a combination of both (Brown, Davies, & Price, 1995; Mogul, Rashid, & Accetto, 1987).

The firewall is used mainly for controlling the traversal of packets across the boundaries of the computer network based on a specific security policy defined by the network administrator. However, the configuration of the firewall requires a considerable understanding of network protocols and of computer security. A small mistake can make the security of the network in a danger.

**Types of Firewalls**

There are two main categories of firewalls: network layer firewalls and application firewalls.

- **Network layer firewall** called also packet filter that operates as IP-packet filter. It allows or disallows the transfer of data on base of certain rules defined by the firewall administrator. It can filter the network traffic based on many packet attributes like: the source IP address, the source port, the destination IP address, the destination port, the protocol type (TCP/UDP), and also the destination service, like www or FTP.
- **Application firewall or proxy** that can be viewed as a relay that sits between a client application and a real server. It is used to filter all requests entering and leaving the network. It can also hide the true network addresses of protected hosts.

**Firewall Implementations**

Firewall can be implemented in both hardware and software, or a combination of the two. In the following, we cite some existing firewall implementations taken from the free encyclopedia Wikipedia at the Web site http://en.wikipedia.org/wiki/Firewall_(networking).