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.
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 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).