Firewalls Essay, Research Paper

The term firewall has seen limited use since the late 1980s to describe a device to block unwanted network traffic while allowing other traffic to pass. The first published description of a “modern” firewall including use of that name was in ‘Practical Unix Security’ written in 1990 and published in 1991. The first description of a firewall, although not by that name, was also in 1990, in a paper by Bill Cheswick. A few of the industry pioneers tried to track down the origin of the word as described in this context. They found several references from the mid-80’s that used the word to describe a damage-limiting device. The earliest use they found that seems to correspond to a security device was by Steve Bellovin, in some email to Phil Karn, in 1987. But the context suggests that Phil knew what Steve meant, yet Steve doesn’t think he invented it.

What is a network firewall? A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one that exists to block traffic, and the other that exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy.

The Internet, like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people’s walls with spray paint, tearing their mailboxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect. Usually, a firewall’s purpose is to keep the jerks out of one s network while still letting one get his or her job done. Many traditional-style corporations and data centers have computing security policies and practices that must be adhered to. In a case where a company’s policies dictate how data must be protected, a firewall is very important, since it is the embodiment of the corporate policy. Frequently, the hardest part of hooking to the Internet, if you’re a large company, is not justifying the expense or effort, but convincing management that it’s safe to do so. A firewall provides not only real security – it often plays an important role as a security blanket for management. Lastly, a firewall can act as your corporate “ambassador” to the Internet. Many corporations use their firewall systems as a place to store public information about corporate products and services, files to download, bug fixes, and so forth.