

Are Open Source Firewalls Enterprise Class

It has been almost 5 years now when a project based on the concept to make Linux a big name in the northern part of India was initiated by leading experts who had a well conversation and great convincing skill to make people bound to this phenomenon. This was started in 2000 and since then has been facing continuous competition and challenges by many well-known organizations like IBM, Novell, etc. upcoming into this. The motive of the people involved in this project was to divert more and more users towards the Linux operating system such that this remains a "home user" for them and this was made possible through talks at events like universities festivals, seminars, etc.

Today, Open Source Software has gained peoples' confidence in almost all small servers functioning as e-mail servers, web servers, domain name servers and firewalls which has in turn made the presence of it in all local universities, small businesses and in departments within large corporations. The most probable reason for this is the Internet service built into Unix-based operating systems. According to I.D.C., 78% of fortune 500 companies already use Linux. These companies are opting Linux as in Linux you do what needs to be done and does it faster, more reliably and less expensively than other platforms. A Linux based server integrates seamlessly into a preexisting MS, Novell or AppleTalk based network as it appears as "just another server" to the end user. From firewalls to advanced file servers, there is an alternative available whether you're a small business or an enterprise

Needless to say but to describe all the well-known Open source softwares under one heading is beyond the scope of this article so, firstly, the most often used Open Source Firewalls would be taken into account, which plays a definitive role in all daily activities of most organizations.

In the absence of any central point of security in the network, there arises a need to develop and create a check point on top of every system, every in-built network which are directly connected to the internet, in order to avoid any interference and prevent any intruders coming into your network. This is made feasible by Firewall. So, by now, it must have now become quite easy to understand what firewall is. A firewall is a system or group of systems that enforces an access control policy between two networks. In simple words, it comprises of two-way system: one exists to block traffic, and the other permits traffic.

The firewalls act as border security force at the verge of any private network and its connection to the internet. Once properly configured, it checks almost every protocol passed through the user to the internet and only when the protocol matches with its policy rules then only it is passed otherwise it is dropped out by it. The advantage of this is that it does not have any serious bugs that can harm your network.

Now, if the firewalls are so important than the question arises are Firewalls OS dependent that is Unix firewalls for Unix-based networks and NT firewalls for Windows NT-based networks? It is to clarify here that this is a common misconception among network administrators that a firewall has to be based on the same operating system as the network servers. These days, most firewalls come as pre-configured computers running a completely proprietary operating system. This is the very reason that now a days majority of firewalls are comprises of LINUX, which give added advantage of open source with the same operational features.

Let us have a look at the different categories of firewalls and differentiate them on the basis of their normal characteristics, which would eventually help to select any particular of them to be functional:

Security Features: The features of virtual private networking (VPN) and encrypted authentication are served by many firewalls but this is a much costly affair, which requires the purchase of an additional license.

Enterprise Functionality: There are firewalls that use a centrally maintained security policy that is replicated among all firewalls in the enterprise.

Security: Another feature that makes the firewall distinct is the security they provide. Some firewall products are fundamentally flawed because they rely too heavily on the host operating system because either they contain bugs that can be exploited or there is a flaw in the authentication protocol used for remote authentication.

Interface: The configuration of firewall is another parameter to classify them. Some firewalls are very difficult to configure because they either require administration through Telnet or very complicated command-line interface. Others, which require graphic interfaces, can be very easily configured.

Service Features: Firewalls that include services, such as FTP, Telnet, HTTP, etc. are very convenient in a way but their obsolete functionality makes them complicated enough on the other hand. This in turn reduces the security they provide. But many hackers can easily reveal these firewalls.

So the primary requirement of any firewall is its ability to provide security and this is possible only when it is properly configured. The secondary function of firewalls is the ease of use. Flashy features, performance, and services galore are tertiary considerations which comes much after the above two and for the interest of all the network administrator and decision makers the point which arises is Open source provides both the features with maximum satisfaction.

As we all know that firewalls are nothing but the gateways for all computers working on LAN. It mediates the communication as well as facilitates the execution of all functions operating through LAN. The comparison of open source firewalls with the commercial ones, which we have dealt earlier, was very interesting and exciting. Those are rather all facts and are not misleading or false in any way. This section would deal with some more technical aspects of the firewalls, which again are based on facts.

The two well-known types of network decide the complexity of firewalls. The first one is a stateless firewalling where the server responds to a request irrespective of the earlier request made. This is in contrast to a stateful firewalling where a great deal of network activity is session-based. The latter one is quite complex and this applies to VPN access, extended database transaction, more complicated web interaction like online purchase etc.

The well-known standard Linux distributions utilize firewall codes since a long time. **Alan Cox** ported BSD's ipfw firewall tool to Linux with the 1.1 version of the Linux kernel, and this has been augmented with ipfwadm, a more feature-rich extension of ipfw, and more recently by IPchains. The working of IPchains is made feasible with a set of configuration files called IPtables, which define the set of filtering rules and the conditions in which these can operate. This

is also accompanied by a set of commands for manipulating these tables. These rules can be based on allowable originating and destination hosts, ports, packet header information, or any combination of these. With these sets, firewalls examine each packet in isolation and determine whether it should be allowed or not. So, a Linux firewall turns off unused or unwanted ports, and listens to network ports designated by the system administrator configuring the firewall. This explanation clearly illustrates the statelessness of the working of firewalls. Though the statelessness working of firewalls is very simple and secure and still it has certain limitations in its functionality.

The higher level of functionality required by VPN access to applications on the company intranet is facilitated by the firewalls code in Linux. This code is based on netfilter, a set of loadable kernel modules that extends Linux's firewalling capabilities to allow session-based packet examination. This greatly increases the performance and the advantage of using kernel module is that when a new functionality is required it can be added on a module-by-module basis without disturbing the original kernel.

The most important point that gives the upper hand to the non-Linux firewall is the "Total Cost of Ownership" (TCO) for the Linux firewall. Whenever we talk about Linux it is always accompanied by the fact that it is acceptable majorly due to the factor TCO but we want to explore how and why? In the case of firewalls, the Linux firewalls follows the IPtables and IPchains for its functionalities and the basic core for all the development remains the same irrespective of the brands available in the market, which is not the case with the non-Linux firewalls which are with its own core. This feature plays an important role in the TCO as once you are familiar with the any Linux firewall you can easily administrate any network with any Linux based firewa ll.

The limitations in evaluating open source software are not that the number of options is limited rather there are unlimited numbers of options which itself becomes a limitation. The choice of a package right for your organization depends on the option that whether you want your own or deploy an out of the box configuration. The former one is more expensive since it requires a great investment for resources and on IT staff but the latter one is very much less expensive in terms of expenditure spent on having limited staff and less number of other commitments.

As an IT decision-maker, in this competitive technical savvy environment, you increasingly have to consider Linux alternatives. The more specific your organization needs, the more likely it is that you'll need a commercial product or one built by your own IT staff. The more your problem has in common with problems faced by other IT departments, the more likely it is that a freely available open source solution will work for you that's why more and more organization are looking towards the Linux products.