Choosing the right firewall platform.

VisNetic Firewall

comphrehensive intrusion protection

Budget, Value, Requirements

Abstract

This paper describes the factors that must be considered when selecting a firewall platform.

Firewall Platforms

Firewall solutions are available on a number of platforms and can generally be segregated into three groups: Hardware-based products and software-based products on Linux/Unix or Windows. For some environments, a hardware-based firewall is a great choice. For others, nothing beats a Linux- or Unix-based firewall and for a great many, a Windows-based firewall is the best choice.

Selection Criteria

Organizations looking to deploy a firewall are trying to solve a security problem. If they are organized in their effort, they have established a "Security Policy", or description of permissible activities using company computers and network(s). A firewall is an important component of the organization's security infrastructure that will enable enforcement of that policy.

Additional selection criteria, beyond the needs specified in your "Security Policy", include:

1) **Budget**: the cost of the firewall and its maintenance must be within the company's means.
2) **Value**: the cost should also be in line with the assets it is there to protect - you won't spend $100,000 to protect information worth $100,000.
3) **Requirements**: The degree of technical expertise held by your firewall administrator will influence your firewall choice.

Each of the three types of firewalls can be compared according to these criteria.

Platform Comparison

Hardware-based Firewalls

These are single-purpose systems. Required hardware and software are

bundled in one easily installed package. Usually, hardware solutions run on a stripped down version of Unix or Linux, where all of the unnecessary Operating System components are removed. The benefits of this model are that they are fast, relatively inexpensive, and don't require the loading of the software. This makes them strong on **Budget** and **Requirements**, but hidden costs often reduce the **Value** of this solution.

Products that cannot be distributed electronically can be difficult to upgrade, and consequently less flexible and scalable. As your needs change, the capabilities of this solution may not keep pace. At a minimum, the time required to update your firewall configuration results in a delay between need and solution implementation. Finally, these solutions require another machine or directory to store and analyze the logs.

Linux/Unix Firewalls

These are software products running on one of the many distributions of Linux or Unix. In some cases, the Operating System is included in the firewall product, requiring a single install on one low-cost computer. In most cases a standard PC will suffice. Linux and Unix are often praised as more effective Operating Systems than Windows. They are typically stripped down to "the bare bones", removing any risk presented by unneeded services.

The most compelling reason to make this choice is **Budget**. Linux and some versions of Unix are available free of charge. However, while the cost of this Operating System is minimal, the expense required to employ its administrator is comparatively high, increasing the **Requirements** for this choice and reducing its overall **Value**.

Windows-based Firewalls

These are software products running on a Windows-based Operating System. The primary benefit of a Windows-based firewall is its low cost. It too runs on an inexpensive PC. Additionally, high quality Windows-based firewalls are available in a wide range of prices, making this choice an easier fit to your **Budget**.

Windows is the most widely known family of Operating Systems. So it is likely that your firewall administrator will know how to use it. This familiarity reduces the **Requirements** and increases the **Value** of this platform.

Refuting Windows Critics

Measuring "total cost of ownership", Windows-based firewall solutions are the most economical. But are they effective?

Do Windows-based Firewalls work?

Given security-related bugs identified in Windows Operating Systems and in Microsoft applications, some industry commentators have concluded that the platform is easily hacked and consequently unstable. On closer examination however, this conclusion proves largely unsubstantiated.

In terms of security, there are three main criticisms with Windows:

1) Security-related bugs have been found in Windows.
2) Security-related bugs have been found in Windows applications.
3) Windows is not a stable enough platform for a firewall.

Addressing the issues in order, there is a long history of security-related bugs being found in Windows Operating Systems. Of course the same can be said for Linux, Unix and any other Operating System connected to the Internet. Should this stop you from choosing either one? Not at all. On all platforms, it is the firewall software that envelops the Operating System, inspecting the data packets before passing them along. The firewall protects not only the network, but the platform on which it runs.

When Windows is "hardened" (removing unnecessary services and configuring for maximum security), most of the known security issues are addressed. When the system has a firewall installed, only the communications allowed by the firewall reach the Operating System, further protecting the system. If a hacker tries to exploit a weakness in Windows, the firewall blocks the attempt. The security of the platform is no longer measured by the Operating System, but by the firewall that surrounds it.

The second concern surrounding bugs identified in Windows applications is also easily negated. A firewall should not have any applications installed that are not required for the task of firewalling. With all these applications removed, the security risks they present are also removed.

The third concern is stability. Linux and Unix users have long championed their platforms as the #1 choice if you are looking to achieve the "five 9s"--99.999% availability. Meaning a downtime of no more than 6 seconds per week or 5 minutes per year.

Five 9s is the target for mission-critical services and, if this is a

requirement, Windows will be hard-pressed to achieve it. However, it can still do very well. Most causes of instability in Windows are attributable to buggy applications, not in the Operating System itself. Windows NT, Windows 2000 and particularly Windows XP are clearly superior to Windows 95, 98 and Me, which were developed to support older software dating back to DOS (Disk Operating System). Therefore, Windows NT and 2000 are the platforms of choice for most Windows-based firewalls. Uptime is better than 99.9% and is easily achievable. That is only 10 minutes of downtime a week.

Yes, they do.

The following criteria combine to make Windows-based firewall solutions the superior choice:

- Low Budget
- High Value
- Minimal Requirements
- Built on a secure and stable platform

VisNetic Firewall – A Windows-based Firewall

VisNetic Firewall protects the Operating System by preventing access to any running service that is not allowed by the administrator. What sets VisNetic Firewall apart from other Windows-based firewalls is its ability to solve for a known Operating System weakness that cannot be hidden. **Sequence Number Hardening** is a feature that prevents hackers from spoofing TCP connections.

TCP Sequence Numbers are used to keep track of the order of data that is sent in a TCP/IP connection. Without a sequence number, data packets would be returned in no particular order, and the resulting page or document would likely appear garbled. While the concept of numbering packets is simple, the Initial Sequence Number (ISN) must be chosen carefully to avoid possible confusion with data from other connections. As a result, the developers who implemented the TCP protocol for different Operating Systems chose their ISNs a little differently. While this is not a problem for normal connections, hackers are still able to exploit the non-random nature of ISNs.

VisNetic Firewall corrects for this weakness. It replaces the Sequence

VisNetic Firewall Features

Numbers in all TCP packets, making them less 'guessable'.

Additional features of VisNetic Firewall include:

- **Stateful Inspection**
  Stateful inspection delivers firewall protection beyond pure packet filtering. Rather than simply verifying the packet source and destination, Stateful Inspection ensures the legitimacy of the packet by matching its presence to an actual request. For example, rather than accepting all ping replies, VisNetic Firewall will permit a ping response only following a confirmed ping request. This example is pertinent because certain DoS (Denial of Service) Attacks can initiate with an unending stream of ping responses to overwhelm and crash a server. Without Stateful Inspection, this attack would be undetected and unblocked.

- **SYN Flood Protection**
  A SYN flood is a large number of valid-looking connection attempts that can overwhelm a server and prevent it from being able to accept connections from legitimate users. VisNetic Firewall recognizes when a SYN flood occurs and prevents it from interrupting normal server operation. When the SYN flood is detected, a log message is generated and "SYN cookies" are used so that valid connections can be made and SYN flood connection attempts are ignored. Once the SYN flood ends, SYN cookies are no longer used.

- **Separate Filtering and Rules Per Device**
  VisNetic Firewall allows filtering to be enabled or disabled per device. Examples of a device include an internal network interface card (NIC), an external NIC linked to a cable modem connecting to the Internet, or a Dial-Up Adapter used to connect to an ISP (Internet Service Provider). If filtering is enabled, unique rules established for each device control the data permitted to pass through the firewall. If filtering is disabled on a given device, the firewall will not filter any traffic traveling through said device. Based on how a particular device is used and the security it requires, the need for filtering and rules may be customized to route or deny packets appropriately through that device, without affecting other devices. VisNetic Firewall not only guards the network from unknown threats, but also preserves access for trusted sources.

Contact Information

Author

James Grant is the lead developer of VisNetic Firewall and co-founder of 8Signs. Founded in 2001 and based in Saratoga California, 8Signs is a collaboration of industry leaders experienced in firewall technology, development, and marketing.

Contact

Deerfield Communications, Inc.

PO Box 851

Gaylord, MI 49735

USA

Telephone 989.732.8856

Fax 989.731.9299

www.deerfield.com

sales@deerfield.com
feedback@deerfield.com