



Top Ten Things About Spam Firewalls

Using a spam firewall to block spam is the most advantageous and efficient way for an organization to keep unsolicited email from reaching the network, server, and end user inboxes. Spam firewalls offload spam filtering from the email server, increase server bandwidth and free up network resources. Spam firewall appliances typically come pre-configured, are setup in minutes, and can be maintained with little effort.

This paper helps IT personnel better understand the power of a spam firewall and how such a solution can work in their organization. Further, this paper clarifies some of the misconceptions regarding what a spam firewall is and is not capable of doing.

What is a spam firewall?

A spam firewall is a single box computing appliance that is set up in front of the email server. This appliance receives all the incoming email for the organization and processes it such that only the good email is passed on to the email server. A spam firewall is normally built on a hardened operating system based on Linux or BSD. However, some vendors do make solutions based on other operating systems. The appliance format and the hardened operating system make the spam firewall less susceptible to hackers and other threats. A proper spam firewall protects the email server from all forms of attack in addition to filtering spam.

What does a spam firewall do?

At the most basic level, a spam firewall blocks unwanted email from entering the network and reaching the email server. This is accomplished using a multi-layered filtering solution. Some spam firewalls use only a single technology for eliminating spam. However, this is not preferred since spammers find it easier to work around a single technology.

What does a spam firewall not do?

In most cases spam firewalls are designed to block inbound spam. Spam firewalls do not act as corporate stronghold to the network itself and should not take the place of a standard Internet firewall. An Internet firewall is set up to limit access to the network via the many protocols that can be used to attack an organization. A spam firewall only defends against attacks on SMTP (Simple Mail Transfer Protocol) port 25. Furthermore, a spam firewall is not an SMTP relay. It is designed only to protect the email server. If it has multiple functions, such as operating as an outbound relay, it may compromise the security it provides to the email server. For example, traditional firewalls very rarely function as routers; to do so would compromise their ability to act as a firewall.

How important is virus scanning?

Most spam firewalls incorporate virus scanning technology to limit spam generated by viruses as well as protect the email server. The Barracuda Spam Firewall provides this functionality as part of the standard solution, using two different virus check systems, both of which are updated hourly with new virus definitions via the Barracuda Energize Update service. This ensures that viruses, which often breakout with little to no warning, are blocked without disruption to regular email service. Virus scanning is very important for protecting the email server from overload. Many virus outbreaks will crash email servers. However, with virus protection incorporated within the spam firewall, these crashes do not happen. Sometimes virus scanning is available as an option, meaning the customer incurs additional costs if they choose to add such functionality. Virus protection is highly recommended.

How is a spam firewall installed?

A spam firewall is typically housed within the DMZ, between the Internet router and the corporate email server. There are several different ways in which a spam firewall can be installed and deployed depending on the needs of the organization. Standard deployment involves simply connecting the spam firewall to the corporate network by assigning it a new IP (Internet Protocol) address. Once the IP is configured the corporate MX records are adjusted to point to the new IP of the spam firewall. The Barracuda Spam Firewall comes pre-configured and begins operating with no additional adjustments. The web interface can be used to further tune or enable additional features. The Barracuda Spam Firewall can also be used to service multiple email servers in one or multiple locations.

How is a spam firewall maintained?

Unlike software solutions, which require corporate IT staff to manually maintain the operating system of the computer that runs the software, a spam firewall is maintenance free. All security updates as well as spam and virus definitions are automatically applied without any IT staff time. For instance, Barracuda Spam Firewall customers can rely on the Barracuda Energize Update service to ensure that hourly updates are made to the firewall's spam and virus definitions. These updates are made automatically with no additional effort required from the user and without disruption to the email service. The only impact on system performance is greater worker productivity.

Many organizations prefer spam firewalls over other solutions because of its central management capabilities. A spam firewall is easily managed from a central location within the organization, whereas third-party spam filtering services and software solutions often rely on remote management, which may pose additional security and liability risks to the organization. The Barracuda Spam Firewall allows access only to authorized users within the organization. All email that passes through the box is secure.

What type of organizations use a spam firewall?

Any organization that operates its own email server can benefit from a spam firewall. Barracuda Networks customers range from small to medium businesses, to large enterprises and ISPs. The ease of deployment and low cost of the Barracuda Spam Firewall make it especially attractive to customers who do not have extensive IT staff or have a very busy IT staff. Large enterprises and ISPs use the Barracuda Spam Firewall for ease of deployment as well as for its ability to seamlessly integrate with other security applications that the organization may already have in place.

How does a spam firewall work?

To filter spam, a spam firewall uses many different techniques. For instance, the Barracuda Spam Firewall employs ten defense layers through which each email must pass in order to make it to the end user's inbox. These defense layers include: denial of service and security protection, IP block list, rate control, virus check with archive decompression, proprietary virus check, user specified rules, spam fingerprint check, final purpose analysis, spam rule-based scoring, and Bayesian analysis. All of these layers provide protection against different types of spam and other attacks.

Why is the Barracuda Spam Firewall so fairly priced?

The pervasiveness of spam throughout all business communication means that implementing a trusted spam solution is no longer a precaution, it is a necessity for all organizations that rely on email as an effective business communications tool. Despite this, the price for many popular spam solutions remains at a premium that many organizations cannot afford. Many vendors determine pricing based on the number of users in an organization. This per-user pricing model can be constricting for businesses looking to expand. As the number of users increases, the price for maintaining the spam solution can quickly spiral out of control.

Barracuda Networks recognizes the need for an effective spam and virus solution that is both cost effective and easy to deploy for any organization. It developed a fair pricing structure that does not involve per-user fees. Such a structure allows organizations to purchase a Barracuda Spam Firewall knowing that the price they pay up front will handle the number of users they currently service as well as provide for additional users without added cost. Barracuda Networks achieved this fair pricing model by developing an optimized hardware architecture using ten defense layers. These layers are sequentially organized such that the low CPU processing layers are first. This allows Barracuda Networks to use lower cost, more effective hardware in its spam firewall design. Additionally, Barracuda Networks has developed a build-to-order system, similar to Dell Computer, for its manufacturing and order processing. This minimizes inventory and overhead, which delivers lower cost for the customer.

What are the benefits to using open source technologies?

Barracuda Networks and other vendors use some open source components, such as Linux OS, in their spam firewall solutions. One of the open source technologies that Barracuda Networks uses within its ten defense layers is SpamAssassin, an open source rules-based spam filter. There are several benefits to using open source technologies in the development of a spam firewall. Open source solutions provide greater flexibility compared to proprietary solutions. Typically a large number of programmers have contributed to the development. Therefore, commercial solutions that use open source technologies can provide a more robust and durable product offering to their customers.



Barracuda Networks

10040 Bubb Road

Cupertino, CA 95014

+1 408 . 342 . 5400

+1 888 . 268 . 4772

www.barracudanetworks.com

info@barracudanetworks.com