

FEATURE

WHAT FIREWALL DO AND WHAT FIREWALLS DON'T DO

By Ian Kilpatrick, chairman Wick Hill Group, specialists in secure IT infrastructure systems

861 words; December 07

Introduction

Over the last few years, security threats to companies have grown and altered dramatically and so have the defences. Traditional firewalls, installed over three years ago, are often not best suited for current threats and don't protect against a number of newer threats.

What Firewalls Do

A firewall is a system designed to prevent unauthorised access to or from a private computer network. Firewalls are frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet (often described as intranets). All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

You need a firewall to protect your confidential information from those not authorised to access it and to protect against malicious users and accidents that originate outside your network. One of the most important elements of a firewall is its access control features, which distinguish between good and bad traffic.

There are various types of firewall. In ascending order, they are

* **Packet layer**

This analyses network traffic at the transport protocol layer.

* **Circuit level**

This validates that packets are either connection or data packets.

* **Application layer**

This ensures valid data at the application level before connecting.

* **Proxy server**

This intercepts all messages entering or leaving the network.

In the real world, threats have evolved over the years and firewalls have evolved to deal with them. While it is still possible to buy packet only firewalls, they are not adequate for business use. Protection against combination threats is best provided by firewalls which combine all of the above elements.

Specific functions performed by firewalls include:

- * Gateway defence
- * Carrying out defined security policies
- * Segregating activity between your trusted network, the Internet and your DMZ (a protected zone midway between your network and the Internet, where you would perhaps have your web or email server).
- * Hiding and protecting your internal network addresses (NAT)
- * Reporting on threats and activity.

What Firewalls Don't Do

Even with a firewall, there are still many areas of risk for your network. The most obvious is malware. Malware is a combination of the words 'malicious' and 'software' and includes viruses, trojan horses, worms, spyware/adware, phishing and pharming. Malware is most commonly acquired through clicking on email attachments and email links.

Viruses, trojans and worms can cause a range of symptoms from the annoying and/or embarrassing to the much more serious which can affect the functioning of your business. Spyware/adware gathers information about you. It can record keystrokes and, as such, can potentially be very dangerous, revealing everything you do on your computer,

Another well-known threat, not covered by your firewall, is SPAM. Dealing with SPAM can seriously affect your productivity and, as SPAM often contains viruses and phishing emails, it is also a direct security threat.

Phishing is about fake emails trying to extract sensitive information, such as your bank passwords or credit card details and a variation of this is pharming, where the criminal sets up a fake web site which looks like one you normally use, typically a banking site. Once you enter your details, the criminal is able to plunder your account.

Many people are also unaware that you can actually acquire malware by simply browsing web sites. This is a rapidly growing threat and some of the malware is used to create Botnets (see below). Some security applications (e.g. those from Finjan) have a facility which protects you against web sites containing malware, by checking the sites before you click on them.

Another danger to your network is from a DDoS (distributed denial of service) attack. This is a malicious attempt to prevent an organisation being able to use its Internet based systems by flooding them with emails until the servers are overwhelmed. These attacks are often carried out by BotNet networks of compromised PCs, which are also used in SPAM campaigns. Specific DDoS software can guard against this threat.

Other dangers to your network include unauthorised access, and the way to deal with this is to have proper authentication procedures in place, for both local and remote access. In many cases, passwords are not enough and the use of strong authentication with tokens provides much better security.

