

## FEATURE

### WHAT FIREWALLS DO AND WHAT FIREWALLS DON'T

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

#### 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.

Further potential problems are from data theft or leakage, for example when a laptop is stolen. The answer here is to encrypt all sensitive data. Finally all wireless use is risky and requires a specific wireless firewall, and wireless VPN for remote access.

## Conclusion

A firewall is no longer enough to protect a company network. Other security solutions to combat the threats outlined above are also necessary, as well as proper staff training.

One of the best ways to protect against the main threats not covered by a firewall is to use a UTM (unified threat management) device. UTM devices are multi-purpose security solutions which have a minimum of a firewall, VPN, anti-virus and intrusion detection/prevention. Some UTMs also incorporate capabilities such as web filtering (blocking problematic web sites), SPAM blocking and spyware protection. UTMs are available from IT security companies such as WatchGuard and Check Point.

## ENDS

### Bio - Ian Kilpatrick

Ian Kilpatrick is chairman of Wick Hill Group plc, specialists in secure infrastructure solutions. Kilpatrick has been involved with the Group for more than 30 years and is the moving force behind its dynamic growth. Wick Hill is an international organisation supplying most of the Time Top 1000 companies through a network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are key factors in IT. He has had numerous articles published in the UK and overseas press, as well as being a regular speaker at IT exhibitions.

### About Wick Hill

Established in 1976, VAD (value added distributor) Wick Hill specialises in secure IT infrastructure solutions. The company's portfolio covers security, performance, access, services and management. Wick Hill sources and delivers best-of-breed, easy-to-use solutions through its channel partners, providing customer support, implementation, training and technical services.

Wick Hill is exhibiting at Infosecurity Europe 2008, Europe's number one dedicated Information security event. Now in its 13th year, the show continues to provide an unrivalled education programme, new products & services, over 300 exhibitors and 11,700 visitors from every segment of the industry. Held on the 22nd - 24th April 2008 in the Grand Hall, Olympia, this is a must attend event for all professionals involved in Information Security. [www.infosec.co.uk](http://www.infosec.co.uk)