



Shutting out new attacks

Corporate network security has never been more crucial, meaning that the firewall / VPN solution has had to evolve rapidly. Nick Booth takes a look at some strategic measures enterprises might like to evaluate.

These days everyone seems to think they're a security expert, thanks to the publicity given to worm viruses like Sasser and MSBlaster. Sadly, this increased awareness doesn't make the IT manager's job any easier, as end users think they know enough about security to assume a firewall and a VPN offer complete protection.

One challenge for the IT department then, is to alert users that they really should do more to protect themselves, because nobody can provide complete protection. Let them know you're in an arms race against a growing range of threats, that's expanded from hackers and virus writers to include an increasing number of organised criminals.

Firewalls, VPNs and anti-virus software have always needed the co-operation of the end user. Once you've convinced end users of their new responsibilities, you may buy yourself some time to investigate the new generations of systems that you'll need to complement your existing foundations.

Not that there's anything too much wrong with the foundations of traditional firewalls and VPNs. OK, virtual private networks were always a bit clunky and fiddly to install. They could also be a nightmare to manage – but they did the job.

The same goes for firewalls. The only reason many of them got bypassed was that many people assumed that installing a firewall was enough, without realising that they needed to fully configure it.

Many hackers know the standard settings of a firewall and can bypass them. As long as every firewall is configured properly on installation, it can become a strong barrier to entry into any network.

But nothing ever stays the same in IT and the ground has shifted in two very important areas.

Firstly, the arms race continues. The malevolent forces of hackers and crackers will continue to dedicate themselves to finding vulnerabilities in the armoury of any new security system, be it a boxed product,

software, or the integrated defences of a corporate. For any one person dedicated to securing company assets, there are usually between 100 and 1000 hackers, criminals or disgruntled end-users trying to outwit them at any one time.

Corporations changing shape

If that wasn't bad enough, the nature of most corporations is changing too. Ollie Ross, head of research for the Corporate IT Forum (tif), the UK's association for users of IT, says the changing shape of most companies will create more chinks in their armour for hackers to exploit.

"Companies are talking about layering, or network de-perimeterisation, which will be a major challenge for everyone," says Ross. "The question is how do you maintain security in an environment when a company needs to be more fluid and flexible?"

The old rigid format, in which firewalls excelled, was great for security, but doesn't work today. "The hardened perimeter model was useless and unsustainable. The only way corporates work

Don't listen to those critics who say virtual private networks are doomed technology either. They're more sophisticated now, and certainly have a part to play too.

"VPNs are valuable in providing a secure remote connection to the network, but their deployment needs to be carefully considered and managed," says May.

"You need to treat remote workstations in the same way as you'd treat office-based machines, applying patches to keep applications secure, then a firewall, updating anti-virus software and carrying out regular software audits."

Token-based access control, where a physical token such as a USB key or a device which generates single use passwords, can help prevent unauthorised use of a VPN connection.

Similarly, some vendors like Neoteris, now part of Juniper Networks, differentiate themselves by providing secure socket layer (SSL) VPNs, which has a standard client that is present on every computer – the web browser. This has made it easier to set up users,

“VPNs are valuable in providing a secure remote connection to the network, but their deployment needs to be carefully considered and managed”

effectively today is with a totally open network," says Ross.

So what should network managers do?

There needs to be less reliance on appliances, says Robert May, md of RAMSAC, a security service supplier, since you can cover every area of vulnerability with a piece of hardware. Software-based security solutions are more fluid.

"Firewalls aren't a complete security solution in a box, they will only protect against specific threats. Organisations need to have a complete security plan which identifies each threat, and how it will be countered."

while still enabling the IT department to ensure each user has a secure connection to the corporate network.

Internet service providers such as AltoHiway and Tiscali have alternative solutions.

If AltoHiway is to be believed, the future is in Private Branch Networks (PBNs) which restrict company information to travelling over a private network (provided by the ISP).

"Companies should not trust any business-critical information to travel over the internet these days," advises Dave Mullender, AltoHiway's chief technical officer.



Managing security yourself

You don't have to go to a service provider for your security – you can manage it yourself, argues Mik Stevens, solutions evangelist for Check Point.

Firewalls and VPNs are the foundation, which CheckPoint has always provided. Like most vendors, they've worked to make them more potent yet easier to manage. Meanwhile, hackers have moved on.

More than half of the most prolific attacks on the internet exploit weaknesses in applications, according to analysis from research company IDC, so Checkpoint and the other vendors have had to develop security to combat this new threat – a firewall these days must be able to identify and protect against specific application attacks.

"Check Point is looking to the expanding use of web applications," says Stevens. "We are also greatly expanding our client-side deployment capabilities." This is why Check Point bought endpoint security vendor Zone Labs earlier this year.

Good foundation

Firewalls and VPNs have always been a good foundation, and the good news is that their scope is extending to combat the new threats being dreamt up by



● **MIK STEVENS OF SECURITY VENDOR CHECK POINT: Protecting against application attacks**

hackers. The bad news is that both VPNs – and to some extent firewalls – can be so difficult to manage they demand too much time and money in maintaining them.

Service providers, like Mitech, Tiscali and AltoHiway, are moving in to fill this gap, by providing the option of managing your security for you.

Which is why Checkpoint and all the leading security vendors are working to make management and deployment easier. It's important to have the right products, but effective, efficient management is essential.

Ease of use and the ability to secure mission-critical applications will be essential for network managers in the coming year. 