



Technology briefing

Think inside the box

The trend for 'security in the one box' has not stopped at UTM. Welcome to the wonders of XTM and SBA. By **Mark Mayne**

The "security in the one box" industry is developing rapidly. Rather than purchasing separate solutions from separate vendors, there are obvious efficiencies in having everything in the one place – an architecture called "unified threat management", or UTM.

The term UTM was coined by IDC in 2004, when it described this technology as an "integrated network appliance that performs firewall, gateway anti-virus and intrusion detection/prevention services".

The UTM concept covers a wide spectrum of security products, but the main UTM architecture combines a firewall, anti-virus and anti-spyware.

Until recently, UTM devices had not added features such as SSL VPN, IM, peer-to-peer and VoIP, but over the past year that has started to change – as have the attitudes of those who are considering purchasing a UTM architecture.

Threats are more sophisticated, leaving enterprise and SMB networks open to targeted attacks, which include blended security threats, such as phishing emails, VoIP exploits and drive-by downloads.

This is prompting UTM device vendors such as Fortinet, WatchGuard and Check Point to introduce the next generation of threat-management devices – "extensible threat management" (XTM) – to counter them. The XTM architecture takes UTM technology one step further by offering flexibility: user-advanced, application-aware technologies, supporting a multitude of network architectures.

Check Point has gone even further along this road by announcing last month that it believes the future is in "software

blade architecture" (SBA) – of which more later. For now, let's take a look at why an enterprise or mid-sized business might adopt a UTM strategy.

Organisations such as these need to mitigate risk, especially in

the light of recent high-profile data breaches, and the cost to reputation and revenue growth expectations.

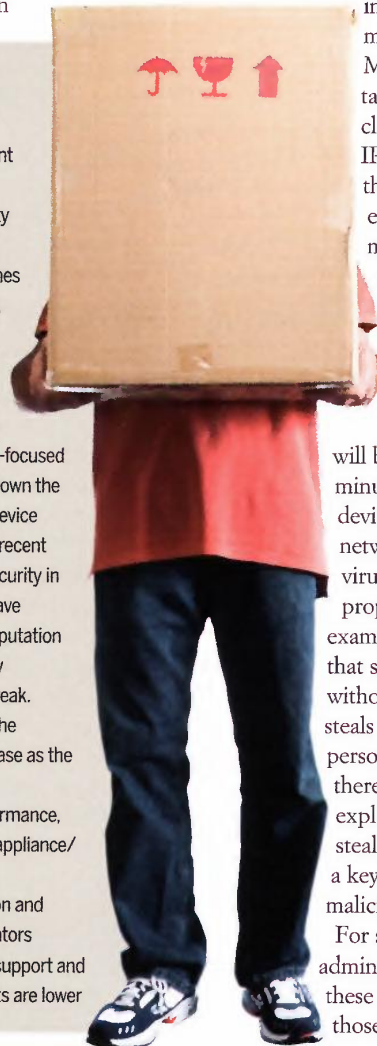
There are many threats facing security administrators and enterprise and SMB information security managers in 2009.

Malicious websites are targeting visitors, with clever manipulation of IP addresses whereby the IP address changes every five minutes – making detection increasingly difficult.

There are threats from automated repackaging applications, which change how malware will be delivered every few minutes. And mobile devices that connect to a network can encourage virus and malware propagation – for example, an SMS worm that sends out an SMS without your knowledge or steals your company and personal contacts. And there are PDF and flash exploits that inject code to steal information using a keylogger or other malicious Trojan/malware. For security administrators to counter these fresh threats and those already in the wild,

Why adopt a UTM strategy?

- To upgrade from an endpoint infrastructure
- To reduce increased security leakage from consumer technologies, such as iPhones – and Web 2.0 applications, such as social networks and mash-ups
- Because vendor business models have moved from a capital-focused to a service-focused model – which is bringing down the cost of purchasing a UTM device
- Budgets are tighter than in recent years – so purchasing a "security in the one box" solution can save money, increase security reputation and deliver future scalability
- Cybercrime isn't taking a break. Some experts believe that the cybercrime threat will increase as the global downturn continues
- The UTM gives higher performance, more capability and better appliance/application control
- It means easier configuration and management for administrators
- Training, certification, tech support and maintenance/licensing costs are lower



PHOTOLIBRARY.COM



Technology briefing

they will need to be supported by a world-class security management research team, so that all vulnerabilities can be identified and removed quickly. These include malware, VoIP exploits, spyware and scareware threats (ie fake scanning websites that don't scan your PC, but drop a malicious payload that collects sensitive information from your computer and network). A UTM that covers all such threats is an attractive proposition.

Threat-management centres will play an increasing role in assisting UTM administrators defend the network from data breaches that could affect the share price and employees' jobs and increase the risk of a company having its reputation damaged in the long term.

CIOs and administrators are looking for a flexible approach to network security management where they can pick and choose which modules (eg anti-virus) they need activated – and where (eg the network gateway). As the move to distributed enterprise solutions continues, so there will be a trend to consider network virtualisation and to manage all the endpoints that are directly connected to the internet. This is already happening and enterprise and mid-sized businesses will be able to adopt information security polices that reflect the virtual wide network with greater ease, more cost-effectively and in a proactive way.

There is a trend where enterprise and mid-sized businesses are requiring sizeable disk space to support the needs for anti-spam, virus quarantining and linking to the corporate directory, so demand for disk space is likely to increase in the rest of 2009 and beyond.

There is also a move to more user personalisation (think Facebook and what you can find out about your employees), where you don't just look up an IP address and run a port inspection, you build a user profile picture based on the employee and a specific department.

This will allow organisations to manage network security (ie through web content filtering and deep packet inspection)

“For administrators to counter these fresh threats, they need to be supported by a world-class security management research team”

more effectively and provide reports on working patterns in an effort to reduce overheads.

As mentioned above, the next step for UTM customers to upgrade to is known

Case study: Pembrokeshire College

A recent example of UTM in action is the deployment last year of a Fortinet FortiGate 1000A-FA2 UTM at Pembrokeshire College in Haverfordwest, south-west Wales. The college has a student population of 8,000 and over 700 teachers and support staff. The college network has 1,400 desktops and laptops, in addition to many other devices for which the IT team needed to find an alternative network security solution.

Having spoken to other users of Fortinet, read reviews and piloted a FortiGate 1000A UTM device, the college decided to purchase a UTM solution. Its main reasons were: achieving a level of performance that met the college's security requirements; running anti-virus and a firewall in tandem; and being able to utilise the platform for VPN. It also decided to turn on an additional security service such as web content filtering (WCF), which did not impinge on performance.

The college found it was able to consolidate its security infrastructure while increasing security functionality – including greater security application flexibility – and the traffic load, without reducing performance.

as XTM – extensible threat management. XTM is just that – an extension of the UTM model, with greater security features, networking capabilities and management flexibility.

WatchGuard is one of the leading vendors in going beyond UTM offerings by providing an XTM solution. It takes an intelligent layered approach to security that provides a multitude of security technologies and application proxy technology to defend against malware, viruses and hackers.

Enterprises will be looking towards XTM for: greater WAN optimisation; better management software; simple one-touch control; greater administration; more security configuration options; the ability to upgrade/work alongside existing appliances and to upgrade subscriptions and security services without having to install new devices; and being able to operate in a network topology environment.

So having considered UTM and XTM, what about the future? Some industry security experts speculate that Check Point's software blade architecture (SBA), launched at the end of February, could signal a new trend in the “security in the one box” sector.

Check Point hopes that SBA will alter network security forever. It says that the main advantage of software blades is that they are independent and modular, which allows administrators to select the exact security software blades they need for each part of the business.

This means a company can create any configuration it requires, allowing it greater flexibility to tackle new threats and business risks.

According to IDC, SBA is expected to be the next-generation technology architecture, driven in part by the current economic climate and its demand for cost-effective solutions.

Security analysts and CIOs will certainly be watching and analysing SBA technology and the development of XTM with interest over the coming months. ■