

HEADLINE

A look at the latest trends in Unified Threat Management devices

The 'security in the one box' industry is developing very quickly these days. Rather than purchasing separate solutions from separate vendors there are obvious efficiencies in having the 'security in the one box' – this architecture is called UTM or Unified Threat Management.

The Unified Threat Management (UTM)* industry has attempted to cover a wide spectrum of security products, but the main UTM architecture combines a firewall, anti-virus and anti-spyware.

Until most recently UTM devices had not added features such as SSL VPN, IM, peer to peer and VoIP – but over the past 12 months that has now started to change and so have the attitudes of those who have and will consider purchasing a UTM architecture.

Threats are becoming more sophisticated so this leaves the enterprise and mid-sized business networks open to targeted attacks which include blended security threats, such as phishing e-mails, VoIP exploits and drive-by downloads.

Therefore the UTM device vendors such as Fortinet, WatchGuard and Checkpoint are introducing the next generation threat management devices – Extensible Threat Management (XTM) - to counter these threats.

Checkpoint however have taken this one step further by announcing last month that they believe the future trend will be Software Blade Architecture (SBA) – more on this later. For now let's take a look at why an enterprise or mid-sized business might adopt a UTM strategy.

*The UTM term was coined by analyst IDC in 2004 which described this technology as an 'integrated network appliance that performs firewall, gateway anti-virus, and intrusion detection/prevention services'. The XTM architecture however takes the UTM technology one step further by offering flexibility; user advanced application aware technologies and supports a multitude of network architectures.

Adopting a UTM strategy

Enterprises and mid-sized businesses need to mitigate risk, especially considering recent high profile data breaches, and the cost to business reputation and revenue growth expectations. Some of the reasons for adopting a UTM strategy might be:

- Upgrading from an endpoint infrastructure
- Increased security leakage from consumer technologies such as iPhones and Web 2.0 applications such as social networks and mash-ups

- 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 now much tighter than they have been 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. In fact some leading information security experts believe the cybercrime threat will only increase as the global down turn continues
- The need for higher performance, more capability and better appliance/application control
- Easier configuration and management for administrators
- Training, certification, technical support and maintenance and licensing costs are far lower

Cybercrime is going to develop faster in 2009 than in previous years

Having considered why enterprises and mid-sized businesses should consider a UTM strategy, the next strategic approach must be to discover how to go about countering the increasing variety of cyber threats, which if not dealt with, could lead to data breaches, increasing enterprise costs, disgruntled shareholders and a loss of business reputation.

Here is a snapshot of some threats facing security administrators and enterprise and mid-sized business information security IS managers in 2009:

- Malicious websites targeting visitors with clever manipulation of IP addresses whereby the IP address changes every five minutes making detection ever increasingly difficult
- Threats from automated repackaging malware applications which change how malware will be delivered every few minutes
- Mobile devices that connect to a network which encourage virus and malware propagation – for example an SMS Worm which sends out an SMS without your knowledge or steals your company and personal contacts
- PDF and Flash exploits that inject code to steal information using a keylogger or other malicious trojan/malware.

For security administrators to counter these threats and those already in the wild, they will need to be supported by a world-class security management research team so that all vulnerabilities which include for example malware, VoIP exploits, spyware and scareware threats (i.e. fake scanning websites that don't scan your PC, but drop a malicious payload which collects sensitive information from your computer and network) can be identified and removed quickly.

Threat Management Centers will play an ever increasing role in assisting UTM administrators defend the network from data breaches (which if breached would of course affect the company share price and employees jobs) and increase the risk of a company having its reputation damaged long term.

CIO's and administrators will be requiring a flexible approach to network security management where they can pick and choose what modules (i.e. anti-virus) they need activated and where (i.e. the network gateway). As the move to distributed enterprise solutions continues so there will be a trend to consider network virtualization and manage all the endpoints that are directly connected to the internet. This has been happening and enterprise and mid-sized businesses will be able to adopt Information Security polices that reflect the virtual wide network with much 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 expect demand for disk space to increase over the rest of 2009 and beyond.

There is also a move to more user personalization (think Facebook and what you can find out about your employees!) whereby you don't just look up an IP address and run a port inspection – you actually build a user profile picture based on the employee and a specific department. This will allow organizations to manage the network security (i.e. through web content filtering and deep packet inspection) more effectively and provide reports on working patterns in an effort to reduce costly overheads.

Recent successful UTM deployment case study

An example of the advantages of UTM can be found with Fortinet who recently deployed to Pembrokeshire College in South West Wales. The college has a student population of 8,000 enrolled in part-time and full-time courses and over 700 teachers and support staff. The college network has 1,400 desktops and laptops in addition to many more devices which the IT team needed to find an alternative network security solution.

Having spoken to other users of Fortinet, read over some reviews and piloted a UTM device they decided to purchase a UTM solution. The main reasons identified were performance which met the College's security requirements, running anti-virus and a firewall in tandem and being able to utilise the platform for VPN.

Of additional importance was they decided to turn on an additional security service such as web content filtering (WCF) which did not impinge on performance. Most important of all, they were able to consolidate their security infrastructure while increasing security functionality (including much greater security application flexibility) and the traffic load without reducing performance.

Extensible Threat Management (XTM)

Enterprise and mid-sized business CIO's and technical decision makers will be looking for increased capabilities, especially considering the next generation threats – mobiles, social networks and mash- ups to name a few. A new technology architecture which allows existing UTM customers to upgrade is known as XTM – Extensible Threat Management. XTM is just that – an extension of the UTM model, with greater security features, networking capabilities and more management flexibility.

WatchGuard is one of the leading vendors in innovating UTM solutions by providing an XTM solution that will deliver the extensibility the enterprise and mid-sized business market requires. Expect to see 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 optimization; better management software; simple one-touch control; greater administration; more security configuration options; the ability to upgrade/work alongside existing appliances; upgrade subscriptions and security services without having to install new devices, and of course being able to operate in a network topology environment.

So having considered the UTM and XTM what about the future? Some industry security experts speculate that Checkpoint's Software Blade Architecture (SBA) which entered the scene at the end of last month looks like it could force a new trend in the 'security in one box' solution.

Software Blade Architecture

Checkpoint hope that by launching the Software Blade Architecture (SBA) solution, they hope this will alter network security forever – and more importantly persuade enterprises and mid-sized businesses to upgrade from a UTM or XTM architecture.

The main advantage of software blades are that they are independent and modular which allow administrators to select the exact security software blades they need for each part of the business. This in essence means you can create any configuration you require, so allowing you greater flexibility tackling new threats and business risks head on.

Conclusion

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

Security analysts and CIO's though will certainly be watching and analyzing this new technology and the development of XTM with interest over the coming months.