

## FEATURE

### UTMs OR POINT SOLUTIONS?

*Ian Kilpatrick, of Wick Hill, looks at the pros and cons of both.*

#### Introduction

Unified threat management systems (UTMs) have been growing in popularity for the last few years and many people are now wondering whether individual point security solutions or a UTM, which incorporates several solutions, is the best answer.

The minimum requirement for a UTM, according to IDC, is a firewall, VPN, antivirus and intrusion detection/prevention. UTMs have, however, evolved from this to incorporate additional capabilities which can include URL filtering, spam blocking and spyware protection, as well as centralized management, monitoring, and logging capabilities.

WatchGuard's SOHO Edge series of UTMs for the SME market, for example, combines stateful firewall, VPN, zero day protection, anti-virus, anti-spyware, anti-spam, intrusion prevention, and URL filtering.

Check Point's Safe@Office, also aimed at the SME market, provides an industry proven firewall, together with protection against worms and viruses, a remote access VPN and web filtering. Check Point's UTM-1 appliance, aimed at the mid-market, is very comprehensive providing a firewall, intrusion prevention, anti-virus, anti-spyware, VoIP security, web application firewall, instant messaging (IM) and peer-to-peer (P2P) blocking, web filtering, plus secure site-to-site and remote access connectivity.

UTMs were designed to provide a range of security solutions in a single appliance, reducing costs and simplifying the whole process of security systems management and installation. While the widest deployment of UTMs has been in SMEs, larger companies are also using them, as they too have begun to appreciate the benefits of less expenditure and easier centralised administration. Large companies are typically using UTMs to centrally secure branch and remote offices; or alongside their existing gateway firewall for the additional UTM functionality.

Check Point has extended its UTM range from its SME Offering, the Safe@Office range, to include the UTM -1, which is specifically aimed at the mid-market. While WatchGuard offers the Firebox X Peak e-Series, a comprehensive UTM appliance aimed at the most demanding of network environments.

#### UTM benefits

Cost is a key issue in the growth of UTMs, with common thought being that a UTM device can cost less than a quarter of the price of equivalent point solutions. UTMs' significant cost savings come from lower pricing than buying and implementing the components separately, simplified and reduced installation, plus fewer ongoing management costs such as training, maintenance and upgrades. And of course, UTMs have only one dedicated platform to support.



As an example, WatchGuard's entry level Firebox X Edge series starts at GBP 273 (SRP), while the Firebox X Peak series, for the most demanding networks, starts from GBP 845 (SRP). Check Point's entry level Safe@Office range starts from GBP 316 (SRP) for the wireless ADSL model, and the enterprise UTM-1 appliance starts from GBP 3947 (SRP).

Management is an important issue. For smaller companies with limited or no specialised knowledge of IT security, UTMs provide an easy way to manage the growing number of security threats. Larger organisations using point solutions are often unable to scale the solutions to the number of sites they have, because of cost, installation, management and ongoing support issues. This can lead to organisations deploying reduced security and inferior policies at remote locations. UTMs can enable them to overcome these problems.

A stated disadvantage of UTMs is that they have a single point of failure with all security systems potentially down at the same time. This is typically dealt with by using high availability.

### Buying a UTM

For any company looking at UTMs, it is essential to define requirements and thoroughly research the market, but going for an established name with a proven record in firewall security is a good place to establish a shortlist. Bear in mind that there is no legal definition of a UTM and that there are significant variations between UTM appliances, both at the top and bottom of the market. The variations are on price, functionality, performance, scalability and most importantly security.

If you're buying a UTM appliance you'll typically be looking for three or more years' life out of the device, so you'll need considerable room for growth or an appliance that is licence upgradeable for both performance and function. Both WatchGuard and Check Point can provide this. You'll also need a firewall that has deep packet inspection as a minimum, not just stateful inspection.

Other key factors to consider with UTMs are future proofing and performance issues. Some UTMs have the ability to start out with just the functions required and then add additional functions, as the need arises. WatchGuard's Firebox Edge, Core and Peak series offer this facility.

Performance is another key element. Many UTMs aren't designed for all the functions to work together, so performance can rapidly decline when all functions are switched on. This is often not apparent from the throughput statistics as the majority of published performance statistics are with most of the functions switched off! In addition, as loads continue to rise over time (who'd have thought only two years ago that 10MB attachments can be fairly commonplace today) any purchase needs to either have significant additional capacity, or the ability to upgrade the box in the rack (i.e. licence upgradeability)

### Conclusion

As different threats continue to emerge, UTM vendors are likely to add increased functionality to their products. As they do, it's likely that more companies will want to use UTMs to simplify the process of securing themselves against the growing number and diversity of security challenges.

*For further press information, please contact Annabelle Brown on 0191 252 8548, email [a\\_brown@dial.pipex.com](mailto:a_brown@dial.pipex.com). For reader queries, please contact Wick Hill on 01483 227600, [www.wickhill.com](http://www.wickhill.com).*