

FIREWALL OR UTM FOR LARGER COMPANIES?

By Ian Kilpatrick, chairman of IT security specialist Wick Hill Group.

Summary of feature

- * UTMs used to be the domain of smaller companies but they are now being used by larger companies.
- * What a UTM includes
- * Benefits of UTMs
- * How larger companies are using UTMs
- * UTMs now available which are aimed at larger companies and can offer powerful performance and multi-gigabit throughput
- * UTMs can help larger companies manage and control security throughout their organisation from a central point
- * UTMs can provide an easy growth path for larger companies.
- * How UTMs can fulfil 'green' policies
- * How to choose a UTM
- * The future of UTMs

UTMs used to be the domain of smaller companies, but Ian Kilpatrick, chairman of security specialist Wick Hill Group, explains why UTMs are now a serious contender for providing firewall protection, and a whole lot more, for enterprises and larger companies.

Unified threat management systems (UTMs) have been growing in popularity for the last few years. Traditionally, they have been widely adopted by SMEs, but larger companies and enterprises are now also deploying UTMs, appreciating the benefits they can offer.

UTMs are designed to provide a range of security solutions in a single appliance, reducing costs and simplifying the whole process of security systems management, reporting and installation.

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

There are many reasons for the growth in popularity of UTMs. Cost is a key issue, with common thought being that a UTM device can cost less than a quarter of the price of equivalent, individual point solutions. Simplified centralised management is a further reason for adopting UTMs. Having multiple security solutions in one appliance makes managing security overall much simpler, as well as enabling easier event consolidation.

Larger companies and enterprises are now also adopting UTMs because they 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. Additionally, many companies are using UTMs as their main gateway security appliance for all functions.

Larger organisations using point solutions are often unable to scale the solutions to the number of sites they have, because of cost, installation, management, reporting and ongoing support issues. This can lead to organisations deploying reduced security and inferior policies at remote locations. UTMs can help overcome these problems.

Where companies use a powerful UTM as their main firewall and also deploy the same brand UTMs at branch offices, they have the big advantage of being able to manage and report on all their branch office

security from one central location. This can give much greater control over branch and remote office security, simplify and improve overall company security, reduce support costs in areas such as patch updating, and reduce data centre costs.

UTM models are now available which are aimed specifically at larger sites, with the high performance and multi-gigabit throughput to deal with thousands of users. Such systems might integrate stateful packet firewalls with VPNs, zero day attack prevention, anti-spyware, gateway anti-virus, intrusion prevention, anti-spam, and URL filtering.

The recent importance of green issues is another reason UTM's are becoming more attractive to larger companies. UTM's integrate several security functions into one single appliance and this fact alone could qualify them to be 'green'.

One single UTM appliance can replace up to five or six separate security appliances or servers. This saves space data centre space in the office and significantly reduces power consumption, both in the rack and in the air conditioning necessary to cool multiple products. Given the increased pressure on data centre's in relation to power issues, this is can be a key benefit.

A UTM could also be considered 'green' if it can easily upgrade to add more functionality and performance. This would allow a UTM to grow and change with a company's needs, rather than having to be wastefully ditched when it fails to cope with increased demands.

A stated disadvantage of UTM's over point solutions is that they have a single point of failure with all security systems potentially down at the same time and this would obviously be a serious problem for large enterprises. However, one additional appliance can provide failover protection for perhaps five key security functions.

Choosing a UTM

For any company looking at UTM's, 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 way of establishing a shortlist. Bear in mind that there is no legal definition of a UTM and that there are significant variations between UTM appliances. The variations are on price, functionality, performance, scalability and most importantly security.

Not all suppliers provide solutions that are suitable for larger companies. Performance is a key element. Many UTM's aren't designed for all the functions to work together, so performance can rapidly decline when all functions are switched on.

You may want considerable room for growth or an appliance that is licence upgradeable for both performance and function. You'll also need a firewall that has deep packet inspection as a minimum, not just stateful inspection.

The future of UTM's

As businesses grow, their security platform will need to grow with them. UTM vendors such as WatchGuard and Check Point are now producing UTM's that will adapt to and grow with future security needs.

Based on the knowledge that they will increasingly be fulfilling the needs of enterprises and larger companies, UTM appliances will be able to proactively adapt to dynamic network environments, as well as protect against unknown future threats.

UTM appliances will be interoperating in and supporting very mixed network topologies and have the inherent security technology to be flexible. Administrators will be able to pick and choose the security service they want from UTM devices.

Conclusion

Enterprises and larger companies are increasingly selecting UTM's as an alternative to firewalls and coupled with multiple point solutions. Costs savings, easier management and green credentials are just a few of the issues which make them attractive.

Powerful UTM appliances with high performance aimed at very large networks are now available. Future development will provide adaptability and future proofing which will help all companies protect in an ever changing and increasingly complex security environment.

ENDS

For further press information, please contact Annabelle Brown on 0191 252 8548, email abpublicrelations@btinternet.com. For reader queries, please contact Wick Hill on 01483 227600, web www.wickhill.com.

Bio - Ian Kilpatrick

Ian Kilpatrick is chairman of value added distributor Wick Hill Group plc, specialists in secure infrastructure solutions. Kilpatrick has been involved with the Group for more than 30 years. 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.