

FEATURE

UTMs CAN SIMPLIFY SECURITY SYSTEMS MANAGEMENT AND CUT COSTS

March 07

Ian Kilpatrick, chairman of Wick Hill Group, looks at how UTMs help with security systems management and advises on choosing a UTM appliance.

Unified threat management systems (UTMs) have been growing in popularity for the last few years. This is largely because they provide an excellent means of reducing security costs and simplifying the whole process of security systems management and installation. UTM growth is predicted by many analysts to significantly exceed that of firewalls and individual point security solutions over the next few years.

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 centralised management, monitoring, and logging capabilities.

UTM benefits

While the widest deployment of UTMs has been in SMEs, larger organisations are also using them, as they increasingly appreciate the benefits of less expenditure and easier centralised administration. Large organisations are typically using UTMs to centrally secure branch and remote offices; or alongside their existing gateway firewall, for the additional UTM functionality.

Cost is a key factor behind the growth of UTMs, with some appliances costing less than a quarter of the price of equivalent point solutions. UTMs' significant cost savings come from simplified and reduced installation, as well as fewer ongoing management costs such as training, maintenance and upgrades. And of course, UTMs have only one dedicated platform to support.

UTMs also provide some major benefits in relation to software and hardware management. A single dedicated appliance is a significant reduction in asset inventory, and of course removes the licence tracking and reporting issues of point solutions installed on servers.

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.

There is no legal definition of a UTM and there are significant variations between UTM appliances. The variations are on price, functionality, performance, scalability and most importantly security.

Buying a UTM

Key factors to consider when buying a UTM are future proofing and performance issues. With some UTMs, you can start off with just the security solutions you need and add extra functionality as required, which is a good option. You should also look for a solution which allows you to easily upgrade performance.

Beware of vendor performance statistics. Many UTMs aren't designed for all the functions to work together, so performance can fall off rapidly when all functions are switched on. This is often not apparent in the statistics, which may give performance details with most of the functions switched off!

Finally, make sure you choose a UTM which has deep packet inspection firewall, as a minimum, not just stateful inspection, which doesn't provide adequate security.

ENDS

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