

FEATURE

SEVEN TIPS FOR SELECTING UTM APPLIANCES

By Ian Kilpatrick, chairman Wick Hill Group

- 1.** Ask whether the UTM does stateful inspection and deep application inspection. Some cheap devices still only do basic packet inspection, while reliance on signature-based protection is extremely processor intensive.
- 2.** Ask whether you need all the functions in a UTM. A solution that contains a high number of functions may be more expensive, or more processor intensive, than one that contains just the functions a customer needs. WatchGuard UTMs, for example, let you add functionality as you need it, which is a huge benefit.
- 3.** Consider what the performance is like in the real world, with all the relevant functions switched on. Most suppliers provide throughput statistics. However the majority of those statistics are for firewall and VPN throughput only; or suppliers may quote performance for a specific function, such as anti-virus, and the quote is with all other functions switched off.

In the real world you are going to switch on some or all of the additional functions. A significant percentage of UTM devices don't scale well and performance can fall off rapidly with additional functions switched on. Major players such as WatchGuard and Check Point have solutions that perform extremely well in live environments.
- 4.** Does the UTM use silo-based or integrated solutions? The ability to grow with your requirements is clearly associated with the ability to scale. Where solutions are built up of multiple components that aren't integrated, good traffic is often repeatedly processed, which seriously impacts performance.
- 5.** Sizing is an important issue to consider. You want a solution that will still be performing in 18 months time. Consider solutions such as those from WatchGuard and Check Point which are performance upgradeable in the rack.
- 6.** Look at support costs, as there can be significant variations between suppliers.
- 7.** What is the centralised management capability? Look for solutions which provide good, low cost centralised reporting and management. Vendors such as WatchGuard and Check Point can provide this.

ENDS

April 07