

BY ERYIN HALMEN

Country Sales Manager, Malaysia & Brunei  
Fortinet Malaysia

## UNLEASHING PURPOSE-BUILT NETWORK SECURITY DEVICES

Today's organisations must account for more points of entry into their networks, more types of resources that require protection, and substantially greater diversity of the threats seeking to exploit any weaknesses that may be present.

From our observation, security strategies based predominately on point products is no longer sufficient mainly because the primary motivation of hackers has shifted from gaining notoriety to making money, causing a step function change in the diversity, sophistication, and elusiveness of threats. The widespread availability of exploit development frameworks means that both new threats and variants of existing ones can be generated very easily and rapidly.

What's more, the impact of enabling much higher degrees of user mobility, interconnectivity, and third-party access to their network systems has led to the introduction of more points of entry for threats, as well as increased physical distribution of the data and resources requiring protection.

To adequately respond to these factors, organisations require a multi-threat management solution that provides comprehensive functional coverage that blends a wide range of countermeasures, including ones that are preventive in nature (e.g. firewall) to complement those that are primarily reactive (e.g. antivirus), comprehensive logical coverage which provides protection for threats against all elements of the computing infrastructure (e.g. networks, systems, services, applications, and data), as well as comprehensive physical coverage which is applicable not just at Internet boundaries but at locations throughout an organisation's computing environment (e.g. the data center, in remote offices, and at choke points on internal networks).

Yet, addressing the above requirements by continuously implementing additional point products to fill in the associated gaps in the defenses is not a sustainable strategy. It invariably results in high capital costs, runaway operating expenses, and, despite the best efforts, is still not very effective due to the holes that inevitably appear at the seams of this type of patchwork solution.

Given this situation, it is not surprising that many organisations have selectively implemented and continue to consider unified threat management (UTM) devices as a means to restore balance to their overall security solution. According

to market researcher IDC, the UTM market in the Asia Pacific will expand to a compound annual growth rate (CAGR) of more than 40% until 2009, making it one of the fastest-growing segments of computer security.

### UTM Solutions

UTM solutions simplify an organisation's overall security solution, despite the factors that are causing the security problem to grow in scope and complexity. Fundamentally, this is accomplished by combining multiple functional and logical security capabilities in a single physical device.

To ensure they can optimally address the prevailing security challenges, organisations should look beyond conventional UTM products and seek solutions that qualify as true, purpose-built network security platforms.

A purpose-built network security platform is effectively an advanced UTM solution – one that employs an optimised design to ensure that organisations can maximise the associated gains.

To optimise security, performance, flexibility, and cost effectiveness, a purpose-built network security platform must be a turn-key system.

For starters, this entails having a pre-packaged device that combines hardware, network security operating system, and all requisite security software. It also must include research-fueled, security subscription services, in addition to conventional maintenance and technical support services.

The next high-level requirement that defines a purpose-built network security platform is that it must exhibit significant degrees of integration, yet still be modular in nature.

The third and final high-level requirement that defines a purpose-built network security platform is that it must be based on engineered hardware. What this means is having hardware that guarantees sufficiently high performance based on it being "matched" to the specific security software, networking services, and implementation scenarios that it is intended to support.

The net result is an exceedingly pragmatic network security solution – one that thoroughly and uniformly addresses the functional, logical, and physical security requirements of today's organisations; achieves the highest levels of security effectiveness and operational efficiency; and, is not disruptive to business critical communications and application transactions. **mb-e**