

**Missing Link**   
**Security Services**  
Mark Bouchard, Founder

## Performance Features Pave the Way for Enterprise-Class UTM

### Capsule

The need for speed is on the rise. Consequently, the only UTM products suitable for enterprise-class deployments will be those characterized by performance-oriented designs and associated performance-centric feature sets.

### About the Author

---

Mark Bouchard, CISSP, is the founder of Missing Link Security Services LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security topics for over 10 years. He is passionate about helping enterprises address their information security challenges. During his career he has assisted hundreds of organizations worldwide with strategic and tactical initiatives alike, from the development of multi-year strategies and overall architectures to the justification, selection, acquisition, implementation and operation of individual security and privacy solutions.



## Context

---

The benefits of Unified Threat Management (UTM) – consolidation and simplification of security infrastructure, stronger security, improved operational efficiency, and lower total cost of ownership – are well established. To date, however, these advantages are, to a great extent, only being realized by SMEs and for the remote/branch office locations of larger enterprises. This is due in no small part to the legitimate concern that UTM devices are not capable of sustaining operation of multiple security functions in enterprise-class scenarios, such as in front of high volume/complexity/criticality Internet DMZs and data centers – at least not without cutting corners somewhere along the line (e.g., in terms of depth or breadth of inspection). To be clear, this concern is well-founded, especially considering the collection of factors driving the need for even higher levels of performance. These include:

- ***The volume and nature of communications traffic.*** Businesses are increasingly data dependent and are continuously seeking operational and competitive advantages via IT. The result is steadily rising throughput requirements and the proliferation of new technologies/applications, many of which are latency sensitive (e.g., VoIP, video, real-time collaboration).
- ***The nature of today's threats.*** A shift in hacker motivation from gaining notoriety to making money has led to increasing diversity and elusiveness of threats. Consequently, security devices must incorporate and/or coordinate multiple countermeasures, in addition to providing compute-intensive application-layer inspection capabilities to counter the advance of threats “up-the-stack”.
- ***The dissolving perimeter.*** Web 2.0, user mobility, extensive support for 3rd-party users, tunneling techniques, and virtualization are all contributing to a situation where communication patterns are becoming far less structured. Any-to-any is becoming the norm and the distinction between “internal” and “external” is steadily being eroded. Thus, it is no longer practical to set policies selectively; rather, it is becoming necessary to inspect every packet of every protocol across every interface for all types of threats.

## Considerations

---

Just because a concern is legitimate does not mean it is insurmountable. The performance challenge for UTM is fairly obvious and, as such, the leading vendors in this segment have sought to tackle it head on. The result, in general, is that UTM solutions are becoming increasingly suitable even for enterprise-class deployment scenarios. Still, there is bound to be considerable variation from one product to the next – not to mention the usual “puffed up” claims, bandwagon jumping, and, in some cases, even “vaporware”. In this regard, absolutely nothing will surpass the value of the purely objective and organization-specific findings that can be obtained by running a full-blown lab test or pilot program. Short of that degree of rigor – or to help select which vendors to invite to the test – UTM products being considered for enterprise-class deployment should be gauged by the extent they exhibit the following performance-centric design characteristics and features.

- ***Purpose-built System*** – Firewalls or, worse yet, networking devices with other security capabilities “bolted on” will be at a significant disadvantage. Instead the focus should be on solutions that are built and optimized from the start to be multi-function security gateways.
- ***Specialized Hardware*** – Off-the shelf PC/server hardware will not get the job done. This doesn't mean that custom silicon is necessary, but at a minimum designs should incorporate multiple processors, specialized accelerators where available (e.g., for crypto), and generous amounts of memory.
- ***Innovative/Scalable Inspection Techniques*** – Much of the performance burden for UTM devices stems from the use of protocol-specific proxies that require full message/session reassembly to inspect files and content for threats. In contrast, stream-based techniques, when applicable, require far less processing power and memory and provide coverage for a broad array of protocols, traffic types, and file sizes all at once.
- ***Rock-solid Reliability*** – The only thing worse than poor performance is no performance. Thus, it is also important to have a full set of high-availability features, such as: interfaces for backup network connections, native failover or clustering capabilities, an out-of-band management interface, and redundant components (e.g., fans, power supplies).



## Conclusion

---

Organizations should not automatically dismiss the use of UTM for enterprise-class deployment scenarios on the basis of historical concerns pertaining to inadequate performance. Overall, UTM products have matured significantly, especially over the past two years. Those that exhibit high-performance designs/architectures and corresponding features, in particular, deserve consideration even for highly demanding use cases.