

Missing Link 
Security Services
Mark Bouchard, Founder

Security Considerations for Enterprise-Class UTM

Capsule

Although robust, coordinated security capabilities are a “must-have” for enterprise-class UTM, a highly effective solution ultimately depends on achieving balance in several related areas.

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

Despite a compelling set of benefits – including consolidation and simplification of security infrastructure, stronger security, improved operational efficiency, and lower total cost of ownership – Unified Threat Management (UTM) technology has had relatively little traction beyond SMEs and the branch-office locations of larger enterprises. One reason for this is the concern that combining multiple security functions on a single device necessarily involves making compromises, for instance, in terms of the consistency of quality, breadth of features, and/or overall effectiveness of the individual countermeasures. And these days, further fuel is being thrown on the fire in the form of several trends that are causing the security “problem” to become even more challenging.

- Threats are being generated more quickly than ever before, thereby driving the need to complement purely reactive countermeasures with ones that are more proactive in nature.
- Threats are becoming more diverse and more elusive. No longer is it just a battle against viruses and worms. Consequently, more and different layers of protection are required to address the new generation of spyware, trojans, rootkits, bots, application-layer threats, and even targeted attacks.
- The volume of vulnerabilities is on the rise. Pressure to remain competitive and/or reduce costs is driving the rapid adoption of new (read: vulnerable) technologies and applications, not to mention the pursuit of deeper levels of interaction and integration. All of this, including the proliferation of rich and real-time applications, introduces more points of entry for threats, driving the need for security infrastructure with both broader coverage and greater performance capabilities.

Considerations

Talk about a conundrum. The trends that are potentially threatening to the quality and overall effectiveness of UTM are the very same ones that are driving the need for a more efficient way to deploy a greater array of countermeasures (in a greater number of locations) in the first place. This should not be misinterpreted, however, as an indication that enterprise-class UTM is impossible. Instead, what it means is that a successful solution must achieve balance. And in the case of security, this balance should be present in three distinct areas.

1. Having a collection of countermeasures that are all individually best-in-class is not really necessary. This may seem counterintuitive. However, the point is that having “very good” capabilities and a rich-but-not-overwhelming set of features for some of the countermeasures is often more than sufficient. Indeed, achieving balance in this area can actually lead to several advantages, such as being able to establish broader coverage of threat types than would otherwise be possible, reduced complexity, and possibly even better performance.

2. Having a collection of countermeasures that is truly comprehensive is not really necessary. In particular, highly specialized countermeasures with a narrow focus or the need for extensive customization (e.g., web application and web services firewalls) should be left to separate, standalone security solutions. Instead, the focus should be on having a set of highly *complementary* services that address a significant percentage of the most prevalent threats facing today’s organizations. Accordingly, an appropriate set of security capabilities for an enterprise-class UTM solution includes the following:

- **Denial-of-service protection** – to thwart related network-level attacks;
- **Virtual private networking** – to support secure communications for remote users and offices;
- **Stateful, multi-layer firewall** – to provide enforcement of access control policies;
- **Deep packet inspection** – to provide network-to-application layer filtering of permitted sessions for malicious traffic;
- **Application classification** – to support setting policies by application type and individual functions;
- **File and content based inspection** – to scan virtually all traffic for threats that reside at the data level;
- **Web/URL filtering** – to prevent misuse of Internet resources and help keep users from connecting to infected websites; and
- **Extensive logging and reporting** – to track both security events and administrator activities.



3. The nature and degree of security integration should be balanced as well. Sharing and coordinating event data and various security management functions are definitely appropriate “points of integration”. In contrast, potential performance gains attributed to low-level merging of different security “engines” must be carefully weighed against the need to avoid cut-through vulnerabilities (i.e., where a flaw in one service automatically allows other services performing traffic inspection to be bypassed).

Conclusion

Organizations should not automatically dismiss the use of UTM for enterprise-class deployment scenarios on the basis of historical concerns pertaining to breadth and depth of security features. Overall, UTM products have matured significantly, especially over the past two years. In particular, those solutions that exhibit balance in terms of the quality, quantity, and level of integration of incorporated countermeasures deserve consideration even for highly demanding use cases.