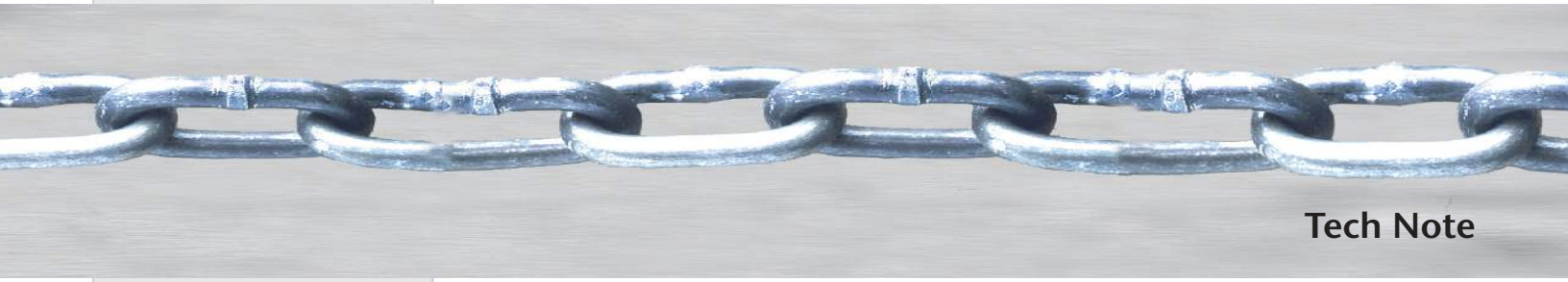


Tech Note

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:

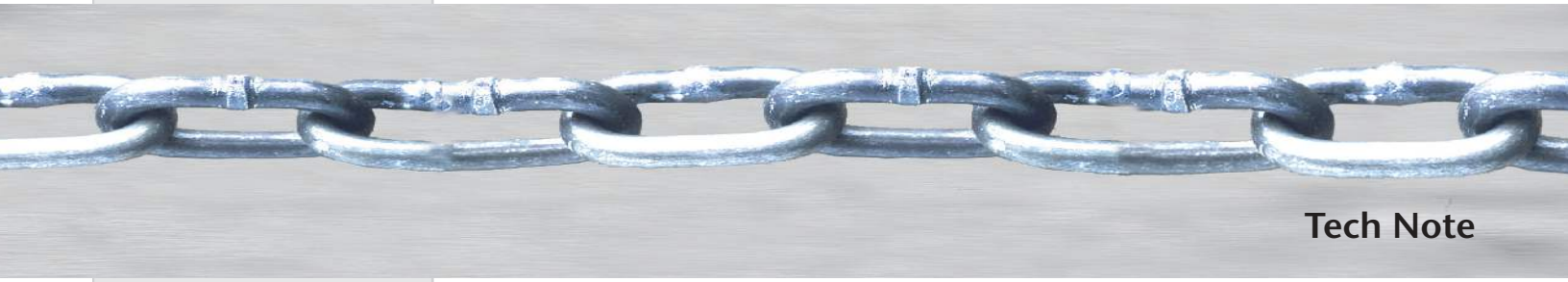
- ***Denial-of-service protection*** – to thwart related network-level attacks;
- ***Virtual private networking*** – to support secure communications for remote users and offices;
- ***Stateful, multi-layer firewall*** – to provide enforcement of access control policies;
- ***Deep packet inspection*** – 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.

© 2007 Missing Link Security Services LLC. All rights reserved.



Tech Note

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 an 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

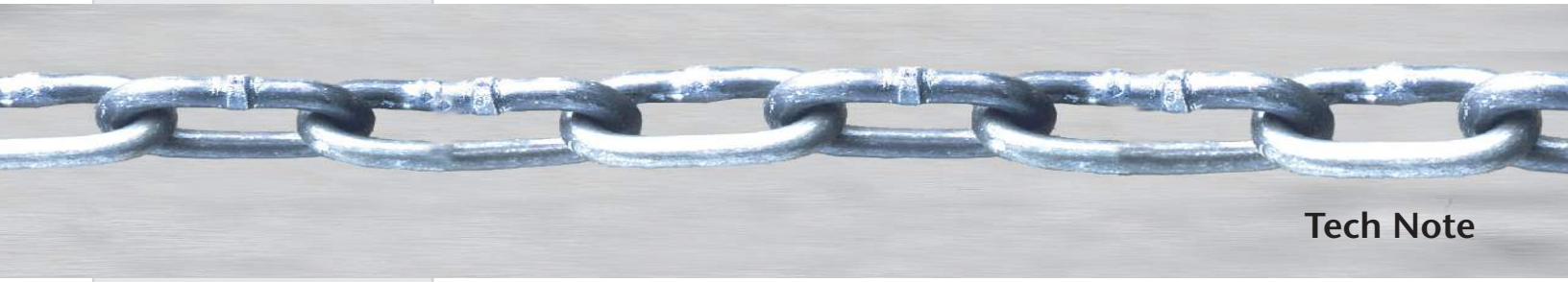
Just because a concern is legitimate does not mean it is insurmountable. The performance challenge for UTM is fairly obvious and, as such, the leading vendors in this segment have sought to tackle it head on. The result, in general, is that UTM solutions are becoming increasingly suitable even for enterprise-class 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.

© 2007 Missing Link Security Services LLC. All rights reserved.



Tech Note

Missing Link Security Services
Mark Bouchard, Founder

Critical Criteria for Enterprise-Class UTM

Capsule

UTM technology definitely deserves consideration for enterprise-class implementation scenarios, but only if associated solutions fully address key criteria and the deploying organization is operationally prepared for functional consolidation.

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

Unified Threat Management (UTM) involves combining multiple security capabilities and packaging them with hardware, typically in the form a multi-function security appliance. At a high level, the point of UTM is consolidation, or enabling organizations to deploy numerous countermeasures without the need to deploy, manage, and maintain a corresponding number of separate, physical "boxes" and corresponding management consoles. But that is really just the tip of the iceberg. Additional benefits typically associated with UTM include stronger security, improved operational efficiency, and lower total cost of ownership.

Not surprisingly, the result over the past few years is an adoption rate that has been nothing short of tremendous. This is particularly true among SMEs and for remote/branch office locations. The nagging question that still remains, though, is whether UTM is "ready for prime time." Is it suitable for enterprise-class deployment scenarios, such as in front of high volume/complexity/criticality Internet DMZs and data centers? The obstacle in this regard has been the relatively reasonable concern that combining numerous security services on a single device has, at least historically, involved making compromises in terms of depth/strength of capabilities, manageability, and solution scalability and performance.

Considerations

The answer to the question posed above is an emphatic though qualified "Yes, UTM is ready for prime time." Leading solutions have had several years to mature and, in general, to address the concerns and requirements associated with enterprise-class deployment scenarios. That said, it should also be clear that not all UTM products are created equal. There will inevitably be significant variation, especially in terms of the degree of integration and unification of both the core security services and how they are managed. Indeed, whether any specific UTM solution is appropriate for enterprise-class deployments will depend on the extent to which it addresses the following key criteria:

Security

There are three aspects to this criteria: all of the individual security technologies must be very good, if not actually best-in-class; "all" in this case means a set of *complementary* services that provide relatively comprehensive protection against prevailing threats, but NOT everything under the sun; and security should be enhanced, not compromised, by having integration between individual services and by having a design where a flaw in one service does not allow other services performing traffic inspection to be bypassed.

Performance

A purpose-built system architecture, specialized hardware, innovative and scalable inspection mechanisms, support for high availability, and other related techniques should be present to ensure both non-stop operation and that rated throughput *and* low latency is consistently attainable with real-world traffic and all services operating.

Management

Centralized control is essential for all life-cycle management functions (e.g., configuration, monitoring, troubleshooting, and reporting) and helps to ensure consistency of policy enforcement. More importantly, though, there should be (a) substantial integration in terms of both data/event sharing and policy/rule development, and (b) extensive role-based administration capabilities.

Flexibility/Compatibility

For starters, which security services get used in any given instance of the UTM device should be selectable, not fixed. In addition, the solution should be modular/upgradeable (to account for future requirements) and, in general, should be designed to seamlessly "fit in" (e.g., by supporting core networking capabilities, multiple deployment modes, and numerous options for features such as authentication, encryption, and network interfaces).

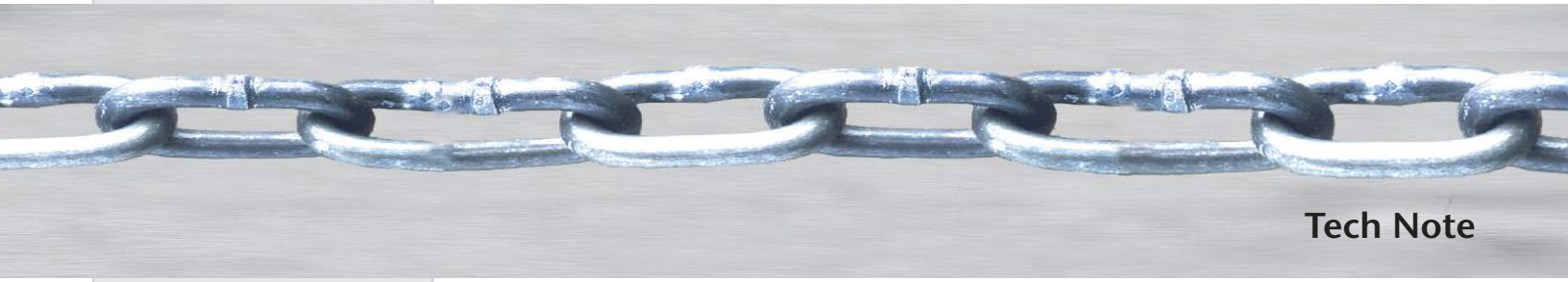
Integration

This criterion is somewhat redundant, since it has already been mentioned elsewhere; but it deserves repeating. Without pervasive integration and coordination (e.g., in terms of processing packets, consolidating event alerts, and management functionality), the benefits of UTM diminish, yielding little more than physical consolidation.

Conclusion

UTM products that stack up well against key criteria in the areas of security, performance, management, flexibility, and integration are definitely appropriate for enterprise-class deployments. However, it is also important to recognize that product readiness is only half of the equation. The other half is readiness of the organization itself. In other words, deploying UTM in high volume/complexity/criticality scenarios will be less appropriate/worthwhile for organizations that (a) have not sufficiently depreciated any recent/significant investments in their security infrastructure, or (b) that are culturally and operationally "siloed" in terms of security system ownership and/or functional responsibilities.

© 2007 Missing Link Security Services LLC. All rights reserved.



Tech Note

Missing Link Security Services
Mark Bouchard, Founder

Management Considerations for Enterprise-Class UTM

Capsule

Having enterprise-class management capabilities is not only a crucial prerequisite to deploying UTM technology in high volume/complex/critical scenarios, but also the key to unlocking truly meaningful reductions in cost of ownership.

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

To date, the promised benefits of Unified Threat Management (UTM) technology – including consolidation and simplification of security infrastructure, stronger security, improved operational efficiency, and lower total cost of ownership – have done relatively little to generate uptake beyond SMBs and the branch-office locations of larger enterprises. However, this situation is poised to change. In general, UTM products have matured considerably over the past couple years and initial concerns pertaining to inadequate performance and security capabilities are steadily being addressed.

That said, there is still one further area to which prospective customers are encouraged to pay close attention. Specifically, the suitability of UTM technology for enterprise-class scenarios also depends on having a solution with enterprise-class management capabilities. Indeed, having a comprehensive set of management features that are flexible yet efficient is instrumental not only to establishing and maintaining effective defenses but also to achieving significantly greater cost savings.

Considerations

The importance of a UTM solution's management capabilities to support both initial deployment and ongoing operations cannot be overstated. Overall, granular configuration control should be complemented with optional presets/defaults and other ease-of-use features to enable organizations to optimize their implementations in terms of both effectiveness and efficiency. Furthermore, it should be recognized that having an appliance-based solution – where all of the associated software has been pre-loaded and pre-hardened and the resulting "system" has been engineered to maximize performance – is merely a starting point. Additional characteristics and capabilities that organizations should insist on (and ideally evaluate) prior to embracing UTM for enterprise-class deployments include the following:

- Management that is centralized, consolidated, and simplified. This entails, respectively, the ability to manage multiple UTM devices at once, having a single management system that covers all of the incorporated countermeasures, and a high degree of intuitiveness and ease of use that is pervasive across the full set of lifecycle management functions (i.e., configuration, monitoring, q troubleshooting, and reporting). The result, ideally, will be significantly enhanced operational efficiency and unified/consistent policy enforcement.
- Device set-up that is facilitated by configuration wizards and pre-defined, yet customizable templates (e.g., pertaining to different security levels).
- Policy development that is sufficiently granular to account for complex scenarios yet efficient in that it is hierarchical/tiered (e.g., with policy inheritance) and supports flexible grouping of resources, users, and rules.
- Active monitoring that facilitates rapid response/troubleshooting by providing alerts and in-depth views of device status, user activity, security events, etc.
- Extensive logging and highly flexible reporting (e.g., real-time/historical, ad-hoc/scheduled, templates/customizable, summary/drill-down) to support trending, troubleshooting, and all manner of auditing/compliance requirements.
- Granular, role-based administration for assignment of management rights (e.g., by function/service or devices).
- Automatic delivery, notification, and optional implementation of updates for system software, security applications, and associated content (e.g., signatures).
- High reliability and scalability, ideally in the form of having support for load-balanced, redundant pairs of management systems.

© 2007 Missing Link Security Services LLC. All rights reserved.

Conclusion

The consolidation and simplification of security infrastructure that it affords is certainly an attractive, cost-saving feature of UTM technology. However, it is the unification, robustness, and flexibility of associated management capabilities that enable recurring returns, and therefore much greater gains, due to both improvements in ongoing operations and greater security effectiveness. Of course, such capabilities are also one of the primary prerequisites to having UTM be suitable for enterprise-class deployments in the first place (with top-notch security, performance, integration, and flexibility being the others).

© 2007 Missing Link Security Services LLC. All rights reserved.