

Astaro OrangePaper

The UTM Explosion: Sifting Through the Rubble

Author:



Angelo Comazzetto
Product Manager

Date:

2008-08-21

Content	Page
Introduction.....	2
UTM Benefits.....	2
UTM Offerings.....	3
UTM Differences.....	3
Unified Management.....	3
Depth of Field.....	4
Example: Spam Protection.....	4
Example: URL Filtering.....	5
Adapting to Changing Demands.....	6
Simple Licensing Options.....	6
Ease of Use.....	7
Performance Numbers.....	8
Conclusion.....	9

Introduction

Unified Threat Management (UTM) offerings have exploded in the past years. As the security marketplace continues to grow at a staggering pace despite a slowing economy, the concept of integrating multiple security features on a single, reliable platform with one graphical user interface is gaining more support than ever before. Not only are existing vendors re-shaping their offerings to best compete in this space, but new start-up companies appear constantly, offering their flavour of UTM. Making the correct decision as to which product to purchase has never offered more possibilities to the consumer. However, this comes with a price. The scramble by manufacturers to capitalize on what will be a 3 billion dollar market in 2008 has produced a deluge of products that offer varying ranges of features, performance, and capabilities. This paper will explain how to sort through the offerings and identify a product that will best solve your problems by deciphering terms commonly used in the security market, providing a buyer with information awareness so an educated purchase of a security solution can be made.

UTM Benefits

A single platform provides many benefits.

The argument and justification for consolidating many network security products onto a single appliance has been well documented as having many areas of advantage. Inherently, managing multiple products presents a multitude of downsides when compared to an effective UTM solution. Administrators must master multiple management environments, all with different terminologies and feel. They must maintain many firmware and pattern updates, and correctly configure the solutions to interoperate with each other in the proper order so as to ensure the correct functionality is achieved by the entire security deployment. Further, multiple network security solutions present a large increase in troubleshooting complexity since there are many points where misconfiguration and error can occur, raising the amount of places that need to be examined to find the problem. Financially, the deployment of multiple point products becomes even less attractive when the individual subscription services for support, maintenance, and updates are tallied, which are all paid independently for each product. The attractiveness of choosing a UTM appliance is strengthened by having to master just one management GUI, pay subscription fees to one company, and troubleshoot any issues at a single point. Further, the applications on a UTM device interoperate and complement each other so as to best take advantage of the architectural approach of running on the same platform. For example, a UTM appliance can first decrypt incoming roadwarrior VPN connections such as IPsec or SSL, and then filter that traffic

through an Intrusion Protection System. This has advantages over point products which must be placed in the correct order and then configured with complex routing and traffic handling rules to ensure that the proper filters are applied in the correct sequence.

UTM Offerings

At a first look most UTM products look similar

At a glance, today's UTM solutions often appear similar in terms of their capabilities, feature set, and overall concept. While aggregating various 3rd party-, open source- and proprietary point products almost every solution is promising to be "all-in-one", most complete, best-of-breed or most comprehensive. The issue is that the alternative point products are purpose-built and usually focus on a single functional area, giving them extra features and a dedicated platform with which to perform their task. In order to effectively combine the functionality of these point products onto a single platform, not only must the product be able to meet performance expectations, but it must deliver enough functionality in multiple areas so as to warrant replacement of existing products along with being able to accommodate future needs.

UTM Differences

Where should I look at?

However, the aggregation of many different functions provides only a small benefit if they are not integrated into one management system at the same time, without making the entire product highly complex and unusable. However, the downside of many UTM solutions is often the lack of such a "Unified Management" architecture.

Unified Management

Integration instead of aggregation

Therefore one of the primary areas to consider when choosing a UTM product should be how polished and concise the user interface is. Since the main draw of UTM is to manage several areas with a single management console, this environment should be easy to understand and become familiar with, and allow the user to solve security needs in the shortest amount of time. It is not only how polished the user interface is, but also how tight the integration is between all areas of the product. Many UTM platforms deliver a convoluted implementation of the various modules that are not truly aware of the others. For example, in order to address a single need as Web Security, many areas of the environment must be visited and configured independently in order to successfully implement the feature. In such a product, not only would the content filter need to be activated and configured, but allowances might need to be made in other modules of the UTM which need to be made aware that the feature has been enabled. This can require opening the packet filter, creating

masquerading rules, and allowing anti-virus updates to be retrieved from the Internet. In contrast, a more evolved UTM product would allow the administrator to activate the content filter from one section, and have the rest of the system automatically reconfigure itself to allow that feature to become operational.

However important being able to harness the dozens of tools present in a modern UTM is, it is not just how things are tied together and by what GUI environment this is achieved. Of critical and most importance is how rich and effective each feature is when compared on its own in solving problems in that area, known as “Depth of Field”.

Depth of Field

Going beyond published features.

When evaluating a new unified device, consider the capabilities of individual features and their ability to address the problem for which they are targeting, not just their inclusion to satisfy a feature checkbox so as to lend credibility during the buying process. For example, two cars of competing price may have engines that vary greatly in power, reliability, and fuel efficiency, while still delivering the feature “engine”. In this manner, UTM solutions will vary greatly once the quality of the included components is examined in detail.

Too often products implement a bare minimum of functionality in order to justify putting terms on a marketing data sheet and the quality of the components is noticeably lacking when the feature is tested against not only its peers, but also against the problem for which it is designed to solve. The following two sections provide just a few examples of how features that at first appear similar in name and function can differ greatly once their true functionality and capabilities are unveiled.

Example: Spam Protection

Not all Email Filters are created equal.

Spam protection can be done using many different approaches and technologies, yet is still often communicated to the consumer as only “Spam Filter” or “Email Scanning”. For example, filtering Email by subscribing to “Real-time Blackhole Lists” is technically a form of email spam protection; however in real world application a filtering solution that is heavily based on this feature is going to fail miserably in solving the problem of eliminating unsolicited Email from a users inbox, since this method relies mainly on reacting to messages based on what others have said about the source of the Email. Since spammers rarely send from the same address that can be quickly identified and distributed to a static list to prevent future mailings, this method of dealing with spam is completely ineffective as a filtering base. However, adding this

minimum of functionality allows vendors to loosely claim that the product offers “Email Filtering” or “Anti-Spam Functionality” in order to generate leads.

In contrast, a quality Email filter will have multiple means of detection using a variety of tools, so as to allow it to stand on its own against dedicated Email filtering products. A common trend today amongst the most effective Email filters is to treat the outbreak of spam messages like a virus. By tying into large ISP backbones and sharing distributed fingerprints submitted automatically by deployed installations, spam outbreaks can be identified in seconds and the filters can be reactively updated in near real-time across all the installations to adapt for the latest wave of messages. Combined with traditional content-examination methods of Email filtering, a powerful solution can be deployed. Here, the concept of Depth of Field is demonstrated between two products that both offer an “Email Filter”, while at the same time having completely different effectiveness rates when attempting to solve the problem.

Example: URL Filtering

Filtering web content can be done using different approaches.

URL filtering is another area that can be delivered in a large variety of ways. In trying to address the fundamental issue of what sites should be allowed to be visited and what sites should be controlled for reasons of ethics, security, or liability, a large amount of solutions exist and are marketed as Web/URL Filters. Some offer a bare minimum of functionality while others are so complex that to actually deploy and manage the solution requires excessive training or massive network restructuring to accommodate. Some solutions offer a “Web Filter” in their UTM product which only allows for manually specifying sites to allow and block. The effectiveness here is minimal since the sites on the Internet are too numerous and ever-changing to meet the needs of the company. A more effective approach is to classify sites into various categories or types, and then provide a means with which to block sites based on their classification. Here still, many solutions with varying levels of effectiveness can be seen. Some UTM products store a few hundred thousand sites classified into a handful of popular categories on the device itself, which can be updated at certain intervals from the Internet. While better than manually addressing the need to block URLs, this database-style lookup is limited in function by its scope and design.

The very best solutions take advantage of enormous classification databases stored at high-speed, redundant locations which offer billions of sites classified into dozens of categories. This approach is made richer still when the UTM product can identify previously unknown sites during regular operations and automatically submit them to be added to the global database in a short

amount of time so that all installations can benefit from the expanded knowledge. It is even possible to change the entire filtering approach in the best products, by offering administrators the ability to block all sites and only allow certain categories and listed URLs, so as to offer administrators relief in having to constantly tune the filter and run reports to ensure acceptable use.

In this case, Depth of Field consideration reveals not only more options, but also entirely new ways of managing solutions which all fall under the “URL/Web Filtering” area of a UTM.

Adapting to Changing Demands

Look for a UTM platform that can grow with your business.

Upgradability and scalability to address future needs are key aspects of a UTM solution. As the security market faces new threats, manufacturers respond with new tools, versions, updates, technology, and entire platforms. Being able to scale a purchase made today to accommodate solutions introduced tomorrow is often overlooked. Being able to upgrade the firmware of the device to run the company's latest version is a major benefit. It is also important to evaluate how, (if at all) a product's power can be increased to accommodate more users being brought under the protection of the system, but also the activation of more features that may not have previously been available or anticipated. A good feature is the ability to purchase more appliances and cluster them together to share load, all while maintaining a single management console which gives the appearance of a sole platform to the administrator. This allows for multiple UTM appliances to be joined together to create a more powerful installation that works as a collective team, and the best solutions introduce fail-over and fault-tolerance as part of this feature as well. Knowing that there are different possible expansion paths can pay dividends by providing options over only having the choice to move to a bigger UTM platform should the existing solution become insufficient to meet the needs of the company.

Simple Licensing Options

Read the fine print.

The licensing scheme on UTM products can be as diverse as it is complex. While many manufacturers advertise that their hardware appliances allow for unlimited users, rarely is this the case. In the past, it was common for security appliances – similar to pure software solutions - to control the choices available to a buyer in selecting a model by structuring product licensing by IP address counters. This practice continued for many years until the market demanded change. A key factor in this movement was the expanded diversity that UTM solutions became capable of. One company might purchase “Box X” and require it only to act as a Firewall and VPN endpoint for a few dial in us-

ers. The same “Box X” might then be purchased by another company which deploys it with full Email, Web, VPN, Intrusion Protection, and other features. While both use the same product, the first customer can effectively filter a larger number of IP addresses than the company that uses more features before running out of resources. The most capable and diverse of UTM solutions will allow users to field them without running into artificial limits; they will run successfully until the methods by which they have been deployed fully tax the hardware resources (such as CPU and RAM) and thus demand an upgrade or a new device to be added to a cluster.

Some companies have various ways of charging or limiting “per user” that are based on IP address, MAC address, and even other factors not immediately apparent. An example is to offer an advertised unlimited “user count” and then place a limit on the number of concurrent connections that can be active at once. This effectively limits the box while still meeting the advertised claim of allowing “unlimited users”. Other manufacturers will place bandwidth limits which effectively limit the maximum amount of throughput a device is capable of, such as limiting the Internet (WAN) uplink to 1 megabit per second.

A related factor to consider when examining UTM products is if certain functionality is presented only in models higher up in the offerings. Vendors sometimes spread features which might be highly in demand or recently introduced to models that cost more or have special product code derivations, again with the goal of making the buyer spend more. In practice, if “UTM Model 1000” is offered at a certain price, make sure that a problem to be solved does not actually require “UTM Model 1000C” or “Model 300” instead. Understanding the licensing of a product can increase the likelihood that a buyer chooses the correct solution that fits.

Ease of Use

Know what you will be working with and what it looks like.

A widely used term by many vendors is “ease of use”. It is amazing how often this phrase is accepted at face value. The core concept is to convey to a possible buyer how intuitive it is to manage the solution, usually via a GUI, which is standard in the UTM arena today. However, almost every product claims that its “ease of use” makes it better than everyone else’s product. A product that makes use of a good design process is immediately evident after looking at just a few screenshots or spending a few minutes inside an online demo or test platform. It becomes easy to see the differences in usability amongst UTM platforms by examining the layout of the GUI, and how the various areas are presented to the administrator. Putting the commonly used tasks in prominent areas and limiting the need to use CTRL or ALT modifiers, right-clicking, or

other hidden commands can do wonders in putting all the information in front of an administrator without having them remember proprietary operating commands.

Furthermore the term “ease of use” is by nature completely subject to who is using the product. For example, an F1 racing car is an immensely complex tool that requires an elite level of training and experience to drive correctly, however F1 drivers are used to it. And while only a handful of people on the planet are capable of operating such a machine, it is technically “a car” that has a wheel, pedals, and other controls almost everyone is familiar with. In the same manner, today’s latest-generation of UTM devices usually have some sort of GUI segmented into various areas, drop down and selection boxes. In the best/newest solutions, various implementations of Web 2.0 AJAX-style interaction are introduced that allow users to move smoothly through the product and make changes without having to become experts in the technology that is being controlled. UTM solutions that still rely on command-line configuration, extra client management programs, or even completely separate GUI environments that launch for individual areas of configuration can be easily eclipsed by a solidly designed product which takes the user into account and not just the technology being configured.

Try before you buy

When evaluating UTM solutions, take the time to attend a webinar, see the interface in action, or request an evaluation box so the GUI can be experienced in person. A good factor to evaluate is what configuration is placed in the product by default at the factory. If the product immediately requires extensive configuration to make it compliant with the security policy of the company, there are more points of possible misconfiguration vs. one that ships in a fully “locked-down” state. A few considerations during the buying process can save dozens of hours when it comes times to deploy the product.

Performance Numbers

*The facts are not always
in the figures.*

Customers experience frequent confusion in published performance numbers. Every vendor offers some level of measurement as to how their product performs however the substance of the numbers and how they are obtained can be relevant.

It is impossible to ascertain the impact of a UTM product via a single number. Like the automotive industry, customers have various requirements for speed, reliability, handling, and safety. Many of the figures that are quoted on various performance datasheets and overviews are not so much incorrect as they are reflecting the best possible case in categories that are listed. If one looks up a specifications sheet on a UTM device in consideration and sees “SMTP Email

Throughput” with just a figure of 120,000 messages per hour, it is important to know that factors can impact this figure, depending on parameters like the size of each message being scanned, the time span during which the messages are sent and received, and at what point during filtering a message is rejected or accepted. As sophisticated Antispam methods are rejecting many spam-emails even before they are reaching the email content scanners, the number of mails passing all filtering components could go down to a fraction of the total emails “seen” by the UTM device. Hence advertised throughput numbers might vary significantly.

Furthermore, if given the same solution in two test cases, there will be a massive throughput variance if the first solution tests Email Filtering with all scanning options enabled, and the second has only a single option turned on, thus asking “less” of the system as it scans each message. Combine this type of feature-specific configuration with the other things that can be asked of a UTM such as VPN or Web Filtering, and many combinations which can cause variations in the performance charts are possible.

Conclusion

Choose a solution that solves your problems.

It is both a positive and a negative that the above statements merely start to scratch the surface of the choices that customers face when choosing a Unified Threat Management product. The sheer amount of vendors in this space, combined with the amount of products and features offered, and the system by which they are delivered and deployed to the target network is quite overwhelming to all but the most seasoned professionals in the security market. However, this same amount of choice allows for educated buyers to select a product that best fits both their needs and budget, provided they ask the right questions to the right vendor. Many customers are overwhelmed by the UTM offerings, technical terms, promises and capabilities, and stray from the key requirement, which is to focus on the problem. Identify what a UTM product needs to do in order to meet expectations, and then seek to solve that problem with the best solution at the best price available.

Do not be confused by marketing terms or performance numbers. Ensure that you have completely understood the licensing scheme and there are upgrade options available so that the most can be made from an investment in a UTM in the months and years to come. Of critical importance is to focus on individual offerings in the UTM portfolio and ensure they contain the right amount of feature richness and Depth of Field to provide a solution to the problems that are faced, not just enough implementation to satisfy a feature checkbox on a comparison or requirements chart. Finally, spending just a few minutes with

the actual solution in order to get a feel for the management interface, how it is laid out, and how it performs will help immensely in the process.

*Astaro's UTM offerings fit
all your needs*

One vendor that strives endlessly to simplify UTM selection is Astaro Corporation. Astaro has been producing their solution for 8 years and offers the UTM solution Astaro Security Gateway (ASG) and a range of complementary products to meet all your network security needs. Astaro manages to deliver every feature on every platform, and with all but a single model, provides truly unlimited licensing on all hardware appliances. An Astaro appliance can therefore be deployed in any network while allowing the administrator to change its role over time as more solutions can be removed from the network and replaced by Astaro Security Gateway functionality. The product has been designed from the ground up with the administrator and their users in mind, to provide needed functionality and features with a minimal level of security expertise. Upon first login to the product, the sleek and modern browser-based GUI puts essential functions directly in front of the administrator and allows security needs to be met smoothly and be further supplemented with more advanced features as the low learning curve is mastered. Astaro's approach of including more value that has been directly developed in response to the feedback of its partners and customers sets it apart from the competition. With ASG administrators can truly deploy powerful features in just a few clicks without spending weeks learning the solution and figuring out how to best use it. Available as both a hardware or software appliance, the product is also flexible enough to be deployed on a virtual platform such as VMWare. This is perfect for companies who are standardized on virtualization technology or wish to evaluate ASG in this manner. Astaro further stands apart from others in the security space by taking all of the functionality of its ASG product and giving the entire product away free for home use with a 10-IP license. Users are encouraged to download the ISO from the Astaro website and install it on their hardware of choice, and enjoy all enterprise offerings (including SSL VPN clients) to protect their home networks from viruses and spyware, protect children from inappropriate content, stop spam messages, and build VPN tunnels to any solution.

*The next generation of
UTM is already here*

Astaro has been so successful of meeting the needs of the market that it was used as inspiration for the new eXtensible Threat Management security platform (XTM), a new market segment created and defined by analyst firm IDC. According to IDC, XTM platforms extend themselves beyond the influx of UTM security solutions by bolstering their product with better management and network security features along with features that are designed to protect a company against the latest in emerging threats. XTM appliances seek to sepa-

rate themselves from everyday UTM solutions by offering more high-end functionality and features with an astonishing degree of usability by the SMB market.

For an overview of Astaro and its line of products, visit www.astaro.com, or download your evaluation or home use license at www.astaro.com/download. You can see the Astaro product line in action via the popular online demos at www.astaro.com/demo.

Contact



www.astaro.com

Europe, Middle East, Africa

Astaro AG
Amalienbadstrasse 36
76227 Karlsruhe Germany
T: +49 721 255 16 0
F: +49 721 255 16 200
emea@astaro.com

The Americas

Astaro Corporation
3 New England Executive
Park
Burlington, MA 01803
USA
T: +1 781 345 5000
F: +1 781 345 5100
americas@astaro.com

Asia Pacific Region

Astaro K.K.
12/F Ark Mori Building
1-12-32 Akasaka Minato-ku
Tokio 107-6012, Japan
T: +81 3 4360 8350
apac@astaro.com

This document may not be copied or distributed by any means, electronically or mechanically, in whole or in part, for any reason, without the express written permission of Astaro AG.

© 2008 Astaro AG. All rights reserved. Astaro Security Gateway, Astaro Command Center and WebAdmin are trademarks of Astaro AG. All further trademarks are the property of their respective owners. No guarantee is given for the correctness of the information contained in this document.