

The Unified Approach to Network Security: End of the Multiple Solutions Era

Lost in the Maze of Solutions.....	2
Threat and Security - Cat and Mouse Game	2
Multiple Solutions: One Threat Leads to Another	2
Multiple Solutions Multiplied the Problems	3
A Logical Progression: Unified Threat Management Solution	3
Identity Based UTM: The Solution	4
Conclusion.....	5

Lost in the Maze of Solutions

One fine day, you receive a call from your office informing that a part of your network is down. You, as a system administrator, are supposed to find what happened, when it happened and how it did happen. If you are able to answer all these questions, you are supposed to take steps to prevent future catastrophes. At this precise moment, what flashes in your mind? Most probably, you will visualize an array of boxes, neatly labeled: Firewall, Gateway Anti-virus, Anti-spam & Anti-Spyware, Intrusion Detection and Prevention, Content Filtering and VPN; all sitting in a row with cables worming in and out of them. You will visualize yourself lost in this maze, looking at various reports and trying to first find, what has “actually happened”. Pity, you have not yet upgraded to UTM.

The sole purpose of this paper is to disentangle you from all this cables and the related visuals. Next time you think of your network security appliance, you might just see a single, silent box sitting and working proficiently; of course, sans the panic call.

Threat and Security - Cat and Mouse Game

In absence of threat, there is no need of security; both co-exist. Whatever means you resort to, ultimately, it is security that takes precedence over every other aspect in a network. The advent of computer networks also heralded the appearance of security appliances. It started with firewalls, which lead to desktop anti-virus solutions and gateway anti-virus, and has recently seen the advent of intrusion detection and prevention (IDP) solutions. Early solutions were software specific, but dedicated hardware coupled with software and an underlying OS has recently surfaced.

All the advances in the security appliances have been primarily goaded by increasing level of threats. Threats that started as viruses, now have graduated into a full blown, blended threats, which may consist of a mail based trojan, that hold a backdoor open for a hacker to get in and plunder the network; or a dissatisfied employee, who is out to get you; or a “non-techi” person, who unwittingly falls prey to social engineering.

To catch the mouse – threat, the cat – security solution, has to learn the tricks of the trade and outsmart the mouse. Remember, the mouse - threat is persistent and always present; the moment the guard is down, the threat triumphs. As an answer to all these ailments, small and medium size companies and organizations, started to deploy multiple solutions. It started with firewall, which reigned supreme till late 90s; then gateway anti-virus solutions came which was followed by anti-spam and content filtering. Then IDP and VPN solutions materialized.

Multiple Solutions: One Threat Leads to Another

There is one other catch, a major one; blended threat cannot be tackled by one solution alone. A blended threat was not just a hobbyist or a lime light savvy kid looking for a few moments of glory. According to IDC, a leading global analyst group, the perpetrators of malware have become more focused and are gunning for quick and huge financial gains. So any one solution proves to be highly insufficient to protect your network.

Let us look at a cross section of some threats and the solutions required for them.

Security Threat	Type of Solution
Virus	Anti-virus
Trojan	Firewall, Anti-virus, IDP
Worm	Firewall, Anti-virus, IDP
Spam	Anti-spam
Spyware / Adware	Spyware Blocker
Unrestricted Surfing	Firewall, Content Filtering
Instant Messaging	Firewall, Content Filtering
OS Vulnerability	Firewall, Content Filtering, IDP
Rogue Intruders	Firewall, IDP
Hackers	Firewall, IDP
Internal Security Breach	Firewall, IDP
Remote Connectivity	VPN, Firewall, Anti-virus, IDP

In other words, for comprehensive security, multiple solutions were required. However, stacking up all the boxes did not prove to be a panacea.

Multiple Solutions Multiplied the Problems

Multiple solutions, often failed to rectify the problem. Moreover, they ushered in a separate set of problems that were unique to them. Every solution would usually be of a different make and breed with no interoperability. To be effective, every solution needed to be fine tuned by an expert. Every solution needed to keep a tab on the multiple parameters. Often, these parameters are duplicated for different solutions, so multiple monitoring of the same parameters causes large number of redundancies and adds to the confusion.

In spite of these redundancies, the solutions often left gaping holes in the security. Every solution needed to be monitored separately and in case of a timely detection of an anomaly, necessary precaution ought to be taken. If a blended threat was detected, multiple solutions should be ready to counter it.

All solutions would have their own native database of signatures and will need updates from time to time. The system administrator should monitor the status of update process. To top it all, as every solution being of a different make and breed, will have a separate annual maintenance contracts to keep them alive and kicking. Last but not the least, every solution will have capital expenditure of its own. In other words, while network security might remain an illusion, multiple solutions may harbor a totally new set of problems that might prove to be a drain to the organization.

A Logical Progression: Unified Threat Management Solution

Unified Threat Management or UTM was defined in 2004 by the leading, global analyst group, IDC, as THE “all in one” security appliance for the small to medium business and branch office user market segments. IDC believes that, over the next five years, the

revenue generated by the sale of UTM appliances will exceed that of standard firewall/VPNs, effectively replacing these products.

Overall, IDC forecasts that the threat management security appliance market will grow at a combined annual growth rate of 17% between 2003 and 2008. This translates into a total market of \$3.45 billion so the rising level of confidence indicates that the UTM appliance is the future of security.

Initially, according to IDC, a UTM appliance must consist of, in order to be regarded as such; first, it must have a real operating system as its base and an installation process that minimizes human intervention. The appliance must contain the ability to perform network firewalling, network intrusion detection and prevention (IDP) and gateway antivirus (AV). All of the capabilities in the appliance need not be utilized, but the functions must exist inherently in the appliance. A UTM appliance may also include other features such as security management and policy management by group or user. The existing UTM appliances have added anti-spam, VPN and, at times, Multi-Link Module and Load Balancing, to the bevy of services offered.

A single UTM appliance makes it very easy to manage your security strategy, with just one device to worry about, one source of support and a single way to set-up and maintain every aspect of your security solution. So not only is it a cost-effective purchase in the first place, but day-to-day "running costs" will also be lowered to the point of being insignificant. Moreover, a UTM is a single console that provides a complete data of the network traffic patterns and user behavior. It is a Unified Threat Management Solution. Yet, all is not well. Most of the UTM appliances focus only on IP address based reporting and controls, while the actual user stays invisible. This approach is self-defeating.

During 2005, financial services giant Citigroup and media powerhouse Time Warner had sensitive data swiped from their "supposedly secure" databases. Smaller companies like Retailer DSW Shoe Warehouse and credit card processor CardSystems, were victims of cyber break-ins which lead to their bankruptcy. The most disturbing threat that came to light was the fact that an insider was a party to these thefts. These internal threats are likely to grow in 2006, forcing more companies to monitor the information accessed and distributed by employees¹. This major flaw often goes undetected in traditional UTM solutions.

Identity Based UTM: The Solution

Traditionally, all the UTM solutions, as they deal with networks, are bound to TCP/IP protocol stack. The protocol stack only recognizes the IP address of a machine on the network, not the actual user. The lacuna here lies in the fact that a machine is just a tool. It is ultimately the user operating on the machine that is more important. In the coming times the internal threat will gain precedence over the external threat, and in such a scenario, user identity-based UTM solutions will be a step ahead of the pack.

In an identity based UTM the access policies are connected not only to an IP address, but also to a user name or a group of users. So the decision, either to allow or deny, will be based on a user's access right. The access rights will depend on the user or the group of users business needs.

Unless a UTM is able to recognize the user and then provide him/her selective access according to his/her profile, any UTM solution is incomplete. An Identity Based UTM should not only be able to authenticate the valid users, but also should be powerful

¹ <http://www.redherring.com/Article.aspx?a=13472&hed=Q%26amp%3bA%3a+Security+Wonk+Dan+Verton+>

enough to apply customized policies on either individual users or a group of users. This will do away with the anonymity that exists on the internal network. Once the anonymity is lifted, it will promote responsible behavior on the part of the user too. This is a completely new approach from the traditional network security solutions, which promotes user-centric network security rather than IP address based security.

Conclusion

A security solution is as good as it is configured. A UTM can prove to be a very powerful solution if it is configured properly. If the major problem of multiple solutions was their maintainability and operability, a UTM can rectify it by providing a single window to the complete network security. Simultaneously, an IP address based reporting can take away all the advantages that a UTM is likely to deliver. It is ultimately the user that operates the machine.

Blurb Quotes

1. All the advances in the security appliances have been primarily goaded by increasing level of threats. Threats that started as viruses, now have graduated into a full blown, blended threats
2. Blended threat cannot be tackled by one solution alone. The perpetrators of malware have become more focused and are gunning for quick and huge financial gains.
3. Multiple solutions, often failed to rectify the problem. Moreover, they ushered in a separate set of problems that were unique to them.
4. "Threat management security appliance market will grow at a combined annual growth rate of 17% between 2003 and 2008. This translates into a total market of \$3.45 billion." - IDC
5. Most of the UTM appliances focus only on IP address based reporting and controls, while the actual user stays invisible. This approach is self-defeating.
6. Unless an UTM is able to recognize the user and then provide him/her selective access according to his/her profile, any UTM is incomplete.
7. Unified Threat Management or UTM was defined in 2004 by the leading, global analyst group, IDC, as THE "all in one" security appliance for the small to medium business and branch office user market segments. IDC believes that, over the next five years, the revenue generated by the sale of UTM appliances will exceed that of standard firewall/VPNs, effectively replacing these products.
8. An Identity Based UTM provides user-specific security, apart from the IP address based security. This added advantage largely simplifies and quickens the decision-making process.