Network Security Systems Using UTM Technology

Mr. Chetan H. Patil[1],Mr. Jaiprakash Shimpi[2], Mr. Kaustubh Markande[3],Mr.Vikram Patil[4]
Assistant Professor[1], Assistant Professor[2], Assistant Professor[3], Assistant Professor[4]
S.G.D.C.O.E Jalgaon[1], S.G.D.C.O.E Jalgaon[2] ,S.G.D.C.O.E Jalgaon[3], S.G.D.C.O.E Jalgaon[4]

*Abstract:***Unified Threat Management (UTM) is an emerging trend in the firewall security market. It is then evolution of the traditional firewall that not only guards against intrusion but performs content filtering, spam filtering, intrusion detection and anti-virus duties traditionally handled by multiple systems. UTM firewall is the only firewall that embeds user identity in firewall rule matching criteria, enabling enterprises to configure policies and identify users directly by the username rather than through IP addresses. It is a powerful hardware firewall that provides stateful and deep packet inspection thereby protecting enterprises from IP spoofing attacks, access control, user authentication, network and application-level protection. This paper will explore the emergence of UTM working criteria, functions and prove how it is better in comparison with the ordinary firewall and VPN.**

*Index Terms:***Unified Threat Management, Network Address Translation, Intrusion Detection (or Prevention) System**

1. INTRODUCTION

The goal of UTM is to simplify the overall security solution despite the growing scope and rising complexity of the security problem. The most apparent aspect of this simplification is the physical consolidation of point products into a single technology, hence the term unified threat management. As the hardware powering today's enterprise firewalls became more robust it became viable to add functions that were traditionally off the technology right into the firewall.

2. COMPONENTS OF UTM TECHNOLOGY

IDC has defined what a UTM technology must consist of to be regarded as such. First, it process that requires a minimum of human intervention. The technology must have the ability to perform network fire walling, intrusion detection and prevention (IDS/IPS) and gateway antivirus(AV). All operations need not be utilized, but the functions must exist in the technology. A UTM technology may also include other features such as security management and policy management by group or user.

3.ADVANTAGES OF USING A UTM TOOL

Why are people buying threat management security technologies when many excellent software-based security applications are already on the market? Simply because convenience and ease of installation are the key advantages of threat management security technologies. The growth of the threat management security technology market is largely due to following reasons:

3.1 Reduced complexity:

The all-in-one approach simplifies product selection, product integration, and ongoing support.

3.2 Easy to deploy:

Customers can easily install and maintain the products. Increasingly, this process is seeing remotely.

3.3 Synergies with high-end software solutions:

Technologies are used in remote sites where anenterprise does not have security professionals on the ground. A plug-and-play technology can be installed and managed remotely. This management is synergistic with large, centralized software-based firewalls.

3.4 Low operator interaction:

Users have a tendency to play with things, and the black technology approach limits the 'damage' users can do. This reduces maintenance calls and improves security.

3.5 Easy Troubleshooting:

When a technology fails, it is easier to swap it out by even a non-technical person than troubleshoot. This process gets the node back online quicker, and is especially important for remote offices.

4. MARKET FOR UTM TECHNOLOGY

Overall, IDC forecasts that the threat management security technology market will grow at a combined annual growth rate of 17 percent between 2003 and 2008. This translates into a global market of $3.45 billion. Technologies have become popular by being a simple means of delivering security software..

5.DIFFERENT CONSIDERATIONS TO JUDGE A UTM TECHNOLOGY.

Here are five simple considerations when evaluating the pros and cons of buying a UTM technology:

- Make sure there are no holes in your security set-up. A UTM technology provides blanket security cover for Internet-based threats
- In order to fully provide unified threat management, the technology must include all the important security elements such as firewall, AV filter, anti-spam filter, URL filter and IDS/IPS
- The UTM technology must be foolproof; update important elements such as AV filter databases and should be easy to use
- A UTM technology should work 24x7x365—forming permanent, transparent protection for your company network
- It should be affordable and comprehensive

5.1 Which companies offer UTM solutions in India?

Fortinet, NetScreen (acquired by Juniper Networks), Symantec, NetScaler, WatchGuard Technologies and Elitecore Technologies.

6. FIREWALLS AND TYPES OF THREATS

Unified threat management (UTM) is used to describe network firewalls that have many features in one technology, including e-mail spam filtering, anti-virus capability, an intrusion detection (or prevention) system (IDS or IPS), and World Wide Web content filtering, along with the traditional activities of a firewall. These are application layer firewalls that use proxies to process and forward all incoming traffic, though they can still frequently work in a transparent mode that disguises this fact However, if this uses too much processor time, the higher-level inspection can be disabled so that the firewall functions like a much simpler network address translation (NAT) gateway. A firewall is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria. A firewall is a dedicated technology, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules. Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance. Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgement to the sender). In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines. On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and trojans. Malware is short for “malicious software” and is defined as any program or file that is harmful to the computer or user. Malware includes viruses, worms, Trojan horses, logic bombs, spyware/adware, etc. An effective security strategy will address malware in two primary ways:

1. Through an acceptable use policy describing appropriate use of Internet/email
2. Through the careful implementation of antivirus software (or other similar software, i.e. anti spyware, etc)

6.1 Defintion Of Threat

Threat means declaration of an intention to hurt or punish by person or thing as a likely cause of harm . Current trends are:

6.1.1 speed and sophistication of cyber–attacks is dramatically increasing Blended threats.

6.1.2 hybrid attacks and automated tools have become popular and getting them is easy.

6.1.3 criticalinfrastructure is dependent on internet and threats are progressively more unpredictable.

Attacker is no longer mere individuals and attacks executed as Joint ventures among professional programmers with access to greater pooled resources and also Consortiums dedicated to the creation and distribution of malicious software intended to steal money from individuals.
Some of motives are:

a. Regional and Targeted Attacks Replace Global Outbreaks to escape attention
b. Attacks driven by financial theft - Money still the main driver for malware authors
c. Deployed in order to steal confidential information from specific companies
d. Identity theft. Small corporations and key Individuals are victims.
e. Attack vectors are Spear phishing exploiting individuals' trust, Community-forming malware-bot, and new hybrid combinations - spy phishing
Insiders acting as initiators themselves or as conduits for other attacks. User Ignorance, Malicious Intent, Intentional security breaches, disguised employees are also included. Insider threats can lead to more damage because Employees carry valid authorization and are privy to the organization's vulnerabilities Dishonest insiders' can exploit an organization's vulnerabilities to commit identity fraud and expose confidential information for personal gain or as part of a larger crime ring. Insider attacks can be more difficult to detect than external penetration attempts, such undetected attacks can cause serious harm, includinglegal liability for compromised data, loss of competitive position and disrupted business operations.

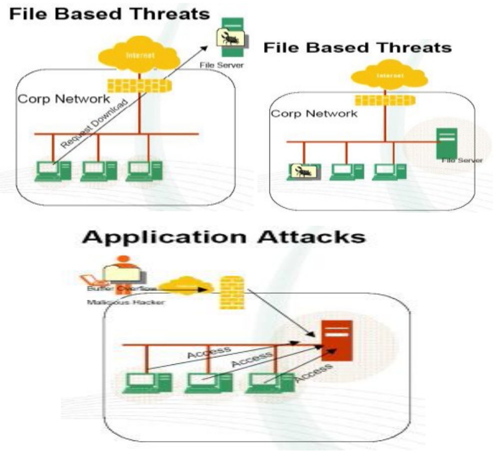


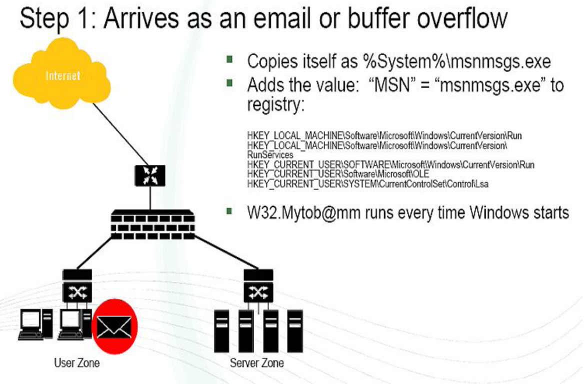
Fig.1 how the viruses enter by infected server to new user

6.2 Threat Penetration:

It is Both External and Internal. Opening up of the network to external users like Partners, Suppliers,Customers, Delegates, Officials.Internal users communicating over multiple protocols. The Problem with Traditional Security Solutions are that they are focused on protection against external threats only so insider threat protection not given due importance. They are ineffective against blended threats. The users are known by static IP addresses. So lack of security in dynamic IP environments. Lack of security for shared desktops, inability to know who is doing what in the network. Types of threatsare viruses, worm, Spam, spyware, phishing, hacking.

6.2.1 Viruses

Self-replicating code maliciously introduced into a computer program and intended to corrupt the system or destroy data. When user downloading data from internet viruses and malicious code also download with that data and infection spread out by peer to peer, instant messaging apps, shareware sites, compromised servers, legitimate corporations, web based email. Threats pass through stateful packet inspection and once inside the network, other are easily affected. Viruses can be uploaded to network drives also. Once on the network drive users can be affected. Nimda was a virus that attacked file servers and opened up a hole to allow a hacker to obtain control of the server. A computer virus designed to steal valuable information like passwords spread Friday through a new technique that converted popular Web sites into virus transmitters. Attacker sends malicious code through a buffer overflow so executes program instructions to the victim's computer for execution. It can also be used as denial-of-service attack, causing the computer to crash. Once the server is infected new users who access server get infected also.


Step 1: Arrives as an email or buffer overflow

- Copies itself as %System%\msnmsgs.exe
- Adds the value: "MSN" = "msnmsgs.exe" to registry:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
RunServices
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\OLE
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\Lsa
```

- W32.Mytob@mm runs every time Windows starts

Fig.2 Shows worm arrives as an email or buffer overflow

6.2.2*Worm*

Self-contained programs that break into a system via remotely exploitable security damage. As shown in Fig.2 MyTob Worm Discovered on February26, 2005. W32.Mytob.@mm is a mass-mailing worm that propagates via network shares and through email. Uses its own SMTP engine to send an email to local email addressed.Exploits the Microsoft windows LSASS remote buffer overflow and RPC/Dcom. In this way it opens a back door into the affected computer and self protects by redirecting AV updates to local computer.

6.2.3 Spam

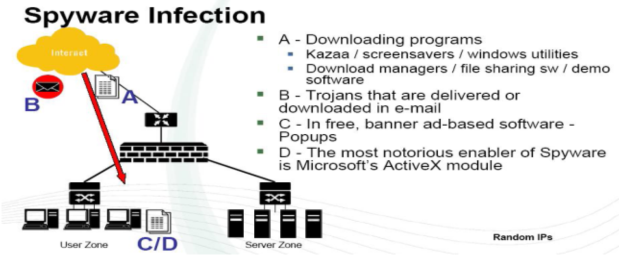
Any software designed to extract email addresses from web sites and other sources, efficiently send unsolicited (and perhaps untraceable) mail to these addresses. As shown in fig.3 Email virus considering as spam example in which Sobig is there it is high-risk massmailing worm. It arrives as an e-mail attachment. When user executed e-mails itself all address book entries. Sobig-F is a Trojen Horse which makes our PC turns into ZOMBIEE, means it controls our PC why virus code writer. E-mail has become the primary means for distributing threats. Trojans are easy to deliver and install. HTML viruses (no user intervention) with web mail. E-mails with attachments containing macros, VB scripts, java Scripts and html scripts

6.2.4 Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

6.2.5 Hacking

Gaining unauthorized access to data in a computer or in a network. Spyware/Adware is type of hacking. Spyware is any software that utilizes a computer's Internet access without the host's knowledge or explicit permission. According to certain experts, approximately 90% of computers have some form of spyware. Aids in gathering information by Browsing habits (sites visited, links clicked, etc.) ,Data entered into forms (including account names, passwords, text of web forms and web-based email, etc.) and Key stokes and work habits.



- A - Downloading programs
  - Kazaa / screensavers / windows utilities
  - Download managers / file sharing sw / demo software
- B - Trojans that are delivered or downloaded in e-mail
- C - In free, banner ad-based software - Popups
- D - The most notorious enabler of Spyware is Microsoft's ActiveX module

Fig.3 Spyware infection by downloadingprograms or emails

6.3EXTERNAL THREAT-SPEAR PHISHING

It is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email or instant messaging, and often directs users to enter details at a website. Phishing , derived or coined from "password harvesting fishing" Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose URL and look and feel are almost identical to the legitimate one. Even when using SSL with strong cryptography for server authentication it is practically difficult to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies A phishing technique was described in detail as early as 1987, in a paper and presentation delivered to the International HP Users Group, Interex. 57 million U.S. Internet users receive at least one phishing e-mail, and as many as 1.7 million give personal information to the attackers.

6.4INTERNAL THREAT USER IGNORANCE

When person downloading software or any document malware enters his computer. The mal-ware significantly slows down his computer. The mal-ware has made his computer a zombie and is made to perform malicious activities. Person is not aware of it.

7. UTM TECHNOLOGY: IDENTITY BASED UNIFIEDTHREAT MANAGEMENT

As you have seen in Fig.4 Before UTM Deployment Multi- layered approach to complete content protection in which firewall defend against intrusions, Antivirus gateway protect email from virus, IPS/DPS protect against malicious, Anti Spam reduce unwanted email, web filters eliminated unproductive web-browsing and VPN delivering secure remote access. So it provides comprehensive security approach and minimizes downtime from individual threats. But some disadvantages are also there like it requires multiple products as we have seen in Fig.4 also it increases network complexity and operational cost and does not defend against blended threats. So we are switch over to unified threat management security that we have seen in Fig.4 after UTM Deployment the Identity based UTM solution that offers Integrated Internet Security with fine granularity through its unique identity - based policies. So in single technology user can get all benefits so in previous security protection with ordinary technology whatever disadvantages are overcome through the use of UTM, more details of UTM benefits.It reduces network complexity and corporation cost and also single technology so no more products are requires.

8. UTM TECHNOLOGY: IDENTITY BASED SECURITY

UTM gives Stamps User Identity it means gives information who is doing what on particular terminal in network. It means allows granular controls with unified policy management through a single window so prevent unnecessary traffic. So whatever unhealthy traffic problem arises in previous one is short out here with the use of UTM technology. It ensures business flexibility based on work profile with the protection in DHCP and Wi-Fi environment with all functionality in single technology. So we can say that complete visibility across corporate and branch offices providing with UTM technology. Users can carry their access rights anywhere in the network with single sign on. From this all above points we can say that UTM technology based security is much useful and flexible as compare to previous one.

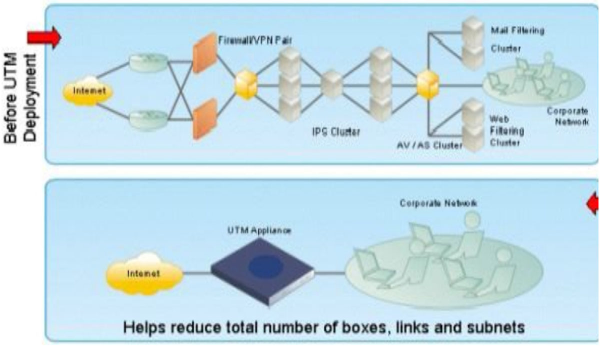


Fig.4 Network overview before UTM deployment and after UTM deployment reducing use of no. OfGateways and firewall devices etc. with the use of single Unified Threat Management technology.

9. UTM WORKING AND BENEFITS

Unified Threat Management works in a 3 level.
(1) stateful inspection firewall – inspects packets headers only but what contents inside
(2) deep packet inspection – perform packet by packet inspection but fragmentation can hide malicious content true security relies on multiple security layers
(3) complete content inspection –reassemble packets into contents and compare against disallowed content and attack lists
(4) complete content protection required enormous processing power so provide complete content protection.
By checking every content. Unified Threat Management gives protections against Blended threats as we discussed earlier. It reduces capital and operating expenses because no need to involve more users for maintain security because UTM means all in one so no need to purchase other any devices. It helps users by creating custom policies to battle Zero-day threats .we can give this type of security also in ordinary network with the use of different firewalls, anti virus software etc. but it has also complexity as we have seen in Fig.4 before UTM deployment. While after UTM deployment in network it offers all protections required are in one single technology. So no more complexity generates in network. With single technology utilization user can also get freedom from Multiple Vendors, from Multiple Technologies and from Registrations also. That is the biggest benefit as per user point of view. UTM technology is easy to deploy manage and monitor and also save user time because in previous one user have to monitor and manage no. Of devices .so for user to handle to network easily is possible. It gives also Centralized On- Technology Reporting. In next point we will see how UTM technologies are more demanded in market and take place of other ordinary network devices. Because it more affordable, powerful, and simple as compare to other security mechanism used by users.

10. COMPARISON

As shown in Fig. 5 we can see how UTM Market Growth is increase and people are diverting to this threat management technology and also conclude that how UTM take place of other technologies from above graph from 2003 to 2008. Comparing UTM with Secure Content Management (SCN) Technologies, V Voip, Wireless, and FW/VPN. The only reason why it is more demanded day-by-day in market is that it is easy to install, use and manage, it is in total cost of ownership means rather than to purchase more devices and manage them, install them as we have seen in Fig. 4

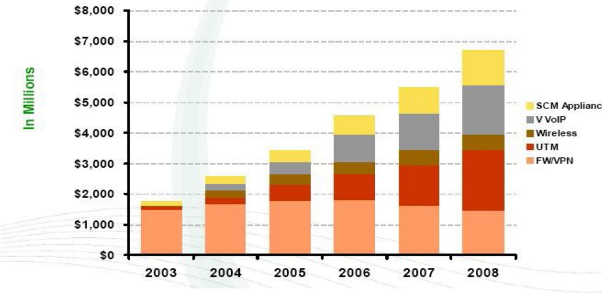


Fig.5 Comparison of the Market Growth of Unified Threat management

CONCLUSION

Unified threat management spawned a new era of IT security. The promise of these integrated security technologies proved to be an exceptional and efficient way of securing commercial networks. However, businesses today face an inflection point, dictated by changing market trends and new technologies that demand more of today's UTM. Hence the need is for extensible threat management (XTM) solutions, the next generation of UTM technologies.

REFERENCES

[1] Yaxuan Qi, Baohua Yang, Bo Xu and Jun Li, “Towards System-level Optimization for High Performance Unified Threat Management”, Proc. of Third International Conference on Networking and Services (ICNS'07), IEEE, 2007.

[2] P. Gupta and N. McKewon, “Algorithms for Packet Classification,” *IEEE Network*, March/April, 2001

[3] Miguel Vargas Martin, Patrick C.K. Hung, “Towards a Security policy for Voip applications”, IEEE conference, May 2005.

[4] *S Viveros*, “The economic impact of malicious code in Wireless mobile networks” , IEE conference ,2003.

[5] *George Lawton*, “Web 2.0 Creates Security Challenges” Technology News, published by IEE Computer Society, October 2007.

[6] Michael B. Greenwald, Sandeep K. Singhal, Jonathan R. Stone, David R. Cheriton, “Designing an Academic Firewall: Policy,Practice, and Experience With SURF” , Published in 1996 Internet Society Symposium on Network and Distributed SystemSecurity (SNDSS).

[7] SenyKamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum, and Michael Frantzen, “Analysis of Vulnerabilities in Internet Firewalls”, Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University.

[8] Michael R. Lyu and Lorrien K. Y. Lau, “Firewall Security: Policies, Testing and Performance Evaluation”, Department of Computer Science and Engineering.

[9] Gregory P. Schaffer, “Worms and Viruses and Botnets Oh My! Rational Responses to Emerging Internet Threats “, Published by the IEEE, Computer Society , 2006.