Unified Threat Management

Vinit Agham

Assistant Professor, Computer Engineering department, R C Patel institute of technology, Shirpur, Maharashtra, India

---

Abstract - ***Unified Threat Management (UTM) or unified security management (USM) is an emergent trend in the firewall security market. It is a solution in the network security industries. It is the advancement of the traditional firewall capable not only guarding against intrusion but also does content filtering, spam filtering, intrusion detection load balancing, data leak prevention and anti-virus duties traditionally handled by multiple systems. UTM firewall is only the firewall that inserts user identity in firewall rule matching criteria, allowing 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 development of UTM working criteria, functions and prove how it is better in comparison with the ordinary firewall and VPN.***

Key Words: *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 [1]. 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. ADVANTAGES OF USING A UTM TOOL

Peoples approach towards threat management security technologies simply because convenience and ease of installation of UTM. The advantages of the threat management security technology are:

1. Reduced complexity: The all-in-one approach makes simpler product selection, product integration, and ongoing support.

2. Easy to deploy: Customers can easily install and maintain the products. Increasingly, this process can be done remotely.

3. Synergies with high-end software solutions: Working together with high-end software solutions: Technologies are used in remote sites where an enterprise does not have security professionals on the ground. A plug-and-play technology can be installed and managed remotely. This is interactive with large, centralized firewalls.

4. Low operator interaction: Users have a tendency to play with things, and the black technology approach limits the number of damages that users can do. This reduces maintenance and improves security.

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 solutions online quicker, and is especially important for remote offices.

3. MARKET FOR UTM TECHNOLOGY

The IDC Press Release "The growth of UTM appliances will be driven by demand in the midmarket for new software features, virtual applications, cloud services, and vulnerabilities associated with internet of things," says Jiaqi Sun, a research analyst at IDC South Africa. "The ultimate objective of security technology development is to protect data or information assets – in other words, minimizing data loss within corporate networks if all layers of an enterprise security system fail." IDC believes that, over the next five years, the revenue generated by the sale of UTM technologies will exceed that of standard firewall/VPNs, effectively replacing these products. DC forecasts that the threat management security technology market will grow at a combined annual growth rate of 17 percent from 2003 to 2008. The technologies are becoming more popular by being a simple means of delivering security software.

3.1 How do you judge a UTM technology?

We have to consider some issues when buying a UTM technology:

1. Make sure there are no holes in your security set-up. A UTM technology provides blanket security cover for Internet-based threats.

2. 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.

3. UTM technology must be foolproof; update important elements such as AV filter databases and should be easy to use.

4. UTM technology should work 24x7x365—forming permanent, transparent protection for your company network

5. It should be affordable and comprehensive.

4. FIREWALLS AND TYPES OF THREATS

Unified threat management (UTM) is described as one technology many features 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. 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 [8]. 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 [6]. 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 [7]. 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.

4.1 Definition of Threat

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

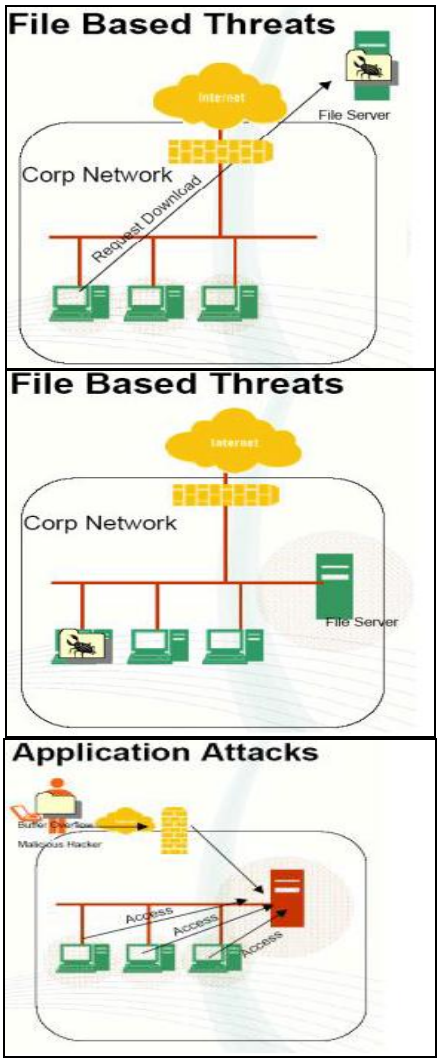


Fig -1: How the viruses enter by infected server to new user (File based threats and Application based threats)

There are some current trends in security from threats like speed and sophistication of cyber–attacks is dramatically increasing Blended threats, Hybrid attacks and automated tools have become popular and getting them is easy, critical infrastructure is dependent on

internet, security problems cost time, money and pain 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 the causes are:

1. Regional and Targeted Attacks Replace Global Outbreaks to escape attention.
2. Attacks driven by financial theft - Money still the main driver for malware authors.
3. Deployed in order to steal confidential information from specific companies.
4. Identity theft. Small corporations and key Individuals are victims.
5. Attack vectors are Spear phishing exploiting individuals trust, Community-forming malware bot, and new hybrid combinations - spy phishing.

Insiders are acting as initiators for themselves or as a conduit for other attacks. User Ignorance, Malicious Intent, Intentional security breaches, disguised employees is 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, including legal liability for compromised data, loss of competitive position and disrupted business operations.

4.2 Threat Penetration

It is Both External and Internal. This is nothing but opening up of the network to external users like partners, suppliers, customers, delegates, officials etc. 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 threats are viruses, worm, spam, spyware, phishing, hacking.

4.2.1 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 [4]. Threats pass through 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.

4.2.2 Worms

Worm deliberated as self-contained programs that break into a system via remotely exploitable security damage. As shown in Fig.2 MyTob Worm was discovered on February 26, 2005.

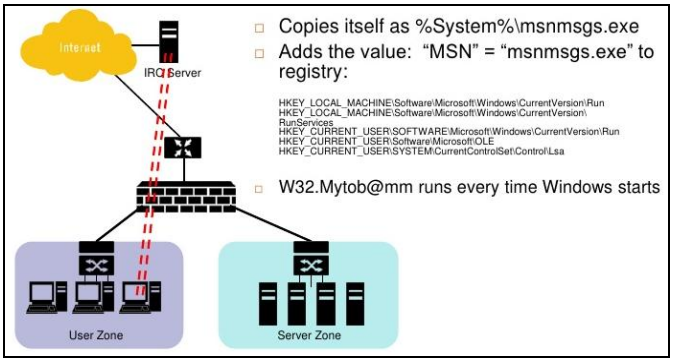


Fig -2: Shows worm arrives as an email or buffer Overflow

"W32.Mytob.@mm" is a mass-mailing worm that propagates via network shares and through email. It uses its own SMTP engine to send an email to local email address. In this way it opens a back door into the affected computer and self protects by redirecting AV updates to local computer.

4.2.3 Spam

Any software designed to extract email addresses from web sites and other sources, efficiently send unsolicited (and perhaps untraceable) mail to these addresses [3]. As shown in Fig.3 Email virus considering as spam in which "Sobig" is there it is high-risk mass mailing 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.

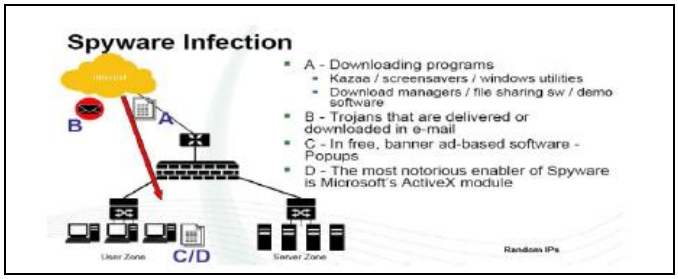


Fig -3: Spyware infection by downloading programs or emails

4.2.4 Phishing

Phishing is any deceptive, online attempt by a third party to obtain confidential information for financial gain. 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.

4.2.5 Hacking

Hacking means the 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 [5]. 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.

4.3 External Threat-Spear Phishing

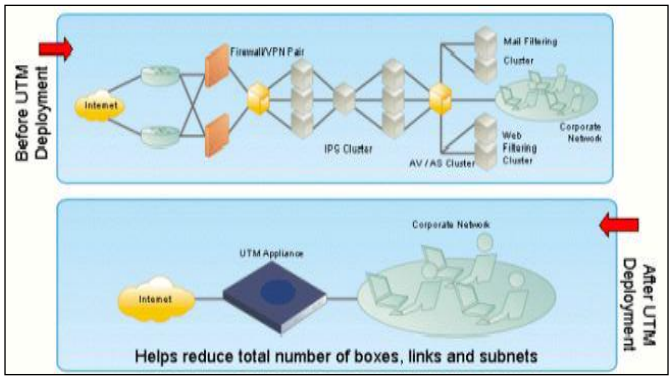
It is an attempt to criminally and fraudulently acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email or instant messaging and often directs users to enter details at a website. Phishing 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.

5. UTM TECHNOLOGY: IDENTITY BASED UNIFIED THREAT 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. 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.

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

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.

6. UTM TECHNOLOGY: IDENTITY BASED SECURITY

UTM gives information that 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. So we can say that UTM technology based security is much useful and flexible as compare to previous one.

7. UTM WORKING AND BENEFITS

Unified Threat Management works in a three levels [1].

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.

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. 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 number of devices. 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.

8. CONCLUSIONS

Unified Threat Management (UTM) reproduced a new era of IT security. The ability 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] J. 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 System Security (SNDSS).

[7] Seny Kamara, 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.