Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 4, April -2015

UTM Secured Network and its Performance

Yoghavel V[1] , Saveetha D[2]

[1]M.Tech student, Department of Information Technology, SRM University
[2]Asst.Professor, Department of Information Technology, SRM University

Abstract - *The era of Internet rules the world today. With the rise in people using Internet influences the increase in security threat and breaches. Preventive and security measures being adopted goes in vein with impact of zero day attacks. It is a great challenge for the users to protect their credential data from the hands of intruders with the attacks growing continually. A traditional firewall or using point solutions such as anti-virus or spy ware will never help us out in securing our network in this crucial scenario. This paper highlights the concept of securing a network using a Unified Threat Management Appliance which is a single component with blended security features and assures to provide a security mechanism that defends the network from threat and testing its performance.*

Keywords-*Threat, Unified Threat Management, Security breach.*

I. INTRODUCTION

Over the past few decades Internet is facing a massive growth. With the emerging services there is an explosive rise in network attacks and data security becomes a question mark. With the continual growth of attacks network monitoring becomes an essential component of computer security to detect and prevent a threat. Just one cannot imagine a life without Internet. People use Internet for banking,shopping, and entertainment with on line transactions, thereby attackers tend to intrude the network so as to gain access over the user credentials. Threat to confidential information makes the usage of Internet to be dreadful.

Threats are the one that affects confidentiality, integrity and availability of information. Threats may be of several forms like viruses, Spam, SQL Injection attack, passwordattack, Denial of Service (DoS) attack, Brute Force attack, session hijacking etc. Threat may exhibit both as inbound and outbound. Many methods are designed and in use to secure the network. Securing a network incorporates monitoring, detecting attacks and mitigating them. Traditional approach of securing a network was to install a firewall so that unauthorized traffic will not be able to enter in the network. Firewall alone was no more able to defend our network and protect it from the hands of outsiders. So there was a need for a system that could withstand to the new attacks growing day by day and protect the network thereby the user credential data are not compromised at any cost and attacks could be mitigated to a larger extent.

II.REVIEW OF LITERATURE

2.1. Evolution of Secure Networking

Before year's together routers known as gateways identified data packets and forwarded to particular destination address. With the rise in technology routers have evolved as specialized hardware capable of delivering high performance traffic. Firewall also evolved under the same iterative fashion, firewall being a step ahead of router is with the ability of packet filtering. Firewalls also had a growth from basic packet inspection to stateful packet inspection and application layer inspection devices.

Then evolved the concept of Virtual Private Network (VPN) which made possible to establish a secure connection over Internet. VPN along with firewall were deployed by many organization and was successful in providing a secured solution, but increase in processing capabilities and the no of users forced for adopting a new technology.

2.2. Common threats in a network

Threats that affects computer security is a computer crime. Computer crime by definition may be stated as "Illegal action which the perpetrator uses special knowledge of computer technology". Threats encountered in our network may be given as follows,

2.2.1. Virus

Virus is the most commonly found threat. It is a small piece of executable code developed by malicious users. It replicates by attaching themselves to a host program. Host program may be executable file, boot sectors, patch files and other third party software running in a system. There are several kind of viruses like stealth virus,boot sector virus, programvirus, multipartitevirus, macrovirus, polymorphism virus etc.

2.2.2. Trojan Horse Program

Trojan Horse Program which appeals to offer a functionality for end user and runs malicious program in background process such as gaining access over victims system,installing a key logger and thereby get credentials like password,deleting files,making the victims system a proxy server and performing illegal financial transactions etc.,There are several kind of Trojan horse program like remote access,data sending,denial of service,proxy,destructive Trojan etc.,

2.2.3.Spyware

Spyware is a malicious software that collects personal information from users like email address,contact information and other user credentials which in turn is sent to attackers and used for marketing,financial crimes and Spam purpose.

2.2.4. Phising

Phising is a form of online theft where the victim is send a mail and he is asked to click on a link. The link redirects to a page that appeals to be a genuine page. The victim will be asked for credentials,which will be used for illegal purpose like gaining access over victim's private network or withdrawing money from the victims account.

2.2.5. Denialof Service

Denial of Service attack is the one where the user does not takes access over the victims system,but can stop a service like access to a website. The attacker sends many no of requests to a particular website,which keeps on waiting for responses and stops accepting new request thereby the website goes down. This is also known as SYN Flood attack.

2.2.6. Password Attacks

Password attack is another major network threat that compromises all the user credentials once achieved. Password is the means through which the system identifies the user. Such passwords can be identified by exhaustive search (Brute Force Attack) or by using rainbow table that consists a list of frequently used password. Password aging,disabling account after specific attempts of entering a wrong password and use of strong password are the ways to mitigate password attacks

III. RELATED WORK

Network security faces a great challenge withstanding against several attacks. New threats arise each and every day,viruses and attacks becomes tedious and complex day by day making network security put to a toss. Added to this there are other burdens like load balancing,network slowdown and trafficking as a result of user activities like social networking,instant messaging that no way helps out with actual work to be done. They not only impacts network bandwidth but also compromises the network security. Restricting network usage to an internal network is not possible,but providing full access over network is a threat to network security. To secure an internal network a choice of stand-alone solutions are used to protect the network against various threats. The point solutions would operate in a same phase and identifies possible threat, thereby providing an enhanced secure network. The table below lists out all possible security threats along with suitable solutions.

Security Threat	Solution
Virus	Anti-Virus
Worm Trojan	Anti-Virus,Firewall, Intrusion Detection and Prevention
Spyware Adware	Spyware Blocker

Spam	Anti-Spam
Unrestricted Surfing Instant Messaging	Content Filtering,Firewall
Hackers,Intruders and Internal Security Breach	Firewall,Intrusion Detection and Prevention
Remote Connectivity	Anti-virus,Virtual Private Network,Firewall,Intrusion Detection and Prevention
OS Vulnerability	Content Filtering,Firewall,Intrusion Detection and Prevention

Table 1. Security Threats and Solution

IV. UNIFIED THREAT MANAGEMENT

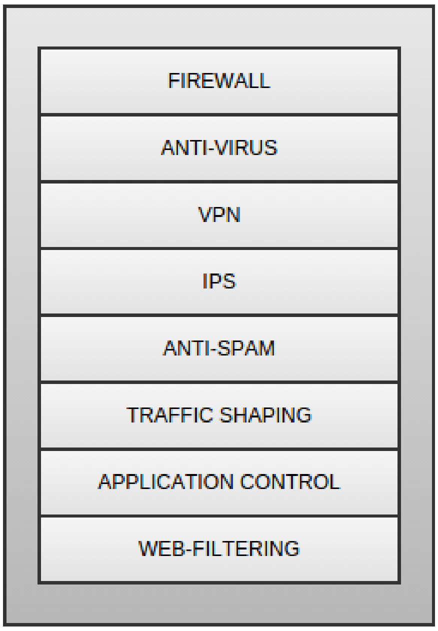
Integrating the point solutions were effective before decades, but it turned out to be a failure with the rise of complex threats in recent years. Compatibility was another issue related in stacking two or more point solutions as they were from different vendors. These point solution proving to be no longer effective led to advent of an integrated entity for providing a secured network known to be as Unified Threat Management Appliance.

4.1. Features of UTM

The primary goal of Unified Threat Management (UTM) is to provide an integrated security solution with reduced cost and complexity. It is a best suited solution for a providing a secured network. Evolving from traditional firewall, Unified Threat Management (UTM) is an entity with security features are Firewall, Virtual Private Network, Anti-Virus, Anti-Spam WebFiltering, Application Control, and Traffic Shaping.

4.2. Types of UTM

Unified Threat Management (UTM) could be constructed in two different ways, first approach is Fully integrated UTM in which one needs to build the complete platform right from the scratch providing the end user a systematic and uniform security solution with user friendly interface. Thereby with an UTM modeled the user can extract best out of it. The second approach is Limited integrated UTM where we have to get license from leading vendors for different technologies and integrating them as a single entity,which make be simple to device out but cannot compete the with performance of UTM shaped up using the first approach.



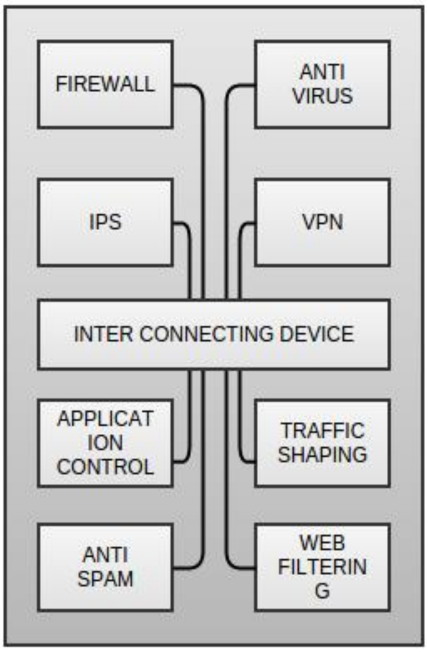


Figure.1.Full Integration **Figure.2. Limited Integration**

4.3. Construction of a secure UTM system

For an enhanced secured solution,we propose a new secure Unified Threat Management System to meet the challenging demands of fast emerging technologies. The high level design of Unified Threat Management (UTM) is as shown in Figure.2. It consists of Content processor, Network processor,Security processor, General purpose processor, Memory and Ethernet interface.

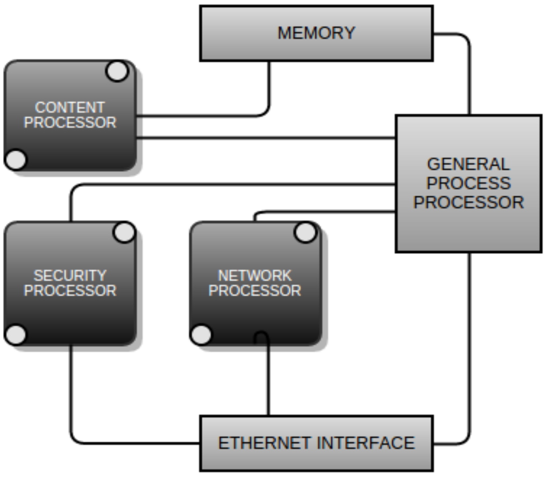


Figure 3. High Level Design of UTM.

4.3.1. Content Processor

Content processor with high speed computational capabilities,perform comparisons between objects in the memory like network packets or files with existing threats. Scanning such objects with threats the content processor triggers intrusion prevention or anti-virus. It works in phase with General purpose processor. Content processor is responsible for monitoring incoming packets and storing threat patterns.

4.3.2.Network Processor

Network processor monitors network flow with high speed networking capabilities. They are generally placed in between general purpose register and network ports such that they can process the incoming network traffic. Functionalities of network processor are packet based communication,encryption/decryption,firewall and Network address translation (NAT).

4.3.3. Security Processor

Security processor is also included in our proposed technique to incorporate flow based inspection technologies such as intrusion prevention,anti-virus,application control etc., if traffic by pass UTM system, security processor can get session processing information from the CPU and scans the packet independently. Using security processor,we can deliver a better system performance.

4.3.4. General Purpose Processor

General purpose processor coordinates and works alongside with the network processor and content processor. They are capable of performing computational task for encrypted communication with the help of cryptographic engine in Content processor.

4.3.5. Ethernet Interface

Ethernet interface is the network port that connects the UTM to the network. The Ethernet interface makes it possible to for the network processor to receive the incoming network traffic.

4.3.6. Memory

Memory stores information about existing threats and also acts as a cache memory for holding the objects while the content processor performs scanning.

V. EVALUATION

Unified Threat Management Appliance is evaluated using a set of policies which are listed as follows,

5.1. Security Capabilities

The UTM being grouped with technologies like Intrusion prevention,anti-virus,spy ware protection etc., will provide its best with known threats. But for unknown threats, update is needed which may take considerable amount of time. During that course of time the network cannot be unprotected. So an ideal UTM should provide a security solution that can defend zero day attack and during downtime. This is achieved by programming UTM in such a way that it defend against a class of threat, by which a new threat could be identified.

5.2. Availability

Single point of failure may be an important drawback of UTM. Being a single entity comprising of various functionality if any failure is encountered the network is vulnerable to attacks. To overcome such an issue UTM has available resources when there is any failure in UTM or during downtime that helps the UTM to serve its functionality until the problem is resolved.

Availability could be achieved in two different way, one is to have a set of additional hardware component that remains idle till there is no interruption in functioning of UTM. Another approach is to provide software solution to repair the problem encountered within the UTM. The latter approach is best suited being simpler and cost effective.

5.3. Flexibility

A reliable UTM should be flexible so as to meet the needs of the end users. UTM should be provisioned to add additional hardware components and to increase the functionalities as and when required. It should also be flexible enough to enable and disable functionalities as per the choice of the user.

5.4. Performance

Performance testing is the best way to evaluate the working of UTM. Measuring performance of a UTM is complex when compared to other security devices. Metrics like throughput or latency will not be enough for portraying the performance of UTM. It depends on the way by which UTM has been configured and the traffic that passes through the UTM.UTM modeled by grouping technologies from different vendors may operate simultaneously and higher power consuming. Same network traffic may be scanned by different applications degrading the overall performance of the UTM.

There are several tools available for efficient measurement of performance of UTM. They are initially tested across the network traffic and a sample data stream is sent through the device ensuring that the data stream received is the actual data stream sent. Performance testing in a test bed environment may be not be reliable when the UTM is connected to a real time network.Also the web application firewall integrated to the UTM is also tested for its performance.

VI. CONCLUSION

This proposed Unified Threat Management (UTM) appliance with enhanced security features helps in defending the internal network from all possible threats. We have incorporated technologies and grouped them under a single entity. It has been designed in such a way that it is capable of maintaining the network traffic, throughput integrity and maintain the performance needs of a high speed network. It also proves be a strong defender against zero day attack. An ideal solution is achieved by integrating hardware, software and security solution. Ease of use and cost effectiveness are two major advantages of UTM. When properly configured, deployed and maintained UTM will help out in productivity of the organization that uses UTM Future work is to evaluate UTM in cloud security.

REFERENCES

[1] M. Stevens, "UTM - one stop protection", Elsevier, Network Security, Vol2006, Issue 2, pp. 12-14, Feb 2006, doi: 10.1016/S1353-4858(06)70336-1

[2] M. Stevens, "UTM - one stop protection", Elsevier, Network Security, Vol 2006, Issue 2, pp. 12- 14, Feb 2006, doi:10.1016/S1353-4858(06)70336-1

[3] IDC Vendor Spotlight, White Paper, "Unified Threat Management Appliances and Identity-Based Security: The Next level in Network Security,"http://www.cyberoam.com/downloads/IDC/ VendorSpotlight.pdf

[4] S. Jajodia, S. Noel and B. O'Berry. 2005. Topological analysis of network attack vulnerability. In Managing Cyber Threats, Ed: Springer. pp. 247-266.

[5] http://www.comodo.com

[6] http://www.untangle.com

[7] http://en.wikipedia.org/wiki/Unified_threat_management

[8] http://en.wikipedia.org/wiki/Stateful_Firewall