Unified Threat Management

Authors Name/s – Sanil Almeida.
Dept. name of organization – Computer Engineering
Name of organization – Fr. Conceicao Rodrigues College of Engineering
E-mail - sanilalmeida007@gmail.com,
Contact number : Sanil Almeida- +919022208189

Abstract - **For many smaller and larger entities over the last couple of decades, information systems and technologies have become an integral part of their operations and played a major role in drastically changing and often improving their business processes. As computers become more and more integrated into our business organizations, we end up leaving and storing confidential, vital business and sensitive information on them. In general, larger organizations have the technical expertise and resources to better secure computing services. The Small to Medium Enterprises (SMEâs), however, often lack the platforms, infrastructure, technical expertise, and the required financial resources to be able to utilize modern secure technologies for computing services. This paper discussed the importance of network security, analyzed different type of threats to network infrastructure, different methodologies that can be used to mitigate network infrastructure threats and have proposed an approach for securing SMEâs network infrastructure.**

***Keywords*— Threat, Application, TATA DOCOMO, Software, Hardware.**

I. Introduction

Unified threat management (UTM) is an approach to security management that allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console.

UTMs, which are typically purchased as cloud services or network appliances, provide firewall, intrusion detection, antimalware, spam and content filtering and VPN capabilities in one integrated package that can be installed and updated easily.

Unified threat management is basically a firewall appliance that not only guards against intrusion but also performs content filtering, spam filtering, intrusion detection and antivirus duties traditionally handled by multiple systems. These devices are designed to combat all levels of malicious activity on the computer network.

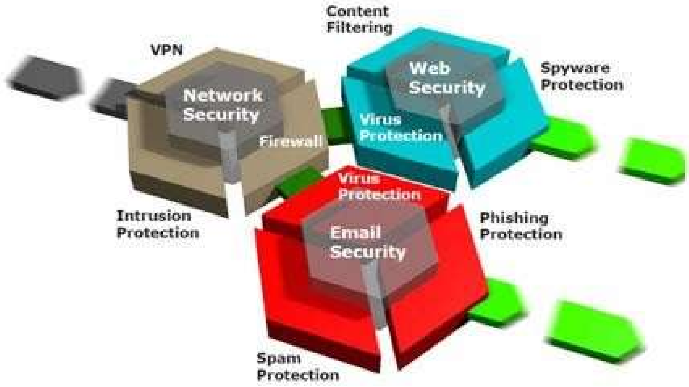

Fig 1. Unified Threat Management

II. Concept of UTM

An effective UTM solution delivers a network security platform that comprises robust and fully integrated security and networking functions such as network firewalling, intrusion detection and prevention systems (IDS/IPS) and gateway antivirus (AV) along with other features, such as security management and policy management by group or user. It is designed to protect against next-generation application layer threats and offers a centralized management through a single console, all without impairing the performance of the network.

III. Working of the UTM

A single UTM appliance simplifies management of a company's security strategy, with just one device taking the place of multiple layers of hardware and software.UTMs represent all-in-one security appliances that carry a variety of security capabilities including firewall, VPN, gateway anti-virus, gateway anti-spam, intrusion prevention, content filtering, bandwidth management, application control and centralized reporting as basic features. The UTM has a customized OS holding all the security features at one place, which can lead to better integration and throughput than a collection of disparate devices.

IV. Advantages of UTM

- Reduced complexity: The integrated all-in-one approach not only simplifies product selection, but product integration and ongoing support as well.

- Ease of deployment: Since there is much less human intervention required, customers themselves or vendors can easily install and maintain these products.
- Integration capabilities: The appliances can easily be deployed at remote sites without the help of any security professional. In this scenario, a plug-and-play appliance can be installed and managed remotely. This kind of management is synergistic with large, centralized software-based firewalls.
- The black box approach: Users have a tendency to play with things, and the black box approach limits the "damage" users can do. This reduces trouble calls and improves network security.
- Troubleshooting ease: When a box fails, it is easier to swap it out than troubleshoot. This process gets the node back online quicker. A non-technical person can do it, which is especially important for remote offices without dedicated technical staff onsite.

V. Application of UTM

UTM by TATA DOCOMO

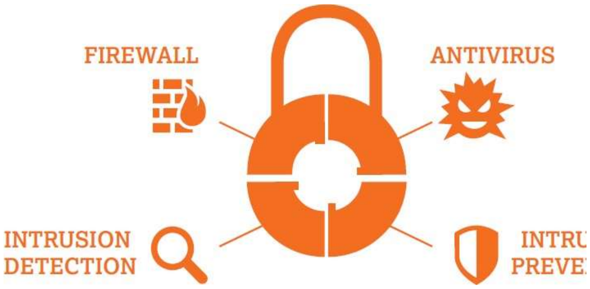

Fig 2. Tata Docomo UTM Module

A. Abstract

Organizations today are seeing an increase in the number of security threats and in the severity of attacks. They are being forced to rethink their IT security infrastructure to protect their assets and information from insider, outsider and blended attacks. The IT landscape is also becoming more complex as a result of cloud computing and virtualized server based environments. Network security has become a critical business requirement. Traditionally, it was handled by multiple devices which carried out specific functions such as a firewall, intrusion detection, anti-spam, anti-virus etc. But this became cumbersome and complex to manage and expensive to scale. Unified Threat Management (UTM) solutions arose from a need to simplify this environment, standardize the security platform and lower operating costs.

B. Introduction

The analyst firm IDC in 2004 defined Unified Threat Management (UTM) as a security appliance that combines firewall, gateway antivirus and intrusion detection (IDS) / intrusion prevention (IPS). Organizations, whether small, medium or large, want to protect and secure their IT assets or networks against threats of all kinds such as viruses, Trojans, malware, Denial of Service attacks and intrusion detection and prevention. These threats are on the increase and occur frequently. They could be external, internal or blended attacks. The current day threats spread quickly and cause extensive damage within hours. In some cases, they are very organized and directed at specific targets. Internal threats could come from employees within the organization with access to valuable information. The breaches may be purely accidental due to negligence about security settings, device loss or theft, or a result of mis-configuration of devices, especially considering the BYOD trend prevalent today.

C. Benefits:

Easy to manage: UTMs use a single management console which simplifies day-to-day management of operations and let IT admins remotely monitor their security environment.
Easy to deploy: Easy to use and configure.
Integration: They usually integrate with standard network configurations.
Easy to troubleshoot: Some UTMs may guide IT admins through trouble
shooting.
Better performance: Recent day appliances use high-performance processors.

D. Types of DOCOMO UTM

There are three types of UTM products. Each has its advantages and disadvantages.

a) Hardware-based or physical appliances:

These are the most common and the most popular. They contain specialized ASIC chip-sets to scan for multiple threats simultaneously. They come equipped with a network security operating system that integrates with all the individual components of the UTM. Each individual component is license based. A UTM solution consisting of a basic firewall, anti-virus and anti-spam can be purchased or the entire range of components can be purchased, with licenses renewed annually. Once the appliance has been configured to work on organization’s network, adding users, groups, setting up security policies, rules and permissions at the individual and group level can be carried out. The hardware appliance provides integration of all security functions with a centralized management console. The disadvantages are that additional hardware UTM appliances add to cost if the organization already has point solutions in place. An appliance could be a single point of failure. Hardware performance can deteriorate when many users and applications use the appliance simultaneously and as a result, the organization may disable a particular function to keep the system operational and compromise security.

b) Software based:

The UTM software is purchased separately and installed on existing hardware saving on hardware costs. The network security operating system and individual UTM components such as anti-spam, intrusion detection are hosted on standard computer servers that meet specific minimum configuration requirements related to number of users and applications that can run simultaneously. Licensing is similar to the hardware based UTMs. The disadvantage is that the UTM software is another layer of vulnerability versus a hardware based one.

c) Virtual:

These are appliances that are deployed remotely on the cloud, typically in cloud computing environments or virtualized server based environments like data centers. The virtual security appliance market is expected to grow significantly. These appliances sit on a virtualized server such as VMware and provide security for many virtual machines on a single server. Traffic between virtual machines within the same server is not inspected by traditional appliances or firewalls that normally inspect traffic coming in and going out of the physical server. But challenges still remain in virtual appliance based security solutions, as the network architecture in a cloud computing or a virtualized environment tends to be complicated, and adds to the complexity of building a security infrastructure to protect such an environment.

E. Usage based on Organisation:

Both large and midsize organizations use UTM solutions today. While midsize organizations may use UTM devices to primarily secure the network, large organizations use them to secure their borders or perimeters while using individual or point solutions in other areas. They may choose specific solutions depending on their needs. One example is a large enterprise deploying multiple devices across various sites, but still managing it from a central console with user access controls and policies replicated across sites. Another example would be to deploy multiple UTM devices, with each device prioritizing a specific security function such as anti-virus scanning. In such cases, a backup strategy is needed to guard against a single point of failure caused by relying on a single device.

F. Choosing the right provider

Organizations should make a checklist of all the security functions their business may need, followed by a list of providers that offer solutions for those functions. Some providers may be best-of-breed in some areas but not so much in others as they have usually evolved from certain core offerings and then expanded through acquisitions. Sometimes nomenclature might also vary - some might call their product offering a UTM appliance, a next gen firewall (NGFW) or just a firewall. It is important to drill down and do some due diligence on what the solution entails and if the solution meets requirements. The UTM appliance needs to be also correctly sized to meet maximum usage requirements.

Conclusion:

Companies today face a multitude of risks to their data from known and unknown sources, making UTM imperative for the business. The nature of UTM required by a company would however be dependent on various factors including the size and nature of its operations. However, a thorough study into the solutions available and their suitability is of great importance before deploying a solution to ensure optimization of benefits for the company. Unified Threat Management can prove very useful and beneficial for organizations with remote branches to control security with centralized secure management. In future if UTM is made available to small scale organizations, instead of purchasing or implementing various security applicatons, one can simply use the UTM facility to ensure the several security concerns related to the organization.

REFERENCES

[1] http://searchnetworking.techtarget.com/tip/Network-security-Using-unified-threat-management-UTM

[2] http://www.informationweek.com/smartadvice-unified-management-is-next-for-security/d/d-id/1030852

[3].http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management

4] http://www.unifiedthreatmanagement.com/

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

[6] http://www.tatadocomo.com/sme/download/Unified-Threat-Management-Whitepaper.pdf