Secure your organization through Unified Threat Management

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. Present-day UTM solutions protect against a multitude of threats with services such as anti-spam, anti-virus, anti-spyware, anti-phishing, intrusion detection, DoS (Denial of Service) attack mitigation, content filtering, application blocking, bandwidth management and regulatory blocking. This white paper discusses the benefits of UTM, how they are used and ways that organizations can secure their IT assets from threats and attacks.

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 misconfiguration of devices, especially considering the BYOD trend prevalent today. They could also be unintentionally downloaded from applications from social networking sites. Gartner reports that Internet attacks target web applications over other services.
Security solutions therefore play a critical role in protecting the organization.

In the early days of network security, stand-alone products or devices such as firewalls and VPNs came as pre-installed software on a PC or a router connecting to the Internet, or as an appliance. But managing and maintaining these numerous stand-alone solutions became complex and led to increased costs. Today these stand-alone products have evolved into security appliances that can be centrally managed and can protect the entire network and form the basis of unified threat management. UTM solutions protect against a multitude of threats with standard network configurations, such as a firewall, intrusion detection, anti-spam, anti-phishing, and DoS (Denial of Service) attack mitigation, content filtering, application blocking, bandwidth management and regulatory blocking.

The complex, present day IT landscape with virtualized servers, desktops and storage, combined with the rise and severity of security threats, is forcing organizations to rethink their security infrastructure and has refocused attention on UTM solutions.

**UTM**

UTM solutions secure against a variety of threats with services such as anti-spam, anti-virus, anti-spyware, anti-phishing, intrusion detection, DoS (Denial of Service) attack mitigation, content filtering, application blocking, bandwidth management and regulatory blocking.

In the beginning, UTM solutions were favored by small businesses as the technology was easily configurable, less expensive and provided sufficient protection. Nowadays it has gained acceptance with organizations of all sizes and can deployed as onsite or virtual appliances or as software. UTM solutions have become all-inclusive products that can protect the breadth of the organization including remote branch locations, telecommuters and mobile employees.

**Benefits**

- **Easy to manage:** UTM solutions 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 troubleshooting.

**Better performance:** Recent day appliances use high-performance processors

UTM solutions have been existence now for a decade. The early UTM appliances were very basic and would sometimes not be capable of high-traffic solutions. That is no longer a problem, with present-day high-speed processors, offering organizations better visibility over their network and reduce network complexity.

Cost savings are a big benefit of a UTM solution as UTM devices usually cost less than their individually deployed point solutions. Moreover one UTM appliance can replace five or six individually deployed point solutions, saving storage space in the data center and reducing energy consumption.

UTM appliances are easy to install, configure and manage when compared to managing many different security applications through separate management consoles. They also reduce the number of upgrades, patches and contracts to manage. It is easier and simpler in terms of time and effort to problem-solve an issue over a single device versus across multiple devices.

A centralized management console makes it easier to set group policies as there is intelligence sharing between security applications. Standardized event reporting, event analysis and activity logs makes it easier for IT staff to analyze problems for cause and effect. The increased visibility that UTM solutions provide, enable IT staff to identify threats quicker.

UTM appliances are also efficient meaning they scan data packets once for all functions such as spam and anti-virus and not as separate security applications.

UTM appliances have progressed to the point where they can identify specific user patterns that may denote misuse, unauthorized intrusions or malicious attacks allowing IT admins to place alerts based on pre-defined patterns of behavior at the individual or group level. Significant deviation can trigger a security alert.

Another major benefit is scalability as it provides organizations with the flexibility to buy the specific security modules they need, and add more later when the number of users increase.
IT Admins can deploy multiple UTM appliances across a widely spread out network configuration of remote branch offices, telecommuters and mobile employees, and manage it all remotely from a central console.

Types of UTM

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

**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.

**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.

**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.

Usage

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.
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.

Some of the common uses of UTM appliances are listed in the table below:

<table>
<thead>
<tr>
<th>Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Load Balancing</td>
<td>Can be used for distributing traffic automatically over multiple links</td>
</tr>
<tr>
<td></td>
<td>Can support routing of traffic based on speed and cost of WAN link</td>
</tr>
<tr>
<td>Layer 8 Identity-based Routing</td>
<td>Can define routing based on</td>
</tr>
<tr>
<td></td>
<td>• Source</td>
</tr>
<tr>
<td></td>
<td>• IP</td>
</tr>
<tr>
<td></td>
<td>• Protocol etc.,</td>
</tr>
<tr>
<td>Automatic Link Failover</td>
<td>Can be used to automatically detect failed WAN link and route traffic to working link</td>
</tr>
<tr>
<td>Wireless WAN Technologies</td>
<td>Can help manage networks by allowing configuration of network links over protocols such as WiMax and 3G</td>
</tr>
</tbody>
</table>

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.