Intelligent Business Solutions Ltd

UTM (UNIFIED THRED MANAGEMENT) OR FIREWALL?

By Maria Ioannidou – Office Administrator

Within the arrange security industry, the terms firewall and UTM appliance are quite common. They are basically used for systems / solutions that can help a company in providing protection for its databases and secure its network against harmful intrusions. UTM is basically an abbreviation of Unified Threat Management. Now, for anyone with limited knowledge of the network security industry, it will be quite easy to figure out that firewalls and UTM appliances both share a lot of similarities with each other. Both are outlined to provide protection, and the main purpose of both is to prevent any sort of harmful / malicious software programs from entering the system. However, even though their main task is similar, both firewalls and UTM Appliance are actually quite diverse from each other.

Firstly, let's find out in few and simple words what is Fire wall and what is UTM.

Unified threat management (**UTM**) is an approach to data security where a single hardware or software installation provides multiple security functions. This contrasts with the traditional method of having point solutions for each security function. UTM simplifies information-security management by providing a single management and reporting point for the security administrator rather than managing multiple products from different vendors. UTM appliances have been gaining popularity since 2009, partly because the all-in-one approach simplifies installation, configuration and maintenance. Such a setup saves time, money and people when compared to the management of multiple security systems. Rather than having several single-function appliances, all needing individual familiarity, attention and support, network administrators can centrally administer their security resistances from one computer.

A firewall is a device which blocks network traffic at the IP and IP: port socket levels (what is IP and IP Port socket: *A **socket** is one endpoint of a two-way communication link between two programs running on the network. A **socket** is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to. An endpoint is a combination of an **IP** address and a port number*). Some have stateful inspection such that it monitors the initial TCP handshake, and some do not. Generally, a firewall is used for blocking entire protocols and types of traffic, but it doesn't see into the actual substance.

On the opposite, Unified Threat Management takes it a step encourage. An arrangement of this sort will be a firewall however it will do deeper inspection into the packets at layers 5, 6 or 7 - the Open Systems Interconnection **model** 'OSI model' (What is **OSI model:** *is a conceptual **model** that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. … The **model** partitions a communication system into abstraction **layers***). In addition to firewall functionality, UTM should also include functionality which is termed Intrusion Detection and/or Intrusion Prevention (IDS or IPS), network based anti-virus or other malware prevention. A UTM or IPS System would coalition the assault, while a firewall would not. So, let's get an example to comprehend it better.

A firewall might be well arranged to allow HTTP port 80 traffic between two hosts (What is Port 80*: is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the port from which a computer sends and receives Web client-based communication and messages from a Web server and is used to send and receive HTML pages or data*). However, you could have someone sending a SQL injection attack (what is SQL Injection: *is a code injection technique that might destroy a database and, is one of the most common web hacking techniques. It places a malicious code in SQL statements, via web page input*) on port 80 to the web server, which in turn sends it to the backend DB (what is DB: *is a database that is accessed by users indirectly through an external application rather than by application programming stored within the database itself or by low level manipulation of the data*), thereby corrupting someone's system. A UTM or IPS system would block that attack, while a firewall would not. In a small or medium sized business, UTM makes more sense because you're bundling usefulness onto a single stack and you likely have more generalists than specialists in network security.

In a large enterprise, however, typically we have usefulness isolated out into firewalls, IPS devices, anti-virus, anti-malware, layer-7 inspection, etc.

Summarizing it, Firewall does review at layer 4 whereas UTM will look at 4, 5, 6 and 7 and, selecting which is more suitable depends on the needs and set-up of each business / enterprise.

Maria Ioannidou is one of the first office administrator employees of IBSCY LTD, employed back in May of 2014. She is the head of office administration team responsible for all the daily tasks of the company including invoicing, collections, recurring fees organization, strategic reporting and payments monitoring.

She is also responsible for the office supplies and she is acting as office manager for any tasks related with the office of IBSCY LTD in Limassol.

Currently, she is using MS Outlook on a daily basis and the above article was written based on her personal experience.