Latest technological developments in firewall

Law, Security

Global organizations are harnessing new ways to transform security, to prevent dangerous internet based communication, transactions, theft of data and virus attack. Some advocate firewall as a service but the lack of skills can be treacherous as threats go hand-in-hand with new developments. About 80 per cent of the US companies make use future methods, that are deployed at their premises as well as on cloud. On cloud most new technologies are based on the area to protect, where the systems need to define the perimeter.

Hardware protection techniques involve smaller devices/ methods, which can be purchased by the user at a smaller scale but software based require configuration, which can be a tough task for organizations to achieve. To handle virus intrusion through emails, software firewall can be used which scans the external files before downloading it to the machine. Each company needs to design a security infrastructure which can evaluate the risk factors in the environment and secure the most critical assets.

Most hardware based firewall is built in and do not need a configuration that can block malicious content and uses statistical info, signature based and protocol analysis to block IP. The hardware on office network provides external safety, which can protect the networks workstations and servers from intrusion. This can protect the printer, equipments, telephones and other devices.

Firewall security controls are based on a set of rules which can prevent the entry of a network data packet into the program but most organizations fails to identify the basic infrastructure for security.

There are various types of firewalls –

Packet filtering method eliminate programs (apps / messages), which do not follow the predefined rules. The method is transparent but can be targeted by IP spoofing.

Proxy firewall device can set a gateway to restrict networks. Proxy server can be configured to allow only the defined files that get access to the network and stateful inspection examines the state, protocol and port.

Firewall can be installed at the TCP / IP or UDP connection where the packets can flow without further authorisation. Administrator based rules can be set for filtering messages on network. Threat focused firewalls can be implemented for decreasing time of detection and cleaning the devices. Such methods reduce complexity as it quickly reacts to risks. Some offer e. g. multiple protocol label switching WAN connectivity which are beneficial as compared to MPLS.

Most complex types of firewall involve a combination of technologies – there are known as – UTM – unified threat management. The future securities will be based on less expensive versions of firewalls which could provide miscellaneous features such as intrusion prevention where the system checks the packet signatures and uses technology to identify threat.

Deep packet inspection will be able to examine the headers of packers and block as it moves through the inspection point.

New mobile features where progressive technology based workers are using mobiles for every work-related actions, different types of devices, multi path WAN technologies, and multi-level cloud based systems and various other complex digital transformations require simple security solutions. Some companies are offering integrated security solutions based on new technologies.