Post by: Zihaad Khan

Firewalls are tools that can be highly effective on protecting an organization infrastructure. Each organization should adapt a specific firewall solution to their own needs. Traditional firewalls can be categorized as: packet filtering, application proxy servers and stateful packet filtering. In general, all these firewalls work as an intermediary agent that filters undesired information from one end to other.

Packet filtering firewalls inspect each packet that travels through the firewall. The packet passes through the firewall if its header and its contents are determined as legitimate. Proxy servers obtain a more detailed analysis of the information traveling from one end to another so it can be filtered more efficiently, nevertheless they represent a higher consumption of resources which makes them a slower alternative. Stateful packet filtering firewalls can be considered between a combination of the latest two, where packets are also analyzed but in the network as a whole.

One of the most significant limitations of these techniques Is that they cannot adapt or react by their own in case of detecting a new attack as an alternative to firewalls, Security Information and Events Management (SIEM) technology is proposed.

SIEM is a technology that constantly acquires information from different sources such as applications, systems and network components. This information is processed into common registers that an intrusion detection system can analyze to prevent potential attacks.

Hunt, R., Verwoerd, T. 2003. Reactive firewalls—a new technique. Available: https://www.sciencedirect.com/science/article/abs/pii/S0140366403001117?via%3Dihub [Acessed 30 September 2021]

Daneshgadeh, S., Hutschenreuter, H., Maeder, C., Kemmerich, T. 2021. A Framework For Intelligent DDoS Attack Detection and Response using SIEM and Ontology Available: https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/document/9473869 [Accessed 28 September 2021]