Initial Post

Firewalls have existed for more than 40 years, and it is implausible to think that the same security mechanisms that functioned decades ago will continue to work without updates. Traditional remedies include attempting to restrict all application traffic or enabling all apps via an ever-growing list of point technologies in addition to the firewall, which can be detrimental to any business, due to increased business and security threats. Next-generation firewalls (NGFWs) and Vulnerability management solutions (VM) help to achieve a balance between permitting and refusing everything and to prevent IT assets from cyber-attacks.

Next-Generation Firewalls (NGFWs):

NGFWs are the cutting-edge digital protection, combining the greatest features of conventional and new technologies to provide excellent digital protection. The benefits of NGFWs are numerous and begin with providing the highest level of network and data protection. The importance of NGFWs is due to their versatility, intelligence-based port management, threat protection, and application layer filtering.

Layer7 Application filtering is comprised of the following components in next-generation firewalls (NGFWs) from Palo Alto, CheckPoint, Juniper, and Fortinet: The User-ID specifies who is attempting to access the application or server, the APP-ID identifies what application traffic is attempting to reach, and the Content-ID identifies how the traffic is granted access to a resource. Layer 7 filtering is the point at which data is analyzed in connection to the application for which it is being used, such as SSL, web-browsing, and DNS instead of using traditional ports like TCP-80, 443, UDP-53 and so on.

Vulnerability Management tools (VM):

VM continually scan for and identify vulnerabilities with Six Sigma precision, thereby securing an organization's IT assets on-premises, in the cloud, and on mobile endpoints. It provides an overview of security posture and provides access to facts about remedies. VM automatically provides customized, role-based reports for different stakeholders, including security documentation for compliance auditors. Important features of VM include the ability to scan for vulnerabilities globally, accurately, and efficiently, to identify and prioritize risks, remediate vulnerabilities, and generate custom reports anytime, anyplace — without rescanning. Today's pervasive cyber threats require you to be constantly vigilant in order to protect any organization.

References:

"Towards an unified policy for Next-Generation Firewalls" by Aslak Gaaserud; master thesis spring 2013; University of Oslo

Garbis, J., Chapman, J.W. (2021). Next-Generation Firewalls. In: Zero Trust Security. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6702-8_10

"Automation of information security audit in the Information System on the example of a standard “CIS Palo Alto 8 Firewall Benchmark”" by Petr Perminov, Tatiana Kosachenko, Anton Konev, Alexander Shelupanov pblished in International Journal of Advanced Trends in Computer Science and Engineering; Volume 9 No.2, March - April 2020

"DEVELOPMENT OF PROCESS AND TOOLS FOR VULNERABILITY MANAGEMENT" by Anssi Ylätalo; Master’s thesis Master's Degree Programme in Cybersecurity 2019; South-Eastern Finland University of Applied Sciences.

Collaborative Discussion 2 - Initial Post - Gokul K.pdf