Darrcelle Jackson
Written Exercise #11 – Chapter 10
ITWP 2600
4/26/2026

Often, firewall problems are a result of cloud-based online sales systems extending their security boundary past a traditional fixed network edge. Firewalls in an on-premise environment will mostly provide security for a single perimeter but, as cloud computing will distribute applications, data and services across multiple locations and platforms, perimeter firewalls will not be an effective way of securing the edge of the network when workloads are moving into the cloud where the controlled edge is not present. According to Fortinet, perimeter firewalls are built to protect the edge of the network, but perimeter firewalls will become less effective when workloads are processed in a cloud-based environment outside of the controlled edge. As stated by Palo Alto Networks, the modern architectural environment requires that distributed security controls be implemented due to no longer having users, applications and data interact only within a hybrid or cloud-based system and therefore creating issues like inconsistent firewall policies, limited visibility into internal cloud-to-cloud traffic and increased risk of misconfigured application programming interfaces or overly permissive access rules. To avoid these issues, organizations are using cloud native firewalls, centralized policy management tools and Zero Trust security models more frequently to provide consistent security across their expanded environments.

Sources: https://www.fortinet.com/resources/cyberglossary/perimeter-firewall?utm_source=chatgpt.com

https://www.paloaltonetworks.com/cyberpedia/what-is-a-perimeter-firewall?utm_source=chatgpt.com