Alex Bazydlo

ITWP 2600

Chapter 10 Exercise

When a company relies on cloud computing for its online sales system, traditional perimeter based firewalls face significant challenges due to the expansion of the network boundary. In cloud environments, data and applications are distributed across multiple servers and locations, making it difficult to enforce a centralized firewall policy. This perimeter expansion problem means that traffic may bypass the company's primary firewall, as cloud services often require direct external access. Additionally, misconfigured cloud security groups or overly permissive rules can create gaps that attackers might exploit. The dynamic nature of cloud scaling further complicates firewall management, as new instances may spin up without proper security controls. To address this, companies must adopt cloud native security tools, such as web application firewalls and zero trust architectures, to complement traditional firewalls and maintain protection across the expanded perimeter.

A second issue arises from the reliance on third party cloud providers, whose shared responsibility models shift some firewall duties away from the company. Without proper oversight, this can lead to assumptions about security coverage that leave vulnerabilities unaddressed. Encrypted traffic in cloud environments also poses a challenge, as firewalls may struggle to inspect encrypted data for threats without impacting performance. Ultimately, the perimeter expansion problem requires a layered security approach, integrating cloud specific protections with existing firewall strategies to ensure comprehensive defense.

Sources:

https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-best-practices/

https://deploy.equinix.com/blog/cloud-network-security-modern-tools-best-practices/