

Thanks, Edward for the great insight. Next-generation firewalls (NGFW) are considered a more robust level of security and can allow a more profound understanding of what is entering and leaving the network (Thomason, 2012). As attacks are ever more sophisticated, deeper learning into Layer 7 applications can allow more effective monitoring to suspect an intended threat. Thomason (2012) suggests that NGFW offers a more granular approach to access and controls for specific users. Many companies are suggesting they use NGFW; however, they are not by definition. Effectively one device can perform all the necessary functions of reporting through a scanning system. Emerging threats are distinguished earlier as the NGFW provides greater accessibility to network traffic and operability across the OSI layer, supporting protective measures (Neupane et al., 2018).

The nature of NGFW inspects content and behaviour that pass through the checkpoint, which ultimately makes data communication safer, particularly with features such as IPS, URL Filtering, Application Control and Threat Emulation (Soewito & Andhika, 2019). Despite these benefits, many companies are reluctant to offer a single device with many linked network security controls. NGFWs can be costly to administer by taking up many system resources, degrading network performance (Mitra, 2017).

- Mitra, A. 2017. *What is NGFW or Next Generation Firewall?* [Online]. Available: <https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-ngfw-or-next-generation-firewall/> [Accessed 22 September 2021].
- Neupane, K., Haddad, R. J. & Chen, L. 2018. Next Generation Firewall for Network Security: A Survey. *SoutheastCon 2018*, 1-6.
- Soewito, B. & Andhika, C. E. Next Generation Firewall for Improving Security in Company and IoT Network. 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), 28-29 Aug. 2019 2019. 205-209.
- Thomason, S. 2012. Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices. *Global Journal of Computer Science and Technology*, Volume XII.