**Peer - Response**

You centered your discussion on cloud firewalls and wire guard VPN. You highlighted several benefits of wire guard VPN, including minimal attack surface, user-friendliness, high performance, and advanced cryptography. Another advantage you did not mention is that it is easy to detect vulnerabilities in Wire Guard (Lipp et al., 2019). I agree with these benefits. However, there are some weaknesses of the wire guard VPN. For example, Abdulazeez et al. (2020) argued that the automation of wire guards could make VPN providers log user data. Dowling and Paterson (2018) argued that a network admin could block the wire guard VPN because it works when it is on user datagram protocol (UDP) only. Although these disadvantages can hinder the effectiveness of wire guard VPN, Abdulazeez et al. (2020) argued that it could be better than other VPN protocols, including generic routing encapsulation (GRE) and internet protocol security (IP sec). Therefore, I support your argument regarding the effectiveness of wire guard VPN.

You also focused on cloud firewalls, emphasizing Firewall as a Service (FWaaS) benefits. However, I think it is important to address some weaknesses of FWaaS. Firewalls have several vulnerabilities. For example, Alsaqour et al. (2021) argued that personal firewalls are vulnerable to hacking due to static IP addresses and open connections. According to Alsaqour et al. (2021), firewalls cannot be used as standalone security measures because of misused security patches, insider attacks, and lack of deep packet inspection. Other vulnerabilities include configuration mistakes and DDoS Attacks (Kumar, 2016). Anwar et al. (2021) argued that the high exposure of firewalls to external attacks renders them ineffective in cloud environments. However, they can be used after taking special security measures. In conclusion, your discussion post is educative and was well-researched.

References

Abdulazeez, A. M., Salim, B. W., Zeebaree, D. Q., & Doghramachi, D. (2020). Comparison of VPN protocols at network layer focusing on wire guard protocol. International Journal of Interactive Mobile Technologies (iJIM), 14(18), 157. <https://doi.org/10.3991/ijim.v14i18.16507>

Alsaqour,, R., Motmi, A., & Abdelhaq, M. (2021). A Systematic Study of Network Firewall and Its Implementation. IJCSNS International Journal of Computer Science and Network Security, 21(4), 199-208. <http://paper.ijcsns.org/07_book/202104/20210424.pdf>

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall best practices for securing smart healthcare environment: A review. Applied Sciences, 11(19), 9183. <https://doi.org/10.3390/app11199183>

Dowling, B., & Paterson, K. G. (2018). A cryptographic analysis of the WireGuard protocol. Applied Cryptography and Network Security, 3-21. <https://doi.org/10.1007/978-3-319-93387-0_1>

Kumar, G. (2016). Denial of service attacks – an updated perspective. Systems Science & Control Engineering, 4(1), 285-294. <https://doi.org/10.1080/21642583.2016.1241193>

Lipp, B., Blanchet, B., & Bhargavan, K. (2019). A mechanised cryptographic proof of the WireGuard virtual private network protocol. 2019 IEEE European Symposium on Security and Privacy (EuroS&P). <https://doi.org/10.1109/eurosp.2019.00026>