In [ ]:

```
Training Day 27 Report– 19 July 2025
 Introduction
 Day 27 focused on firewall architectures, secure network zoning, and principl
 exposure to reduce attack surfaces across networks.
 Key Concepts Discussed
 We studied packet filtering concepts, stateful inspection, and how to design
 policies that separate critical services from user devices.
 Lab Preparation in Theory
 The trainer explained how to design a network segmentation plan and how to re
 policies in rule sets conceptually without touching production environments.
 Practical Understanding (Theory)
 We discussed how to map business services to policy templates and how to adop
 default-deny stance while allowing required services explicitly.
 Key Takeaways
 Segmentation and strict default-deny rules reduce the available attack surfac
cantly.
 Conclusion
 Next session will cover secure remote access and VPN considerations.
```