1. Which device filters traffic between two networks and is typically used to protect internal networks from external threats?

a) Switch

b) Router

c) Firewall

d) Hub

Answer: c) Firewall

2. What does IDS stand for in network security?

a) Internal Data Service

b) Intrusion Detection System

c) Internet Detection Server

d) Internal Detection Security

Answer: b) Intrusion Detection System

3. Which device monitors network traffic for suspicious activity and issues alerts?

a) IPS

b) IDS

c) Firewall

d) VPN

Answer: b) IDS

4. What is the main function of a VPN?

a) Boost internet speed

b) Encrypt network traffic

c) Filter emails

d) Host websites

Answer: b) Encrypt network traffic

5. Which device can act as a middleman between a user and the internet to filter requests and improve security?

a) Proxy Server

b) Firewall

c) Switch

d) Router

Answer: a) Proxy Server

6. What is the key difference between IDS and IPS?

a) IDS blocks traffic; IPS only monitors

b) IDS only monitors; IPS can block traffic

c) IDS is hardware only; IPS is software only

d) No difference

Answer: b) IDS only monitors; IPS can block traffic

7. What is a DMZ in network security?

a) Data Management Zone

b) De-Militarized Zone

c) Direct Machine Zone

d) Default Management Zone

Answer: b) De-Militarized Zone

8. Which of the following provides stateful inspection of traffic?

a) Basic Router

b) Hub

c) Firewall

d) IDS

Answer: c) Firewall

9. Which device provides all-in-one security functions like firewall, antivirus, and IDS/IPS?

a) Proxy Server

b) UTM

c) VPN

d) Switch

Answer: b) UTM

10. What is the purpose of a honeypot in network security?

a) Speed up network traffic

b) Detect unauthorized access

c) Filter spam

d) Store backup data

Answer: b) Detect unauthorized access

11. Which device ensures secure remote access to a private network over the internet?

a) IDS

b) IPS

c) VPN

d) Proxy

Answer: c) VPN

12. Which network device uses packet filtering to allow or deny traffic?

a) IDS

b) IPS

c) Firewall

d) Proxy

Answer: c) Firewall

13. What is the primary purpose of a proxy server?

a) IDS

b) IPS

c) Act as an intermediary for requests

d) Proxy

Answer: c) Act as an intermediary for requests

14. Which system can detect and prevent vulnerability exploits in real-time?

a) IDS

b) IPS

c) IPS

d) Proxy

Answer: c) IPS

15. What does UTM stand for?

a) IDS

b) IPS

c) Unified Threat Management

d) Proxy

Answer: c) Unified Threat Management

16. Which device connects different networks and routes packets between them?

a) IDS

b) IPS

c) Router

d) Proxy

Answer: c) Router

17. What does NAT stand for?

a) IDS

b) IPS

c) Network Address Translation

d) Proxy

Answer: c) Network Address Translation

18. Which protocol is commonly used in VPNs for encryption?

a) IDS

b) IPS

c) IPSec

d) Proxy

Answer: c) IPSec

19. What type of firewall inspects the state of active connections?

a) IDS

b) IPS

c) Stateful firewall

d) Proxy

Answer: c) Stateful firewall

20. Which device splits a network connection into multiple devices but does not filter data?

a) IDS

b) IPS

c) Hub

d) Proxy

21. Which device ensures secure remote access to a private network over the internet?

a) IDS

b) IPS

c) VPN

d) Proxy

22. Which network device uses packet filtering to allow or deny traffic?

a) IDS

b) IPS

c) Firewall

d) Proxy

23. What is the primary purpose of a proxy server?

a) IDS

b) IPS

c) Act as an intermediary for requests

d) Proxy

24. Which system can detect and prevent vulnerability exploits in real-time?

a) IDS

b) IPS

c) IPS

d) Proxy

25. What does UTM stand for?

a) IDS

b) IPS

c) Unified Threat Management

d) Proxy

26. Which device connects different networks and routes packets between them?

a) IDS

b) IPS

c) Router

d) Proxy

27. What does NAT stand for?

a) IDS

b) IPS

c) Network Address Translation

d) Proxy

28. Which protocol is commonly used in VPNs for encryption?

a) IDS

b) IPS

c) IPSec

d) Proxy

Answer: c) IPSec

29. What type of firewall inspects the state of active connections?

a) IDS

b) IPS

c) Stateful firewall

d) Proxy

Answer: c) Stateful firewall

30. Which device splits a network connection into multiple devices but does not filter data?

a) IDS

b) IPS

c) Hub

d) Proxy

Answer: c) Hub

31. Which device ensures secure remote access to a private network over the internet?

a) IDS

b) IPS

c) VPN

d) Proxy

Answer: c) VPN

32. Which network device uses packet filtering to allow or deny traffic?

a) IDS

b) IPS

c) Firewall

d) Proxy

33. What is the primary purpose of a proxy server?

a) IDS

b) IPS

c) Act as an intermediary for requests

d) Proxy

34. Which system can detect and prevent vulnerability exploits in real-time?

a) IDS

b) IPS

c) IPS

d) Proxy

35. What does UTM stand for?

a) IDS

b) IPS

c) Unified Threat Management

d) Proxy

36. Which device connects different networks and routes packets between them?

a) IDS

b) IPS

c) Router

d) Proxy

Answer: c) Router

37. What does NAT stand for?

a) IDS

b) IPS

c) Network Address Translation

d) Proxy

Answer: c) Network Address Translation

38. Which protocol is commonly used in VPNs for encryption?

a) IDS

b) IPS

c) IPSec

d) Proxy

Answer: c) IPSec

39. What type of firewall inspects the state of active connections?

a) IDS

b) IPS

c) Stateful firewall

d) Proxy

Answer: c) Stateful firewall

40. Which device splits a network connection into multiple devices but does not filter data?

a) IDS

b) IPS

c) Hub

d) Proxy

Answer: c) Hub

41. Which device ensures secure remote access to a private network over the internet?

a) IDS

b) IPS

c) VPN

d) Proxy

Answer: c) VPN

42. Which network device uses packet filtering to allow or deny traffic?

a) IDS

b) IPS

c) Firewall

d) Proxy

Answer: c) Firewall

43. What is the primary purpose of a proxy server?

a) IDS

b) IPS

c) Act as an intermediary for requests

d) Proxy

Answer: c) Act as an intermediary for requests

44. Which system can detect and prevent vulnerability exploits in real-time?

a) IDS

b) IPS

c) IPS

d) Proxy

45. What does UTM stand for?

a) IDS

b) IPS

c) Unified Threat Management

d) Proxy

46. Which device connects different networks and routes packets between them?

a) IDS

b) IPS

c) Router

d) Proxy

47. What does NAT stand for?

a) IDS

b) IPS

c) Network Address Translation

d) Proxy

48. Which protocol is commonly used in VPNs for encryption?

a) IDS

b) IPS

c) IPSec

d) Proxy

Answer: c) IPSec

49. What type of firewall inspects the state of active connections?

a) IDS

b) IPS

c) Stateful firewall

d) Proxy

Answer: c) Stateful firewall

50. Which device splits a network connection into multiple devices but does not filter data?

a) IDS

b) IPS

c) Hub

d) Proxy

Answer: c) Hub