Question 1) Explain the role of a Unified Threat Management (UTM) appliance in network security. What are the key security functions typically integrated into a UTM, and how does it simplify the management of security policies and controls within an organization?

Answer: The role of the UTM appliance is to be an all-in-one solution that combines firewall, malware scanner, IDS, ETC. You can monitor and manage the controls from a single console.

Question 2) Describe the role of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in network security. How do these appliances work to detect and respond to potential threats and vulnerabilities in a network?

Answer: IDS is using software tools to provide real time analysis of either network traffic or system and application logs. On the other hand, an IPS can provide an active response to any network threat that it matches. As discussed before IDS uses logs and tracking to give an idea of where a threat or potential attack is coming from. Whereas the IPS actually can provide a response to the attack happening. This can happen by the IDS ending the TCP session and sending a TCP reset packet to the attacking host.