Network Protection Systems FAQ

1. What are Network Protection Systems and what are some examples?
Network Protection Systems are any devices or systems designed to protect a network. They can range from individual components such as a router or firewall to complete systems like a Unified Threat Management (UTM) device. A UTM device combines many network protection functions into a single device such as a firewall, intrusion detection and prevention systems, VPNs, and malware detection and filtering systems.

2. What is the purpose of a router and how does it protect a network?
Routers are hardware devices that send packets to different network segments. They operate at the network layer of the OSI model and use routing protocols to determine the best path for data to travel across a network. Routers can protect a network by using Access Control Lists (ACLs) to filter traffic based on source and destination IP addresses, port numbers, and protocol types.

3. What are the main types of firewalls and what are their advantages and disadvantages?
Firewalls are devices that control access to all traffic entering and leaving an internal network. There are two main types of firewalls: hardware firewalls and software firewalls.

- **Hardware firewalls** are dedicated devices with embedded operating systems. They are typically faster and can handle larger throughput than software firewalls. However, they can be expensive and users are locked into the functionality provided by the specific hardware.
- **Software firewalls** are installed on a computer system and use the system's resources to filter traffic. They are typically less expensive than hardware firewalls and more flexible as the system can be easily upgraded and more NICs added. However, they can be slower and more susceptible to configuration problems as they rely on the underlying host operating system.

4. What are the key technologies used by firewalls to protect a network?
Firewalls use several technologies to protect a network:

- **Network Address Translation (NAT):** Maps internal private IP addresses to public external IP addresses, effectively hiding the internal network infrastructure from the outside world.
- **Access Lists (ACLs):** Filter traffic based on criteria such as source IP address, destination IP address, port number, and protocol type.
- **Packet Filtering:** Screens packets based on information contained in the packet header, such as protocol type, IP address, and TCP/UDP port.
- **Stateful Packet Inspection:** Records session-specific information about a network connection, providing a more sophisticated level of filtering than packet filtering by recognizing anomalies in traffic patterns.
- **Application Layer Inspection:** Inspects network traffic at a higher level in the OSI model to ensure that the application protocol being used is allowed by a rule.

5. What is a Demilitarized Zone (DMZ) and why is it important for network security?
A DMZ is a small network located between the internet and a private network. It contains resources that a company wants to make available to internet users but are not considered part of the trusted internal network. This provides an extra layer of security as it isolates these publicly accessible resources from the sensitive data and systems on the internal network. If a system in the DMZ is compromised, it will be more difficult for an attacker to gain access to the internal network.

6. What is the difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS)?
Both IDSs and IPSs monitor network devices for malicious activity. However, an IDS only detects and alerts administrators to suspicious activity, while an IPS takes action to prevent the intrusion. This action could include blocking the traffic, resetting the connection, or dropping the malicious packets.

7. What are honeypots and how do they help enhance network security?
A honeypot is a computer system or network segment that is intentionally designed to be vulnerable to attack. It is used to lure in attackers and distract them from real targets on the network. Honeypots are also valuable tools for gathering information about attacker techniques and tools. By monitoring the activities of attackers within the honeypot, security professionals can learn about new threats and vulnerabilities and improve their overall security posture.

8. What is web filtering and how does it protect users?
Web filtering is a security feature that blocks access to websites deemed inappropriate or dangerous. It is typically implemented on a firewall or a dedicated web filtering appliance and utilizes blacklists and whitelists of websites along with content analysis to identify and block potentially malicious web pages. This helps protect users from malware, phishing attacks, and other web-based threats.