2017494095 李启佳

1.Yes, link and end-to-end encryption can both be used on the same communication. The advantage of using both forms of encryption is that it provides an additional layer of security. If an attacker were able to intercept the encrypted data in transit, they would still need to break the end-to-end encryption to access the actual content of the message. A situation where both link and end-to-end encryption might be desirable is in the case of a large enterprise that wants to protect sensitive data as it is transmitted between its various offices and employees.

2.Wasteful inspection firewalls can determine information about a traffic stream even when the stream may be out of order or damaged because they keep track of the state of network connections. The firewall maintains a table of active connections and can match incoming packets against the table to determine whether they belong to an existing connection. By doing so, the firewall can reassemble packets in the correct order and filter out damaged packets.

3.An organization might want two or more firewalls on a single network for added security. By using multiple firewalls, an organization can create a defense-in-depth strategy that provides layers of protection against network threats. Additionally, different firewalls can be used for different purposes, such as one firewall for inbound traffic and another for outbound traffic.

4.The advantage of an IDS that generates an alert for every action is that it provides the most comprehensive monitoring of network activity. However, the disadvantage is that it can generate a large number of false positives, which can be time-consuming for administrators to review and can lead to alert fatigue. By adjusting the settings of the IDS to filter out benign activities, the number of false positives can be reduced, but there is a risk that some malicious activity may go undetected.

5.A network administrator should not put a firewall in front of a honeypot because the purpose of a honeypot is to attract attackers and study their behavior. A firewall would block access to the honeypot and defeat its purpose. However, the honeypot should be isolated from the rest of the network to prevent attackers from accessing other systems.

6.A website can distinguish between lack of capacity and a denial-of-service attack by analyzing the pattern and characteristics of the traffic. In the case of a sudden spike in traffic, the website can look for signs of malicious traffic such as traffic from a single source or traffic with anomalous characteristics. The website can also analyze the traffic to determine if it is coming from legitimate users or bots. If the traffic appears to be from legitimate users, the website may conclude that the increase in traffic is reasonable.

7.Spam senders frequently change their email address and domain to avoid being blocked by spam filters. By changing their address and domain, they can evade filters that are designed to block messages from known spammers. However, changing the address does not prevent victims from responding to their messages because the reply-to address can be different from the sending address. Additionally, some spammers use a technique called email spoofing to make their messages appear to come from a legitimate source.

8.A web server needs to know the address, browser type, and cookies for a requesting client to provide personalized content and to maintain state across multiple requests. The address is used to identify the client and can be used to track the client's behavior on the site. The browser type is used to determine what features the client's browser supports and to provide content that is optimized for that browser. Cookies are used to store information about the client's session, such as login credentials or preferences.

9.The advantage of an IDS that generates an alert for every action is that it provides the most comprehensive monitoring of network activity. However, the disadvantage is that it can generate a large number of false positives, which can be time-consuming for administrators to review and can lead to alert fatigue. By adjusting the settings of the IDS to filter out benign activities, the number of false positives can be reduced, but there is a risk that some malicious activity may go undetected.

10.A DMZ (Demilitarized Zone) network is a network segment that is separate from the internal network and the public internet. It is designed to provide an additional layer of security by placing publicly accessible servers such as web servers or mail servers on this network. This isolates the servers from the internal network, making it more difficult for attackers to gain access to sensitive information. Typically, a DMZ network would contain servers such as web servers, mail servers, and FTP servers.

An internal firewall is used to protect the internal network from threats originating from within the network. It is designed to control traffic between network segments within the organization. An external firewall is used to protect the network from threats originating from the public internet. It is designed to control traffic between the organization and the outside world.

11.

a. A packet filtering firewall is a type of firewall that examines the header information of a packet and decides whether to forward or drop it based on a set of predefined rules. It works by inspecting the source and destination IP addresses, ports, and protocols of each packet and comparing them to the rules in its rule set. Packet filtering firewalls are generally faster and less complex than other types of firewalls, but they have some weaknesses. For example, they can only filter traffic based on the information in the packet header, which can be spoofed or manipulated. They are also vulnerable to IP and MAC address spoofing attacks.

b. Rule A allows inbound SMTP traffic from external sources to internal servers on port 25, as long as the source port is above 1023. Rule B allows outbound SMTP traffic from internal servers to external destinations on port 25, as long as the destination port is above 1023. Rule E denies any traffic that does not match the previous rules.

c. The attack will not succeed because rule E denies any traffic that does not match the previous rules, and there is no rule that permits traffic on port 5150 or to port 8080. Therefore, the packet filtering firewall will drop the packet.