1. **Describe four (4) protection mechanisms that you must put in place if a device is exposed directly to the Internet or to any untrusted network.**

   Answer: Four protection mechanisms that directly exposed to the internet or untrusted network are:

   - Host-based firewalls for servers and personal firewalls for desktop and laptop computers provide an additional layer of security against network-based attacks.
   - Anti-virus software must be used to block viruses, and anti-spam software must be used if an e-mail client application is installed.
   - Access control policies should be configured with strict access control rules. This means only authorized users and applications should be allowed to access certain data and services.
   - Regular software updates and security patches ensures that vulnerabilities are fixed before attackers can exploit them. Applying security patches regularly reduces the risk of cyber threats.

2. Fill in the blanks:

   With a _**site to site VPN**_________, the tunnel exists only between the two gateways, but all traffic that passes through the tunnel is _**encrypted**_____.

3. **Describe the advantages and disadvantages of setting up a DMZ.**

   Answer: DMZ is a network that protects an organization's internal network from untrusted traffic. Here are the advantages and disadvantages of setting up a DMZ:

Advantages	**Disadvantages**
A DMZ creates an additional layer of defense, making it harder for attackers to reach sensitive data.	Setting up and managing firewall rules for a DMZ requires advanced network knowledge.
It allows only necessary traffic to reach internal networks while blocking unauthorized access.	If the firewall controlling the DMZ in compromised, attackers could gain access to internal system
firewall in a DMZ inspect inbound and outbound traffic to detect and block unauthorized.	The single firewall must also take care of all traffic to the DMZ and internal network.
Organizations can host web servers, email servers, and other public services safely without exposing their private network.	DMZ systems must be regularly updated and monitored to prevent vulnerabilities.

4. Fill in all four (4) blanks:

   A packet should never arrive at a firewall for delivery and have both the _**SYN**__ flag and the _**ACK**__ flag set unless it is part of an _**stablished connection**______, and it should be in response to a packet sent from _**the internal network**____ with the SYN flag set.

5. Describe in detail how does a firewall handle traffic when the traffic originates from a public network and it travels to the private network.

   Answer: When traffic comes from a public network like the Internet and tries to enter a private network, the firewall checks which one should allow or block the data.

   - The firewall inspects packets based on set rules, checking details like the source and destination IP addresses, port numbers, and protocols.
   - If the firewall is stateful, it maintains a record of active connections and only allows packets that belong to an ongoing, legitimate session.
   - The firewall blocks harmful traffic, such as IP spoofing attempts or Denial-of-Service (DoS) attacks.
   - Some firewalls can scan deeper into network packets to detect threats in application.

6. Which ONE of these statements describes a typical security policy for a DMZ firewall configuration?

   a. Traffic that originates from the DMZ interface is selectively permitted to the outside interface.
   b. Return traffic from the inside that is associated with traffic originating from the outside is permitted to traverse from the inside interface to the outside interface.
   c. Return traffic from the outside that is associated with traffic originating from the inside is permitted to traverse from the outside interface to the DMZ interface.
   d. Traffic that originates from the inside interface is generally blocked entirely or very selectively permitted to the outside interface.
   e. Traffic that originates from the outside interface is permitted to traverse the firewall to the inside interface with few or no restrictions.

7. Which statement**s** describe ACL processing of packets? Select all the correct answers. (6 points)

   a. An implicit deny any rejects any packet that does not match any ACE.
   b. A packet can either be rejected or forwarded as directed by the ACE that is matched.
   c. A packet that has been denied by one ACE can be permitted by a subsequent ACE.
   d. A packet that does not match the conditions of any ACE will be forwarded by default.
   e. Each statement is checked only until a match is detected or until the end of the ACE list.
   f. Each packet is compared to the conditions of every ACE in the ACL before a forwarding decision is made.

8. Which of the following are the characteristics of a stateful firewall? Select all correct answers.

   a. uses static packet filtering techniques
   b. uses connection information maintained in a state table
   c. analyzes traffic at Layers 3, 4 and 5 of the OSI model
   d. uses complex ACLs which can be difficult to configure
   e. prevents Layer 7 attacks

9. Define the term "DMZ" as it pertains to network security, and name two (2) different, yet common services that are typically found there. Describe the benefit of a perimeter network.

   Answer: DMZ is a security zone designed to isolate public-facing services from an internal private network.

   Common services in DMZ:

   i. Web servers – Host websites accessible from the Internet.
   ii. Email servers - Manage external email communications.

   Perimeter network benefit:

   - Prevents unauthorized access to the private network.
   - DMZ service is compromised, the attacker still cannot access sensitive data.

10. Describe two (2) scenarios where your corporate firewall will be used as a VPN server (i.e., what type of VPN connections are possible using a corporate firewall).

    Answer: Two VPN connections are possible used corporate firewall:

    - **Remote Employee Access (Client-to-Gateway VPN):** Employees working remotely can securely connect to the corporate network through a VPN tunnel.
    - **Inter-Office Secure Communication (Site-to-Site VPN):** Two office locations can establish a secure VPN connection over the Internet to share resources as if they were in the same physical location.

11. What is the very first step you should take when considering securing your network and why?

    Answer: The first step is to create a firewall policy that defines how inbound and outbound traffic should be managed. This ensures that security measures align with business requirements and risk assessments.

    Why:

    Understanding which assets need protection, the threats and vulnerabilities present, and the business requirements is essential before deploying any security devices. This analysis forms the basis for creating rules that explicitly permit only the necessary traffic.

12. Describe how does the concept of zero trust work in conjunction with Firewalls? Explain what must be changed to approach what is described by Zero Trust.

    Answer: The **Zero Trust model** operates on the principle of never trust, always verify, requiring strict authentication and access controls for all users and devices, regardless of their location. When applied to firewalls:

    - **Authentication and Access control:** zero trust firewall enforce multi factor authentication (MFA) and granular access policies based on user identity, device type, and location. This ensures that only verified entities can access specific resources.

- **Microsegmentation**: Network segmentation is a core feature, dividing the network into smaller zones to limit lateral movement of threats. Firewalls are configured to enforce strict rules between these zones.
- **Continuous Monitoring**: All traffic is inspected and logged to detect abnormal behavior or potential threats in real time.

To align with Zero Trust principles, organizations must:

- Replace implicit trust models with continuous verification.
- Implement micro segmentation and least-privilege access policies.
- Integrate advanced firewalls like Next-Generation Firewalls (NGFWs) for deeper inspection and control.

13. Name three (3) attacks that packet filtering firewalls cannot prevent.
    Answer: Packet filtering firewalls are limited in their capabilities and cannot prevent:
    - **Application-Layer Attacks**: These include SQL injection or cross-site scripting (XSS), which exploit vulnerabilities at higher OSI layers.
    - **Spoofing Attacks**: IP spoofing bypasses packet filters by mimicking trusted IP addresses.
    - **Encrypted Traffic Threats**: Malicious payloads within encrypted traffic go undetected by basic packet filtering firewalls

14. What is the significance of the default deny policy in firewalls?
    Answer: Traffic that is not explicitly allowed should be blocked by default. This reduces the risk of unauthorized access.
    - Prevents Unauthorized Access: Ensures no unintended traffic is permitted.
    - Reduces Attack Surface: Blocks unknown threats by default.
    - Forces Intentional Security Rules: Admins must define specific allow rules, reducing misconfigurations.
    - Minimizes Insider Threats: Restricts unnecessary internal communications.

15. What are the challenges of deploying firewalls in cloud environments, and how can they be addressed?
    Answer: Challenges of Deploying Firewalls in Cloud Environments & Solutions
    Challenges:
    - Complex Configuration: Cloud environments require intricate rule setups across diverse platforms.
    - Policy Consistency: Ensuring uniform security policies across multi-cloud environments is difficult.
    - Performance Impact: High traffic volumes can degrade firewall performance due to resource limitations.
    - Single Point of Failure: A malfunctioning cloud firewall can disrupt the entire network's security.

    Solutions:
    - Automate policy synchronization across platforms to maintain consistency.

- Use scalable cloud-native firewalls to handle high traffic efficiently.
- Implement redundancy mechanisms to avoid single points of failure

16. How do cloud-based firewalls differ from traditional hardware firewalls?

Answer: Cloud-based firewalls and traditional hardware firewalls differ in several key ways, reflecting their respective design purposes and deployment environments.

Feature	Cloud-Based Firewalls	Traditional Hardware Firewalls
Deployment	Virtual; no physical setup required	Requires physical installation
Scalability	Easily scalable; adjusts resources	Limited by hardware capacity
Cost Efficiency	Lower maintenance costs	Higher due to hardware upkeep
Flexibility	Accessible from anywhere	Restricted to on-premises environments
Updates	Automatic software updates	Manual updates often required

Cloud-based firewalls are ideal for dynamic, cloud-centric operations, while traditional firewalls suit static, on-premises setups

17. How does a Next-Generation Firewall (NGFW) differ from traditional firewalls?

Answer: Here's a concise comparison of Next-Generation Firewalls (NGFWs) and traditional firewalls:

Traditional Firewalls:

- **Focus:** Basic packet filtering (IP addresses, ports) and stateful inspection (tracking connections).
- **Strengths:** Simple, cost-effective for basic security needs.
- **Weaknesses:** Limited application awareness, no built-in intrusion prevention, vulnerable to sophisticated attacks.

Next-Generation Firewalls (NGFWs):

- **Focus:** Deep packet inspection (DPI), application awareness and control, integrated intrusion prevention, advanced threat intelligence.
- **Strengths:** Comprehensive protection against modern threats, granular control, improved visibility.

- **Weaknesses:** More complex, higher cost.

In a nutshell: Traditional firewalls provide a basic level of security, while NGFWs offer a more advanced and comprehensive approach to protect against today's cyber threats.