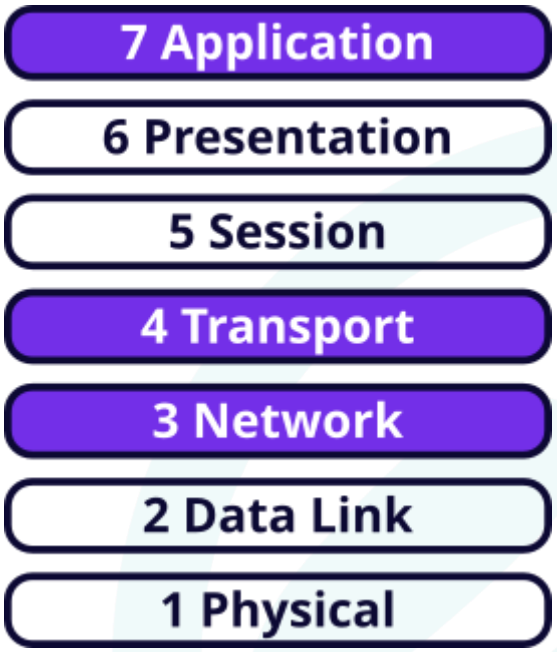
Network Layers

Understanding the different layers of the network stack is essential for protecting systems against a wide range of cyber threats. The **OSI** (Open Systems Interconnection) **model** is a conceptual framework that describes how networking protocols interact within a network. It separates network communication into seven layers, each with specific functions and responsibilities. By understanding how these layers operate and where they are vulnerable—particularly Layers 3, 4, and 7—you can better understand where threats may arise and how to deploy effective defenses. From securing data packets at the network level to protecting applications from sophisticated attacks, knowledge of network layers is foundational to building a robust cybersecurity strategy.



WEDOS.protection operates on Layers 3, 4 and 7.

Layer 3 – Network Layer Protection

Layer 3 handles the routing of data packets between devices across different networks. The primary protocol at this layer is the **IP** (Internet Protocol). Common threats include:

- **IP Spoofing**: Attackers forge (spoof) source IP addresses to bypass filters or disguise traffic origins.

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS)**: Attackers overwhelm network resources by flooding the target with traffic.
- **Man-in-the-Middle (MitM) Attacks**: Attackers intercept or alter traffic during transmission.

To mitigate these threats, you (or your web hosting / protection provider) can set up:

- **Firewalls and Routers.** Routers and firewalls are essential components of Internet infrastructure. Use routers for packet forwarding and routing. Use firewalls to enhance security and control the flow of traffic between network segments within your infrastructure.
- **IPsec (IP Security)**: IPsec is a suite of protocols used to secure IP communications, providing encryption, authentication, and data integrity between devices. It is widely used across the Internet for securing VPNs (Virtual Private Networks) and for encrypting communications. Use IPsec to secure communication between your servers.
- **Access Control Lists (ACLs)**: ACLs are a set of rules used to permit or deny traffic based on IP addresses, subnets, or ports. Use ACLs to control traffic to and from your servers, typically at the router or firewall level.
- **DDoS Protection**: Apply traffic filtering, rate-limiting, and challenge-response tools to reduce the impact of volumetric attacks on your infrastructure.

Layer 4 – Transport Layer Protection

Layer 4 handles end-to-end communication and error recovery. The primary protocols at this layer are **TCP** (Transmission Control Protocol) and **UDP** (User Datagram Protocol). Common threats include:

- **TCP SYN Flood**: Attackers exhaust server resources by sending a large number of SYN requests (used to establish a connection between a client and server) to a target.
- **Session Hijacking**: Attackers gain unauthorized access by exploiting an active session between two parties.
- **Port Scanning**: Attackers probe open ports to identify and exploit vulnerabilities.

To mitigate these threats, you (or your web hosting / protection provider) can set up:

- **Stateful Firewalls**: Stateful firewalls track the state of active connections and can filter traffic based on connection state, preventing SYN flood attacks.
- **Transport Layer Encryption**: **SSL** (Secure Sockets Layer) and **TLS** (Transport Layer Security) security protocols secure data transmissions between clients and servers, particularly for services like HTTPS, email, and VPNs.
- **Intrusion Detection/Prevention Systems (IDS/IPS)**: Deploy and configure IDS/IPS systems to detect and block malicious traffic and attacks targeting your servers or network infrastructure.
- **Rate Limiting**: Implement rate limiting to control the number of requests a client can make to a server within a certain timeframe. This is commonly used to protect against brute-force login attempts, excessive API calls, malicious scraping of web pages, and DDoS attacks.

Layer 7 – Application Layer Protection

Layer 7 handles application-specific communication such as HTTP for web browsing or SMTP for email. This layer is most closely tied to end-user services and functions. Common threats include:

- **Application Layer DDoS Attacks**: Attackers exploiting the application's vulnerability to cause service disruptions.
- **SQL Injection and Cross-Site Scripting (XSS)**: Attackers exploit improper input handling to access data or execute malicious code.
- **Web Application Vulnerabilities**: Attackers exploit weaknesses in application design, gaining unauthorized access or causing damage.

To mitigate these threats, you (or your web hosting / protection provider) can set up:

- **Web Application Firewalls (WAFs)**: WAFs protect web applications by filtering and monitoring incoming and outgoing HTTP traffic, blocking malicious traffic like SQL injection, cross-site scripting (XSS), and other OWASP Top 10 threats.
- **Content Delivery Networks (CDNs)**: CDNs optimize content delivery by caching content at edge locations. Use CDNs to absorb large-scale DDoS attacks at the edge of the network before they reach the origin server.
- **Secure Coding Practices** and **Patch Management**: Ensure applications are resistant to common attacks like SQL injection and buffer overflow by validating

inputs and using prepared statements. Avoid vulnerabilities by regularly updating software and libraries.

b2b@wedos.com
WEDOS.com

WEDOS Group SA
7 Rue Robert Stümper
L - 2557 Luxembourg
Luxembourg
EU