Layer wise security Concerns

- Physical layer – Frequency Jamming, Limited physical Security, Attacks on Channels
- Data Link Layer – Denial of service (DoS), Location privacy, Spoofing, Service Disruption
- Network Layer – DoS, Black Hole, Mobile addressing (handoff), Privacy, Serivce Disruption
- Transport Layer – Syn, flood, Split TCP (handoff)
- Session Layer- Session hijacking
- Presentation – Attack on Cryptography
- Application Layer – Billing, Service Awareness, Users Authentication, Data secrecy, Access control.

Application Layer

Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks

Presentation Layer

The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host

Session Layer

Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability

Transport Layer

Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service

Network Layer

Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance

DoS mitigation

Some DDoS Mitigation Actions and Hardware

- ☐ Stateful inspection firewalls
- ☐ Stateful SYN Proxy Mechanisms
- ☐ Limiting the number of SYNs per second per IP
- ☐ Limiting the number of SYNs per second per destination IP
- ☐ Set ICMP flood SCREEN settings (thresholds) in the firewall
- ☐ Set UDP flood SCREEN settings (thresholds) in the firewall
- ☐ Rate limit routers adjacent to the firewall and network

Data Link Layer

Disrupts the usual sender to recipient flow of data -- blasting across all ports	Many advances switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered

Physical Layer

Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets