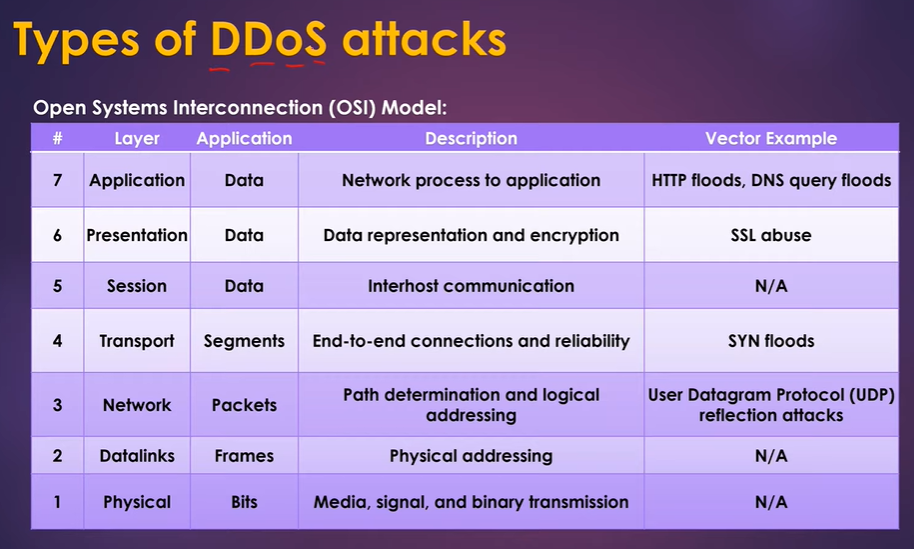
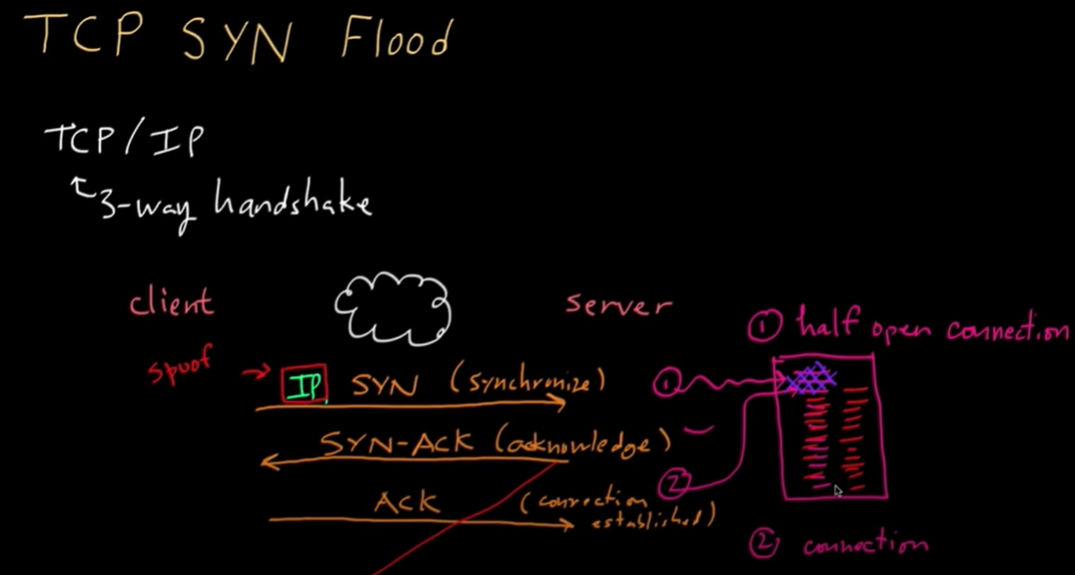
AWS Shield

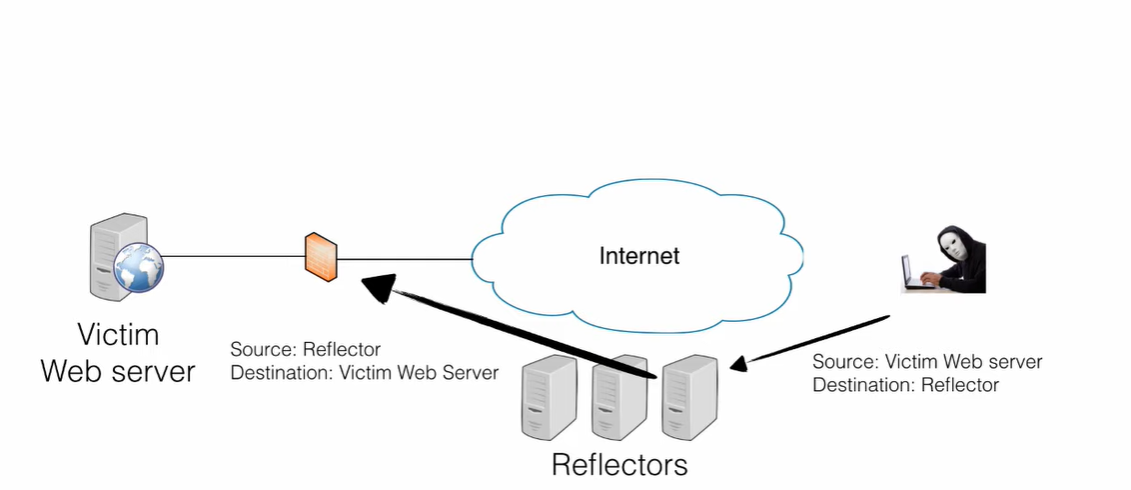
* AWS Shield is a service built on AWS to protect mainly against DDoS attacks. DDoS (Distributed Denial of Service) is an attack that uses a large number of servers to put a load on web services, bringing down servers and applications and making them unusable.
* AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS.
* provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.
* provides two tiers of AWS Shield: Standard and Advanced.
* AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services.
* AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator accelerators. AWS Shield Advanced incurs additional charges.
* You can use AWS WAF web access control lists (web ACLs) to help minimize the effects of a distributed denial of service (DDoS) attack. For additional protection against DDoS attacks, AWS also provides AWS Shield Standard and AWS Shield Advanced.
* While AWS WAF can mitigate DDoS attacks at layer 7 of the OSI reference model, AWS Shield protects web services from DDoS attacks at layer 3 and 4 of the OSI reference model.

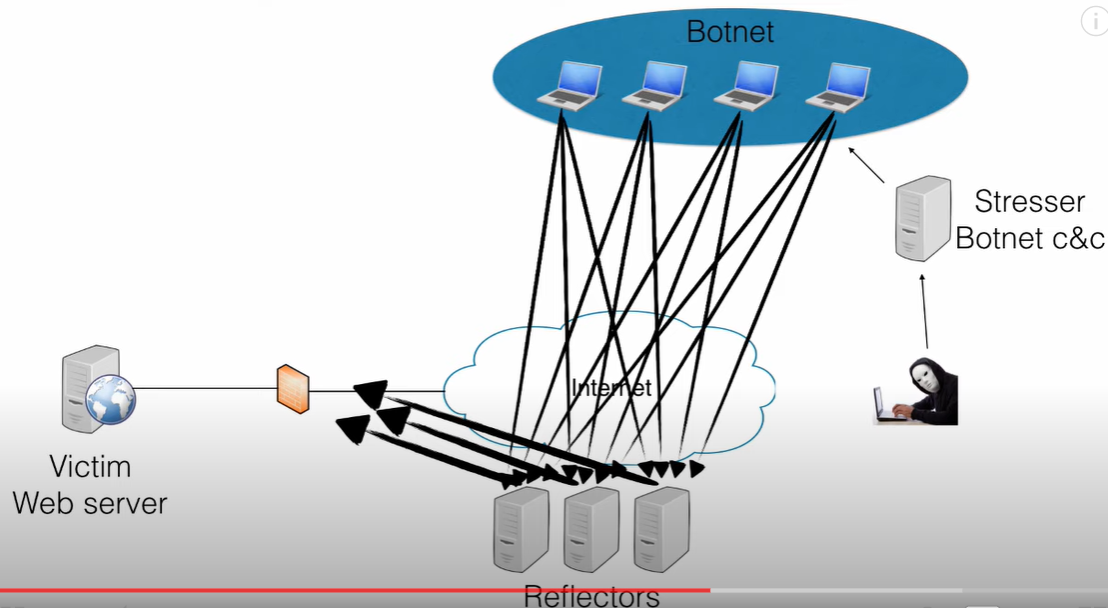


**TCP SYN Flood** : DDOS attacker can spoof fake IP which will not not release space on server resulting apps goes down.



**UDP reflection attack**: DDOS attacker use botnets to create traffic via reflector (which amplifies traffic) to increase traffic that could hit connection maximum bandwidth.





**DNS Query Attach**: DDOS attacker use botnets to create take traffic that can bring down DNS server.

