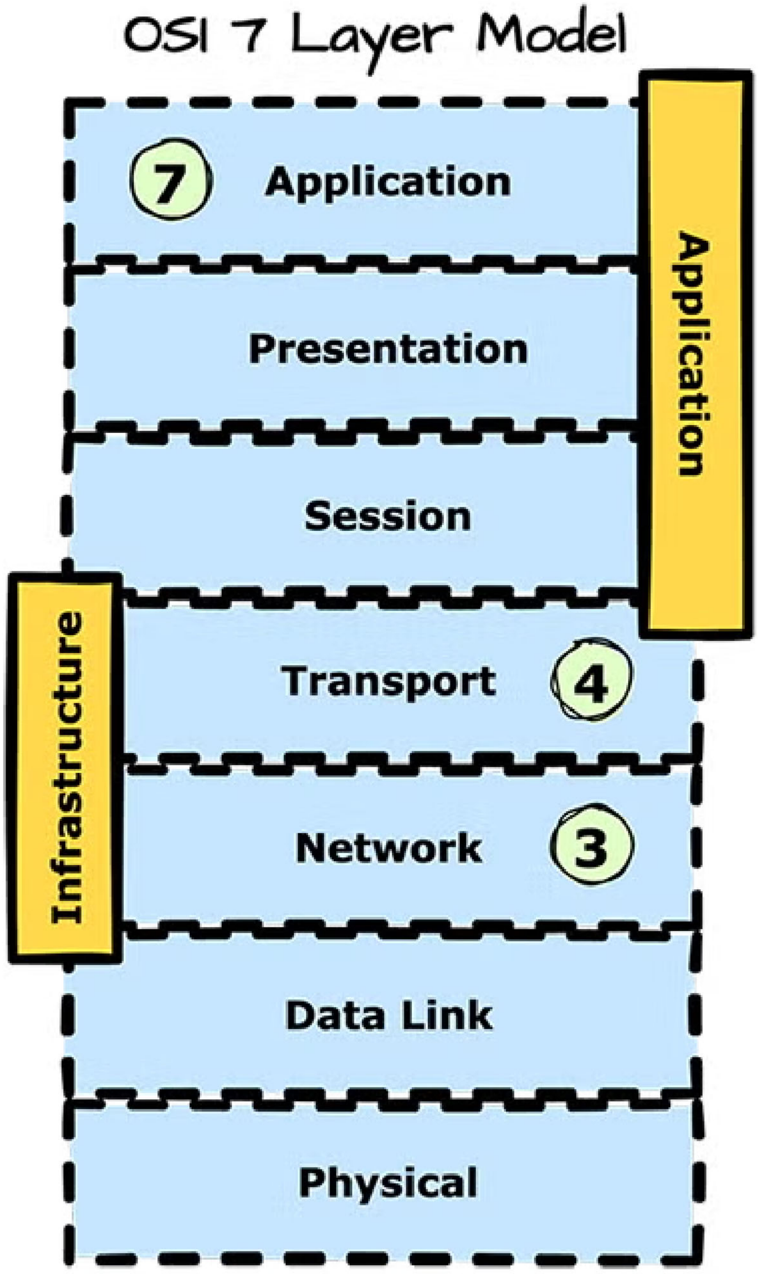
What is DDoS?

Before protecting against a Denial of Service (DOS) attack, you must understand what one is. A DoS attack is a malicious attempt to impact the availability of a targeted system. These systems range from applications to websites or even target end users directly. The target system is eventually overwhelmed by generating an abnormally large amount of packets. A Distributed Denial of Service (DDoS) attack is when the attacker uses multiple compromised sources to produce a volumetric attack.

You can group DDoS attacks based on the targeted Open Systems Interconnection (OSI) layer. Most common attacks happen at the Network (OSI layer 3), Transport (OSI layer 4), and Application (OSI layer 7) layers. Few of the many cyberattacks today are more overwhelming and devastating than DDoS attacks. NortonLifeLock calls DDoS attacks "one of the most powerful weapons on the internet"—and for a good reason. These malicious attacks can come at any time and take targeted websites offline, leading to massive service interruptions and substantial financial losses. Worse, the number of DDoS attacks worldwide is rising, with recent research depicting a 29% year-on-year increase in Q4 2021.



What is a layer 3/4 DDoS attack?

Layers 3 and 4 are the infrastructure layer. Common DDoS attack vectors at these layers include SYN floods, UDP floods, and Internet Control Message Protocol (ICMP) attacks. Layer 3 is the network layer responsible for deciding which physical path data should move through the network. Layer 4 provides data transfer between hosts and ensures data integrity and completeness of transfer performed by the Transport Control Protocol (TCP). Attacks targeting these two layers generate massive traffic volume and aim to overload the network's available capacity or group of hosts. The good news is these styles of attacks have clear signatures and are easier to detect and mitigate.

What is a layer 7 DDoS attack?

Layer 7 is the application layer. These attacks tend to be less common, while also being more sophisticated. From a volume standpoint, these attacks are less about a sudden influx of traffic than infrastructure layer attacks. Still, they target critical vital parts of the application, negatively impacting the performance of the target. A real-world example of this attack is to flood an application login page or target an exposed API with an expensive search request, resulting in a degraded experience for the end users. Reactive remediation of these attacks is costly. Small to medium-sized businesses (SMBs) spend an average of $120,000 restoring service and managing operations during a DDoS attack.

How can you protect your applications?

1. **Understand traffic patterns**
   The first line of defense is to create a traffic profile. This profile includes what "good" traffic looks like and sets expectations for expected traffic volumes across your network. Monitoring your traffic through this profile allows you to configure rules to accept as much traffic as your infrastructure can handle without impacting your end users. Rate limiting provides a baseline, and you can then put advanced detection methods in place to receive traffic that has been validated by analyzing additional variables. It takes one minor security blip to cause irreparable harm to your network and servers and send your employees through the five emotional stages of a DDoS attack. So do your diligence from the onset.

2. **Minimize exposure**
   One of the easiest ways to mitigate DDoS attacks is to shrink the surface area that can be attacked, ultimately reducing the options for attackers and enabling you to architect countermeasures and protections in one place. You should ensure that you are not exposing your applications and hosts to ports, protocols, and other applications from which you do not expect communication. In most cases, you can achieve this by placing your infrastructure resources behind a proxy Content Delivery Network (CDN), which restricts direct internet traffic to certain parts of your infrastructure. In other cases, you can use a firewall or Access Control Lists (ACLS) to control traffic reaching specific applications.

3. **Deploy an application-based firewall**
   If your application has internet access, you get attacked multiple times daily. On average, an application with internet connectivity gets attacked every 39 seconds. A good practice is to use a Web Application Firewall (WAF) against attacks. A good starting point is to mitigate OWASP Top 10 type attacks actively, and then you should be able to create a customized traffic profile against additional invalid requests. For example, these requests may be masquerading as legitimate traffic from known

malicious IPs or from a geographic part of the world in which you don’t do business. A WAF is also helpful in mitigating attacks as you can leverage experienced support to study the traffic heuristics and create custom-tailored protection for your application.

4. **Scale by design**
   While not the best solution in isolation, increasing your bandwidth (transit) capacity or server (computational) capacity to absorb and mitigate attacks may be an option. When designing and building your applications, make sure you have redundant connectivity to the internet that allows you to handle spikes in traffic. A common practice is to use load balancing to continually monitor and shift loads between available resources to prevent overloading any one point. Additionally, you can create your web applications with a CDN in mind, providing an additional layer of network infrastructure for serving content often closer to your end-users. Most DDoS attacks are volumetric and consume massive amounts of resources, and your application must scale up or down quickly on computation. The distributed nature of a CDN essentially spreads out the attack to the point that it becomes easily absorbed. CDNs also unlock additional methods to thwart the most sophisticated attacks. Developing an attack profile allows CDNs to remove or slow down malicious traffic.

So what now?

When fighting against today's highly sophisticated DDoS attacks, an ounce of prevention is worth a pound of cure. So make sure that at any given time, your organization is adequately prepared for, and can handle, much higher volumes of server traffic or network requests than you need. The best time to take action was yesterday; the second-best time is now.

If you need a hand fighting DDoS attacks, Fastly can help. Our high-bandwidth, globally distributed network can absorb DDoS attacks. Fastly's entire network acts as a DDoS scrubbing center, so you never have to sacrifice performance for protection. We allow you to respond in real-time, filtering out malicious requests at our network edge.

Watch this video to get a feel of how our high-performance DDoS mitigation service works, and try Fastly for free today!