A SYN flood can occur in three different ways:

1. Direct attack: A SYN flood where the IP address is not spoofed is known as a direct attack. In this attack, the attacker does not mask their IP address at all. As a result of the attacker using a single source device with a real IP address to create the attack, the attacker is highly vulnerable to discovery and mitigation. In order to create the half-open state on the targeted machine, the hacker prevents their machine from responding to the server’s SYN-ACK packets. This is often achieved by firewall rules that stop outgoing packets other than SYN packets or by filtering out any incoming SYN-ACK packets before they reach the malicious users machine. In practice this method is used rarely (if ever), as mitigation is fairly straightforward – just block the IP address of each malicious system. If the attacker is using a botnet such as the Mirai botnet they won’t care about masking the IP of the infected device

2. Spoofed Attack: A malicious user can also spoof the IP address on each SYN packet they send in order to inhibit mitigation efforts and make their identity more difficult to discover. While the packets may be spoofed, those packets can potentially be traced back to their source. It’s difficult to do this sort of detective work but it’s not impossible, especially if Internet service providers (ISPs) are willing to help.

3. Distributed attack (DDoS): If an attack is created using a botnet the likelihood of tracking the attack back to its source is low. For an added level of obfuscation(Confusion resulting from failure to understand), an attacker may have each distributed device also spoof the IP addresses from which it sends packets. If the attacker is using a botnet such as the Mirai botnet, they generally won’t care about masking the IP of the infected device

By using a SYN flood attack, a bad actor can attempt to create denial-of-service in a target device or service with substantially less traffic than other DDoS attacks. Instead of volumetric attacks, which aim to saturate the network infrastructure surrounding the target, SYN attacks only need to be larger than the available backlog in the target’s operating system. If the attacker is able to determine the size of the backlog and how long each connection will be left open before timing out, the attacker can target the exact parameters needed to disable the system, thereby reducing the total traffic to the minimum necessary amount to create denial-of-service.

Botnet means: a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam messages.

Masking IP Address: Using VPN, Proxy and using other method you may hide your IP address or public IP address.