SYN flood DDoS attack

Archived: 2026-04-05 23:19:16 UTC

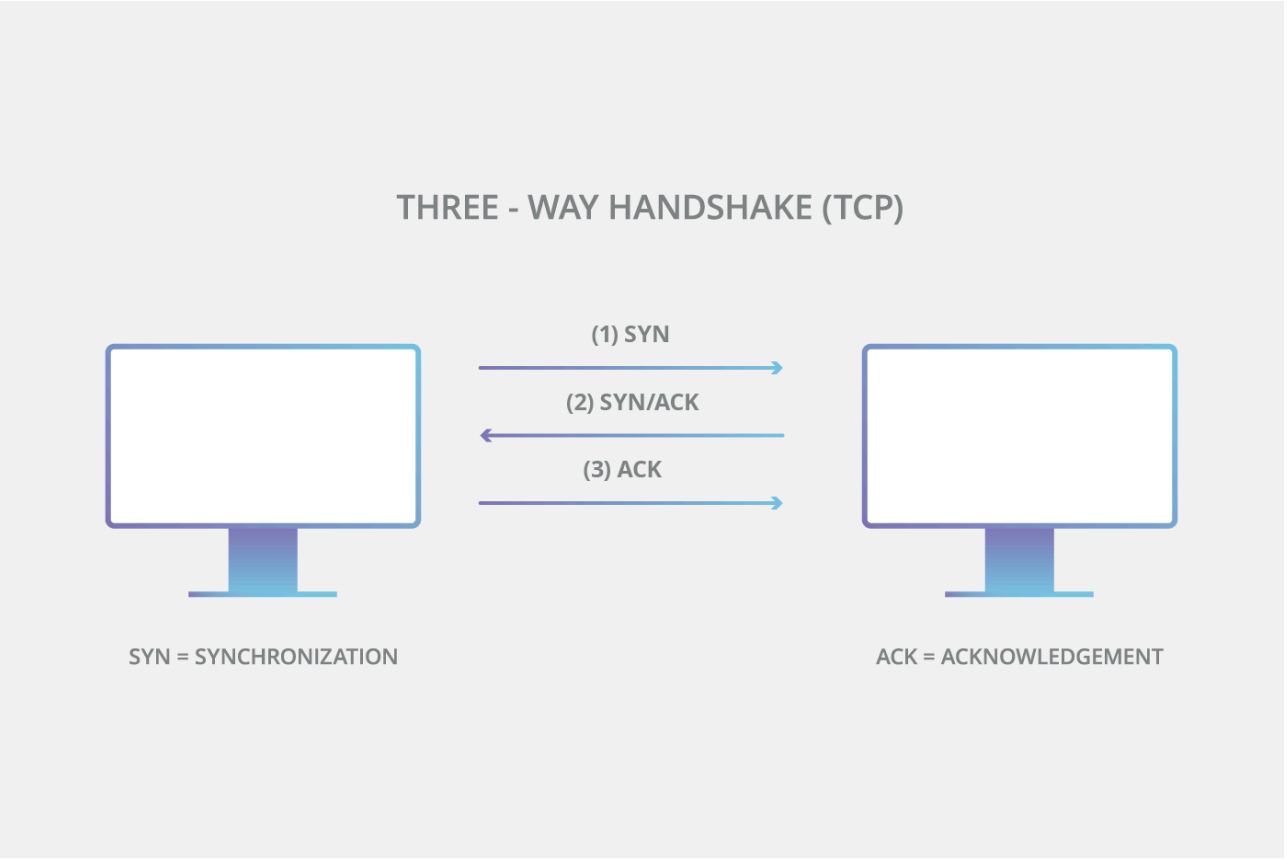
What is a SYN flood attack?

A SYN flood (half-open attack) is a type of denial-of-service (DDoS) attack which aims to make a server unavailable to legitimate traffic by consuming all available server resources. By repeatedly sending initial connection request (SYN) packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device to respond to legitimate traffic sluggishly or not at all.

How does a SYN flood attack work?

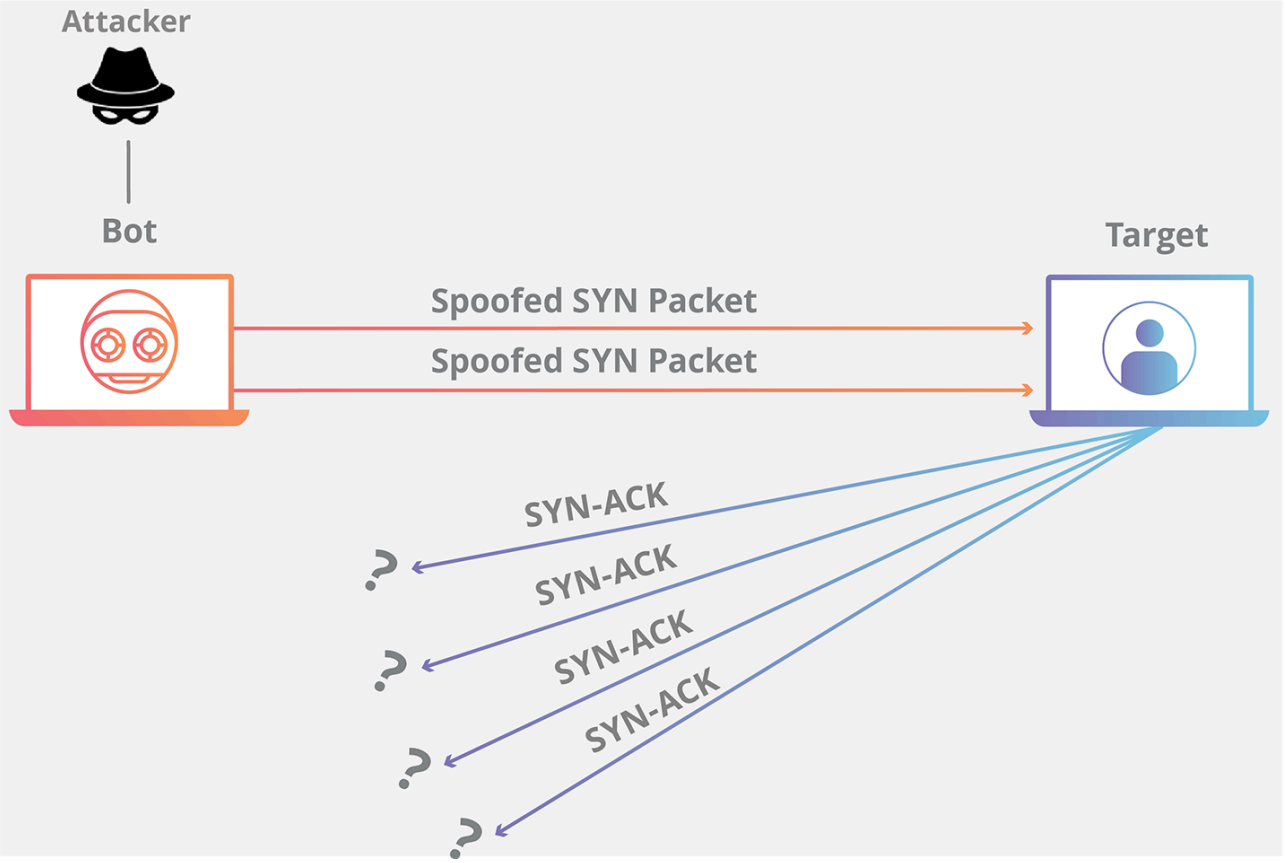
SYN flood attacks work by exploiting the handshake process of a TCP connection. Under normal conditions, TCP connection exhibits three distinct processes in order to make a connection.

1. First, the client sends a SYN packet to the server in order to initiate the connection.
2. The server then responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication.
3. Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.



To create denial-of-service, an attacker exploits the fact that after an initial SYN packet has been received, the server will respond back with one or more SYN/ACK packets and wait for the final step in the handshake. Here's how it works:

1. The attacker sends a high volume of SYN packets to the targeted server, often with spoofed IP addresses.
2. The server then responds to each one of the connection requests and leaves an open port ready to receive the response.
3. While the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the server to temporarily maintain a new open port connection for a certain length of time, and once all the available ports have been utilized the server is unable to function normally.



In networking, when a server is leaving a connection open but the machine on the other side of the connection is not, the connection is considered half-open. In this type of DDoS attack, the targeted server is continuously leaving open connections and waiting for each connection to timeout before the ports become available again. The result is that this type of attack can be considered a “half-open attack”.

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 user's 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, 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.

How is a SYN flood attack mitigated?

SYN flood vulnerability has been known for a long time and a number of mitigation pathways have been utilized. A few approaches include:

Increasing Backlog queue

Each operating system on a targeted device has a certain number of half-open connections that it will allow. One response to high volumes of SYN packets is to increase the maximum number of possible half-open connections the operating system will allow. In order to successfully increase the maximum backlog, the system must reserve additional memory resources to deal with all the new requests. If the system does not have enough memory to be able to handle the increased backlog queue size, system performance will be negatively impacted, but that still may be better than denial-of-service.

Recycling the Oldest Half-Open TCP connection

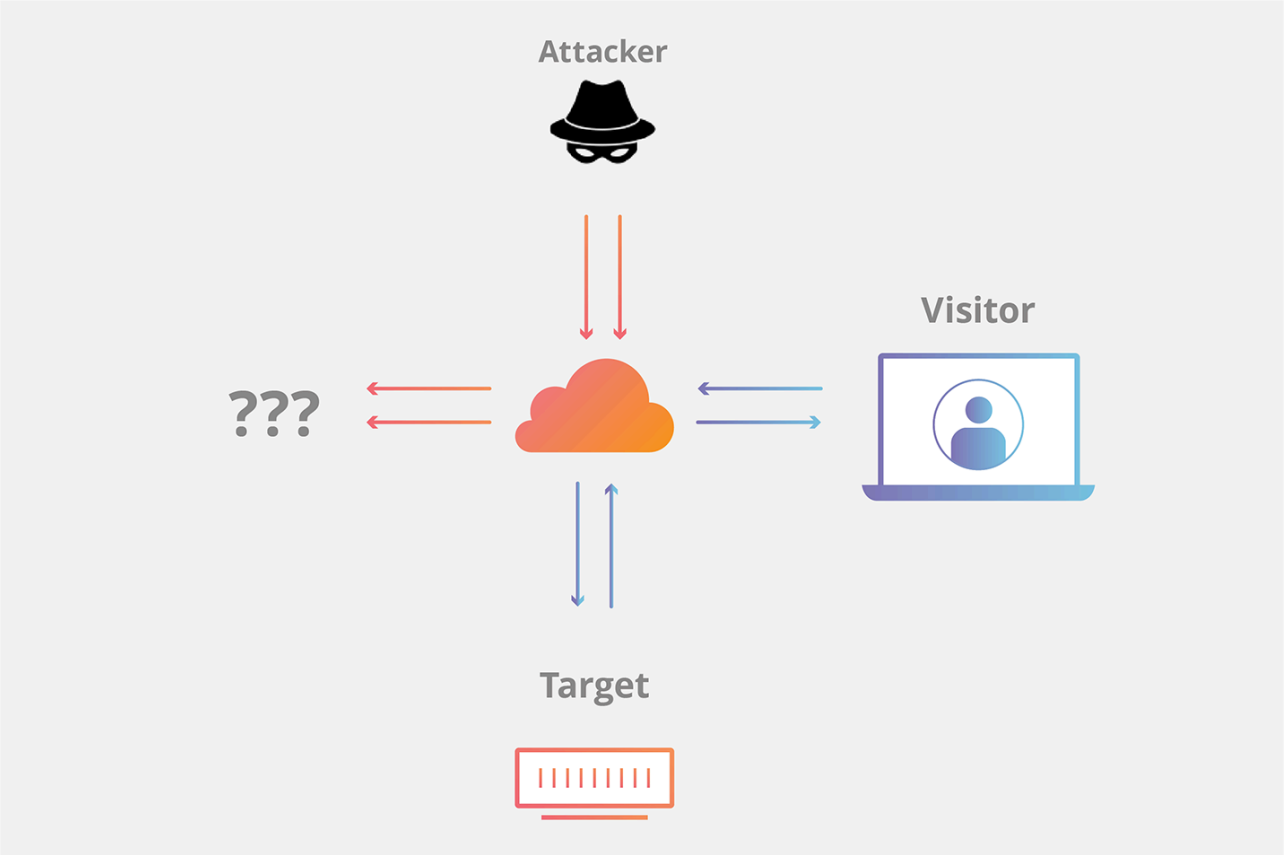
Another mitigation strategy involves overwriting the oldest half-open connection once the backlog has been filled. This strategy requires that the legitimate connections can be fully established in less time than the backlog can be filled with malicious SYN packets. This particular defense fails when the attack volume is increased, or if the backlog size is too small to be practical.

SYN cookies

This strategy involves the creation of a cookie by the server. In order to avoid the risk of dropping connections when the backlog has been filled, the server responds to each connection request with a SYN-ACK packet but then drops the SYN request from the backlog, removing the request from memory and leaving the port open and ready to make a new connection. If the connection is a legitimate request, and a final ACK packet is sent from the client machine back to the server, the server will then reconstruct (with some limitations) the SYN backlog queue entry. While this mitigation effort does lose some information about the TCP connection, it is better than allowing denial-of-service to occur to legitimate users as a result of an attack.

How does Cloudflare mitigate SYN Flood attacks?

Cloudflare mitigates this type of attack in part by standing between the targeted server and the SYN flood. When the initial SYN request is made, Cloudflare handles the handshake process in the cloud, withholding the connection with the targeted server until the TCP handshake is complete. This strategy takes the resource cost of maintaining the connections with the bogus SYN packets off the targeted server and places it on Cloudflare's Anycast network. Learn more about how Cloudflare's DDoS Protection works.



Source: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/