How to Prevent DDoS Attacks

DDoS attack means a distributed denial-of-service attack. It is a malicious attempt to disrupt the regular traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. It achieves effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. It is mainly carried out with networks of Internet-connected machines. A DDoS attacker uses malware-infected devices that allow the target devices to be controlled by the DDoS attacker. These individual devices are called bots, and a group of bots is called a botnet. The DDoS attacker can attack devices by the botnet by sending remote instructions to each bot. Furthermore, each bot sends requests to the target's IP address, which causes the server or network to become overwhelmed. Therefore, a DDoS attack occurs. To prevent the DDoS attack on a serious note, we must follow six steps. Firstly, we must buy more bandwidth for our server or network. The use of bandwidth means unlimited bandwidth. Secondly, we must build redundancy into our infrastructure. Thirdly, we must configure our network hardware against DDoS attacks. Fourthly, we must deploy anti-DDoS hardware and software modules. Fifthly, we must deploy a DDoS protection appliance. Sixthly, we must protect our DNS server. If we use a firewall or a DDoS shield in our devices, that firewall or DDoS shield allows only one request from the DDoS attack and rejects the rest. When the firewall or DDoS shield detects the unusual request from one IP address simultaneously, it directly blocks that IP address for the following server or network. One of the best companies for the DDoS shield is Cloudflare. When a request comes into our server or network, it is directly sent to the Cloudflare Edge, where the request is scanned to detect only one single request from one dedicated IP address. When the Cloud Edge confirms all conditions, it sends the request to our original server or network. Furthermore, if it detects more than one request from the same IP address, it directly blocks that IP address and can never send it to the original server or network, preventing DDoS attacks. Therefore, we can prevent DDoS attacks from our servers or networks by following the above six steps.