What are the counter-measures of DDOS attack?

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

As a general rule, there are two ways to prevent DDoS attacks using manual operations:
System optimization - Optimize and enhance key parameters of core devices and systems to improve resiliency in the case of a DDoS attack. This method works only in the event of a low-traffic DDoS attack, a large attack (either in bandwidth or packets per second) will quickly overwhelm these defenses.
Source IP tracing - Most system administrator\'s first response when under a DDoS attack would be to consult the uplink network service carriers to find out the source of the attack and null-route it. But if the source IP address of the DDoS attack is forged, the process of finding the attack source often involves many carriers and organizations. Even if the attack source is found out, blocking the traffic from there may cause the loss of normal traffic (you cut off the good along with the bad - effectively DoSing yourself). Moreover, the prevailing Botnets and newer, more sophisticated DDoS attacks make it impossible to prevent DDoS attacks by network tracing, as the sources are many and changing.Firewalls
Firewalls are the most commonly used security products, and something that every business should use. They do a great job at what they are designed for, but DDoS attack prevention is not a core function in its design. In
some cases, firewalls even become the target of DDoS attacks and cause denial of service of the entire network.
Deficiency of DDoS detection capability Firewalls are usually deployed in the network as Layer-3 packet forwarding devices. They not only protect the intranet but also provide access for devices that provide external
Internet services for internal needs. If DDoS attacks exploit legal protocols allowed by servers, firewalls will be
unable to identify attack traffic from the hybrid traffic precisely. Although some firewalls are equipped embedded modules that can detect attacks, the detection mechanisms are generally based on signatures and firewalls can fail to notice the attacks if DDoS attackers change packets slightly. The detection of DDoS attacks
is most effective using an algorithm of behavior patterns.
Limitation of calculation capability Traditional firewalls perform intensive deep packet inspection to detect DDoS attacks, which costs a lot of processing power. The potential massive traffic seen in DDoS attacks will cause a severe impact to the firewall\'s performance, resulting in the ineffective completion of the packet forwarding tasks.
The deployment locations also influence firewalls\' capability to prevent DDoS attacks. Traditional firewalls are
generally deployed at the network ingress. This type of deployment is a good way to protect all resources inside the network, but firewalls in this kind of deployment often become the victims in DDoS attacks

IPS/IDS
Currently, the most commonly used tools for attack prevention or detection are the IPS (Intrusion Prevention System) and IDS (Intrusion Detection System). But when it comes to DDoS attacks, IPS/IDS products often fall short of full protection.
The reason is that although the IDS can detect attacks at the application layer, its most basic level is a signature-based mechanism that needs recovering protocol sessions. But most of todayâ??s attacks adopt legal packets to hit the targets, and the IPS/IDS products can hardly detect these attacks. Some newer IPS/IDS

products have the capability of detecting anomalous protocols, but they take effect only after the manual configuration by security experts, and this is a complex and inelastic process. Another concerns is the same as with Firewalls - under a massive attack, deep-packet inspection can take a heavy toll on processing power (can your IPS handle 15 MILLION packets per second?).
IPS/IDS products were initially designed to be a signature-based attack prevention/detection tool for the application layer. But most of DDoS attacks still feature protocol anomalies at layer 3 and layer 4, many IPS/IDS will fail to detect, making them unsuitable for DDoS detection and prevention.