What are DoS and DDoS denial of service attacks? What are their harmful effects?

What are DoS, DDoS, what are the signs to recognize DoS, DDoS and what are their harmful effects? In this article, TipsMake.com.com will find out with you.

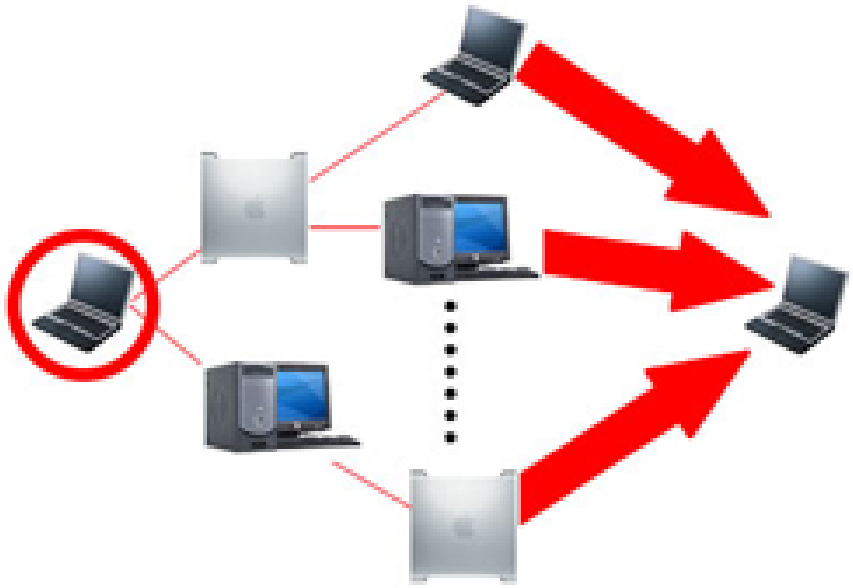
You may have heard a lot about DoS, DDoS or denial of service attacks and may have also been a victim of this type of attack. So what are DoS, DDoS, what are the signs to recognize DoS, DDoS and what are their harmful effects? In this article, TipsMake will help you learn about this classic type of attack, as well as give you some things to do if you suspect your service is being DDoS, and how to check and prevent DDoS attacks. applied in data centers.

What is DoS?

DoS's full English name is Denial of Service, translated into Vietnamese as denial of service. A DoS attack is an attack aimed at bringing down a server or network, making it impossible for other users to access that server/network. The attacker does this by massively "smuggling" traffic or sending information that can trigger an incident to the target server, system or network, thereby causing legitimate users (employees, members, account owners) cannot access the services and resources they expect.

Victims of DoS attacks are often web servers of high-end organizations such as banks, commercial enterprises, media companies, newspaper sites, social networks.

For example, when you enter a website's URL into your browser, you are sending a request to the website's server to view it. The server can only process a certain number of requests at a time, so if an attacker floods the server with many requests, it will overload it and your request will not be processed. This is a type of 'denial of service' because it makes it impossible for you to access that page.



Attackers can use spam to perform similar attacks on your email account. Whether you have a company email account or use a free service like Gmail, there is still a limit to the amount of data in your account. By sending multiple emails to your account, an attacker can fill up your inbox and prevent you from receiving further emails.

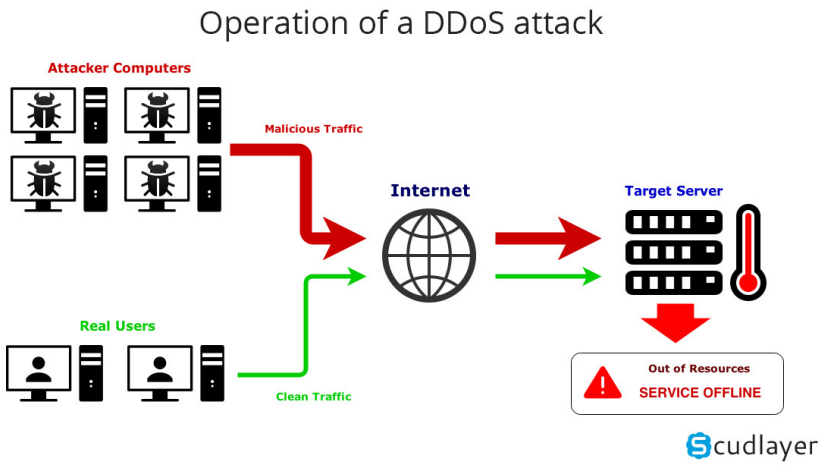
What is DDoS?

DDoS (Distributed Denial of Service), Vietnamese meaning is distributed denial of service. A DDoS attack is an attempt to bring down an online service by flooding it with traffic from multiple sources.

During DDoS, attackers can use your computer to attack other computers. By taking advantage of security holes and ignorance, this person can gain control of your computer. They then use your computer to send large amounts of data to a website or send spam to an email address. This is a distributed attack because the attacker uses many computers, including yours, to perform Dos attacks.

Although DDoS offers a less complex attack mode than other forms of cyberattacks, they are becoming more powerful and sophisticated. There are three basic types of attacks:

1. Volume-based: Uses high traffic to flood network bandwidth
2. Protocol: Focuses on exploiting server resources
3. Application: Focuses on web applications and is considered the most sophisticated and serious type of attack



DDoS attacks are carried out against a network of machines connected to the Internet.

These networks include computers and other devices (such as IoT devices) that have been infected with malware, allowing attackers to control them remotely. These individual devices are called bots (or zombies), and a group of bots is called a botnet. Once the botnet has been established, an attacker can direct an attack by sending remote instructions to each bot.

When a victim's server or network is targeted by a botnet, each bot sends requests to the target's IP address, potentially overloading the server or network, resulting in denial of service to traffic. normal traffic. Because each bot is a legitimate Internet device, separating attack traffic from regular traffic will be difficult.

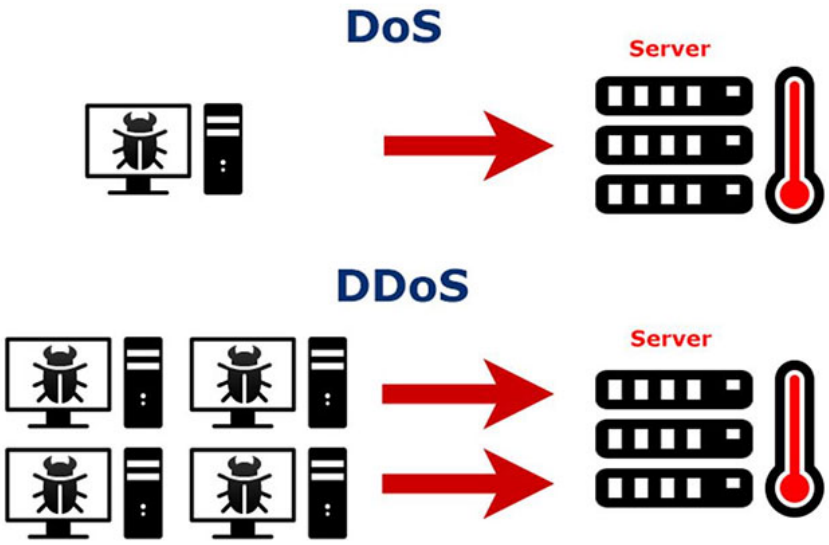
The most obvious symptom of a DDoS attack is a website or service that suddenly becomes slow or unavailable. But because some causes - such traffic spikes - can create similar performance problems, further investigation is often needed. Traffic analysis tools can help you detect some of the following telltale signs of a DDoS attack:

1. Suspicious amount of traffic originating from an IP address or IP range
2. Large amounts of traffic from users who share a behavioral profile, such as device type, geographic location, or web browser version
3. An unexplained increase in requests to a page or endpoint
4. Strange traffic patterns such as spikes at specific hours of the day or that appear unnatural (for example, spikes every 10 minutes)
5. There are other, more specific signs of a DDoS attack that can vary depending on the type of attack.

Difference between DoS and DDoS attacks

In short, a DoS attack means a computer sends a large amount of traffic to the victim's computer and "crashes" it. A DoS attack is an online attack used to make a website unavailable to users, when performed on a website. This attack causes the server of a website connected to the Internet to "crash" by sending a large amount of traffic to it.

In DDoS attacks, attacks are carried out from many different locations using multiple systems.



These two types of attacks have the following differences:

DOS	DDOS
DoS stands for Denial of service.	DDoS stands for Distributed Denial of service.
In a DoS attack, only one system targets the victim system.	In DDos, multiple systems attack the victim system.
The targeted PC is loaded from data packets sent from a single location.	The targeted PC is loaded from data packets sent from multiple locations.
DoS attacks are slower than DDoS.	DDoS attacks are faster than DoS attacks.
Can be blocked easily because only one system is used.	It is difficult to prevent this attack because multiple devices are sending packets and attacking from multiple locations.
In a DoS attack, only a single device is used with DoS attack tools.	In a DDoS attack, multiple bots are used to attack at the same time.
DoS attacks are easy to track.	DDoS attacks are difficult to track.
Traffic during a DoS attack is less than during a DDoS.	DDoS attacks allow attackers to send large amounts of traffic to the victim network.
Types of DoS attacks are: 1. Buffer overflow attack 2. Ping of Death or ICMP flood attack 3. Teardrop attack	Types of DDoS attacks are: 1. Volumetric attack (bandwidth attack) 2. Fragmentation attack (data fragmentation) 3. Application Layer Attack (exploiting vulnerabilities in applications)

Harmful effects of DoS and DDoS

These are the typical consequences that DDoS and DoS cause:

1. Systems and servers affected by DoS will crash, making it impossible for users to access
2. Businesses that own servers and systems will lose revenue, not to mention the costs needed to fix problems.

3. When the network goes down, all work that requires the network cannot be performed, interrupting work and affecting work performance.
4. If users access the website when it crashes, it will affect the company's reputation. If the website crashes for a long time, users may leave and choose another service instead.
5. Highly technical DDoS attacks can lead to the theft of money and customer data of the company.

Common types of denial of service attacks today

SYN Flood:

SYN Flood exploits a weakness in the TCP connection chain, known as the three-way handshake. The server will receive a synchronization message (SYN) to initiate the "handshake". The server receives the message by sending an acknowledgment (ACK) flag to the originating host, then closes the connection. However, in a SYN Flood, spoofed messages are sent and the connection is not closed => the service crashes.

UDP Flood:

User Datagram Protocol (UDP) is a sessionless network protocol. A UDP Flood targets random ports on a computer or network with UDP packets. The server checks for applications at those ports but finds none.

HTTP Flood:

HTTP Floods are almost like legitimate GET or POST requests exploited by a hacker. It uses less bandwidth than other types of attacks but it can force the server to use maximum resources.

Ping of Death:

Ping of Death manipulates IP protocols by sending malicious code to a system. This type of DDoS was popular two decades ago but is no longer effective today.

Smurf Attack:

Smurf Attack exploits Internet Protocol (IP) and ICMP (Internet Control Message Protocol) using a malware program called smurf. It spoofs an IP address and uses ICMP, then pings IP addresses on a given network.

Fraggle Attack:

Fraggle Attack uses a large amount of UDP traffic to the router's broadcast network. It's like a Smurf attack, using UDP more than ICMP.

Slowloris:

Slowloris allows attackers to use minimal resources in an attack and target web servers. Once connected to the desired target, Slowloris keeps that link open as long as possible with HTTP flooding. This type of attack has been used in several high-profile hacktivist DDoSings, including the 2009 Iranian presidential election. Mitigating the impact of this type of attack is critical. hard.

Application Level Attacks:

Application Level Attacks exploit vulnerabilities in applications. The target of this type of attack is not the entire server, but applications with known weaknesses.

NTP Amplification:

NTPAmplification exploits NTP (Network Time Protocol) servers, a protocol used to synchronize network time, to flood UDP traffic. This is an amplified reflection attack. In any reflection attack, there will be a response from the server to the fake IP. When amplified, the response from the server will no longer match the original request. Because it uses large bandwidth when suffering from DDoS, this type of attack is highly destructive and volumne.

Advanced Persistent DoS (APDoS):

Advanced Persistent DoS (APDoS) is a type of attack used by hackers hoping to cause serious damage. It uses many of the attacks mentioned previously (HTTP Flood, SYN Flood, etc.) and is typically aimed at sending millions of requests/second. APDoS attacks can last for weeks, depending on the hacker's ability to switch tactics at any time and create variety to avoid security protections.

Zero-day DDoS Attacks:

Zero-day DDoS Attacks is the name given to new DDoS attack methods that exploit unpatched vulnerabilities.

HTTP GET

HTTP GET is an application layer attack, smaller in scale and more targeted. Application Level Attacks exploit vulnerabilities in applications. The target of this type of attack is not the entire server, but applications with known weaknesses.

This type of attack will target Layer 7 of the OSI model. This is the layer with the highest network traffic, instead of targeting the third layer that is often chosen as the target in Bulk Volumetric attacks. HTTP GET exploits the submission process of some web browser or HTTP application and requests an application or server for each HTTP request, which is either a GET or POST.

HTTP Floods are almost like legitimate GET or POST requests exploited by a hacker. It uses less bandwidth than other types of attacks but it can force the server to use maximum resources. This type of attack is difficult to defend against because they use standard URL requests, rather than corrupted or high-volume scripts.

How to avoid denial of service attacks?

There really is no specific way to avoid becoming a victim of DoS or DDoS. However, we will introduce you to a few steps with the aim of somewhat reducing the type of attack that will use your computer to attack other computers.

1. Install and maintain anti-virus software.

2. Install a firewall and configure it to limit traffic to and from your computer.

3. Follow safe practice guidelines for distributing your email addresses.

4. Use email filters to help you manage unwanted traffic.

Specifically, for a data center, for example, the following preventive measures should be implemented:

ISPs often have DDoS protection at layers 3 and 4 (network traffic), but ignore Layer 7, which is more targeted, and overall the uniformity of protection layers is not good. ensure.

Companies handle DDoS: they use their existing infrastructure to fight any threat that comes their way. Typically, this is done through a load balancer, a content delivery network (CDN), or a combination of both. Smaller websites and services can outsource to third parties if they do not have the capital to maintain a bunch of servers.

Anti-DDoS service providers are always available. Typically, they will reroute your incoming traffic through their own system and "scrubbing" it against known attack methods. They can scan for suspicious traffic from sources or from uncommon geolocations. Or they can also reroute your legitimate traffic away from botnet sources.

Most modern firewalls and Intrusion Protection Systems (IPS) provide defense against DDoS attacks. These devices can take the form of a single device that scans all traffic to the system or software distributed at the server level. Dedicated anti-DDoS applications are also available on the market and can provide better protection against attacks targeting Layer 7.

Regularly scanning your network and monitoring traffic with alerts can also help you catch the risks of a DDoS attack early, as well as take action to minimize the damage.

Recognize Dos and DDos attacks

Not every complete failure of service is the result of a denial of service attack. There are many technical problems with a network or with the administrators performing maintenance and management. However, with the following symptoms you can recognize a DoS or DDoS attack:

1. Unusually slow network performance (opening files or accessing websites)

2. If you can't access the website, you still look at it

3. Cannot access any website

4. The number of letters has increased dramatically in your account.

What should you do if you think you are experiencing a denial of service attack?

Even if you correctly identify a DoS or DDoS attack, you cannot identify the source or destination of the attack. Therefore, you should contact technical experts for support.

1. If you find that you cannot access your own files or any external websites from your computer, you should contact the network administrator of that network. This could indicate whether your computer or your organization's network is under attack.

2. If you notice problems with your computer, contact your service provider (ISP). If there are problems, your ISP can advise you on appropriate actions.

Inspection and preparation work in response to DDoS at data centers

When you have a DDoS protection system in place, the first step to take is to identify attack vectors and critical applications. Which port is open? What bandwidth is available for you to use? Where is there likely to be network congestion? Which critical systems require additional protection?

Pay extra attention to areas of vulnerability based on dependencies on other systems in your infrastructure, for example central databases that may remove functionality for some applications in case it gets overloaded.

There are many open source software tools you can use to test mitigation from DDoS, as well as hardware options that can reach multi-gigabit throughput levels. However, hardware options will be a costly solution. Instead, a professional white hat security company can provide you with testing as an optional service.

DDoS attacks will certainly cause a lot of trouble, but with careful preparation, you can be ready to prevent or come up with solutions quickly, thereby avoiding disruptions. services for users while significantly minimizing the damage caused by DDoS.