IPSERVERONE®

IPSERVERONE

DDoS Protection

A-1-1 & A-1-2, Block A,
Glomac Damansara,
Jalan Damansara,
60000 Kuala Lumpur,
Wilayah Persekutuan, Malaysia.

T. +603 2026 1688
F. +603 7728 3188
E. sales@ipserverone.com

www.ipserverone.com

ISO Certificate No: IS 651738

bsi. ISO/IEC 27001 Information Security Management

" Don't be the next victim of a DDoS attack ... ... "

What is a DDoS attack?

In a distributed denial-of-service (DDoS) attack, an attacker may use multiple systems to perform a denial-of-service attack, also known as a DoS attack. By taking advantage of security vulnerabilities or weaknesses, an attacker can easily take control of your online business by overloading or flooding it with an amount of data that it cannot handle.

DDoS attacks have become a common way for sabotaging businesses, consuming all your resources while jeopardising business continuity and causing revenue loss. Have you ever wondered where all the unnecessary traffic comes from when your network is under heavy load?

What are the signs of a denial of service attack?

If a system that handles the day to day operations smoothly; encounters a period of excessive load suddenly and the services that are offered by the system are experiencing an unusual slow down, then it is possible that the server is currently experiencing an attempted denial-of-service attack.

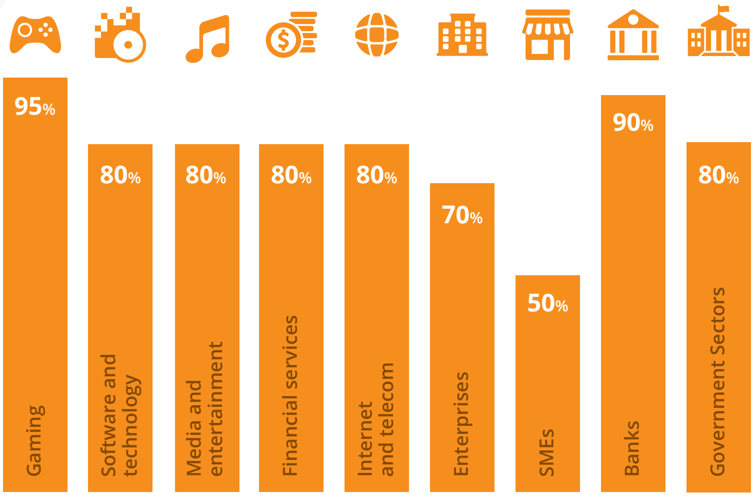
The financial impact of distributed DDoS attacks

In any DDoS attack there are both direct and indirect costs to the victim. Direct costs, in general, are easier to measure and can be immediately associated with the attack. Indirect costs, on the other hand, are more difficult to identify and their effects are often not felt for weeks, months or in some cases years following the actual attack itself.

The impact of a successful DDoS attack is widespread. Site performance is severely compromised, resulting in frustrated customers and other users. Service-level agreements (SLAs) are violated, triggering costly service credits. Company reputations are tarnished, sometimes permanently. Lost revenue, lost productivity, increased IT expenses, litigation costs—the losses just keep mounting.

What industry is the most often affected by DDoS attacks?

Whether you are the owner of a large enterprise, a small business, an e-commerce company or a government institution; if your business is the internet related, it can easily be a potential target where no industry is completely immune to these attacks.



Different kinds of DDoS attacks

01 Volumetric Based Attacks

These attacks are characterized by the presence of an abnormal and overwhelming number of packets on the network. Threat actors attempt to consume all available network bandwidth and/or exhaust router, switch and server forwarding capacity by flooding these devices with malicious traffic so that legitimate user traffic is starved. Some examples of volumetric based attacks include UDP, ICMP and SYN flood attacks.

02 Application Based Attacks

Application Based Attacks are designed to exploit weaknesses or software defects that exist in the protocols and applications themselves. They attempt to disrupt service by consuming CPU, memory or storage resources in target servers that are running the application so that the application is no longer able to serve legitimate users. They may also attempt to crash the application by supplying malformed messages or unanticipated input to the application. Some examples of application attacks include HTTP GET/POST attacks, SIP header manipulation attacks and SQL injection attacks.

03 Bandwidth Attacks

These DDoS attacks consume resources such as network bandwidth or equipment by overwhelming one or the other (or both) with a high volume of packets. Routers, servers and firewalls all of which have limited processing resources are rendered unavailable for valid transactions and can fail under the load. The most common form of bandwidth attack is a packet-flooding attack, in which a large number of seemingly legitimate TCP, UDP or ICMP packets are directed to a specific destination. To make detection even more difficult, such attacks might also spoof the source address — that is, misrepresent the IP address that supposedly generated the request to prevent identification.

04 Hybrid Attacks

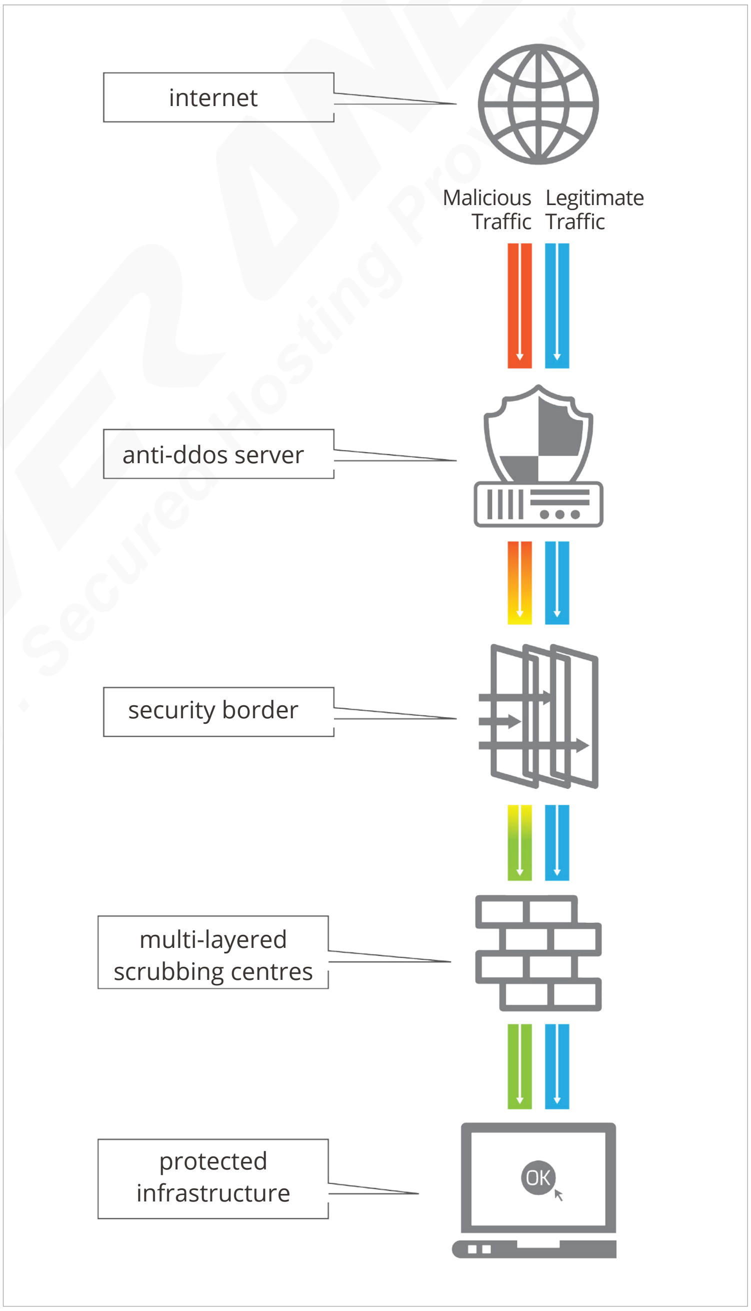
Modern DDoS attacks are very sophisticated and often blend several volumetric and application based attacks in order to disrupt service. These so called “hybrid” attacks attempt to consume all network bandwidth while simultaneously exhausting server resources. Frequently these attacks are used to not only create a catastrophic denial of service condition but also distract security operations personnel from other malicious activity such as the installation of backdoors or other advanced persistent threats (APT) tools designed to steal vital data. Another common attack technique is to probe an organization’s DDoS response capabilities using a series of short duration attacks over a longer period of time in order to craft a site-specific plan designed to circumvent existing DDoS protection solutions.

»

IP ServerOne's newest technology helps to mitigate these attacks without causing any trouble to your server performance by automatically blocking the attack with the 'Always On' feature, letting only legitimate traffic through with a peace of mind.

IP ServerOne DDoS Protection

We provide network-based, "Always-On" protection and with the assurance of 24 x 7 monitoring. Today's DDoS attacks are growing in size, frequency and complexity where no enterprise is immune to these threats. A smart and high-performance DDoS mitigation device has been deployed which is able to detect and mitigate immediately. Our service monitors all incoming traffic to our network and as soon as suspicious traffic hits, it will be flagged and sent to our own anti DDoS infrastructure automatically with reporting data and analytics. You may rest assure that we do protect you against attacks on any level; network (layer 3), protocol (layer 4), or application (layer 7):



Anti-DDoS diagram

DDoS Attack level

Name of attack	OSI level	Type of attack	Explanation of attack principle
ICMP Echo Request Flood	L3	Resource	Also called Ping Flood, mass sending of packets implicating the response of the victim, which has the same content as the original packet
IP Packet Fragment Attack	L3	Resource	Sending of IP packets that voluntarily reference other packets that will never be sent, which saturates the victim’s memory
SMURF	L3	Bandwidth	ICMP broadcast attack usurping the source address to redirect multiple responses to the victim
IGMP Flood	L3	Resource	Mass sending of IGMP packets (multi-cast management protocol)
Ping of Death	L3	Exploit	Sending of ICMP packets which exploit an implementation bug in certain operating systems
TCP SYN Flood	L4	Resource	Mass sending of TCP connections requests
TCP Spoofed SYN Flood	L4	Resource	Mass sending of TCP connections requests to usurp the source address
TCP SYN ACK Reflection Flood	L4	Bandwidth	Mass sending of TCP connections requests to a large number of machines, usurping the victim's source address. The bandwidth of the victim will be saturated by the responses to these requests
TCP ACK Flood	L4	Resource	Mass sending of TCP segment delivery receipts
TCP Fragmented Attack	L4	Resource	Sending of TCP segments that voluntarily reference other segments that will never be sent, which saturates the victim's memory
UDP Flood	L4	Bandwidth	Mass sending of UDP packets (not requiring a previously-established connection)
UDP Fragment Flood	L4	Resource	Sending of UDP datagrams that voluntarily reference other datagrams that will never be sent, which saturates the victim's memory
Distributed DNS Amplification Attack	L7	Bandwidth	Mass sending of DNS requests usurping the source address of the victim, to a large number of legitimate servers. As the response is more voluminous than the question, an amplification of the attack follows
DNS Flood	L7	Resource	Attack of a DNS server by mass sending of requests
HTTP(S) GET/POST Flood	L7	Resource	Attack of a web server by mass sending of requests
DDoS DNS	L7	Resource	Attack of a DNS server by mass sending of requests from a large set of machines which are under the attacker's control

Solution benefits

01 **Up-to 500Gbps of attack mitigation capacity**

02 **Automated and “Always ON” protection**

03 **Both local and international mitigations**

04 **Volumetric and Application layer attack mitigation.**

05 **Advanced behavioural analytics technology**

06 **In-house filtering for no added latency**

07 **Completely transparent to regular traffic**

08 **Prevent service disruptions during attacks**

09 **Having a detailed report after any kind of attack**

10 **Multi-level DDoS protection to ensure service availability**