imperva

DATASHEET

5 Reasons to choose Imperva DDoS Protection over the basic DDoS solution offered by your Internet Service Provider

With the increase in complex, multi-vector Distributed Denial of Service (DDoS) attacks and the ease with which DDoS-for-hire services are acquired today, the need for sophisticated DDoS protection is intensifying. DDoS attacks result in slow website response times and often prevent customers from accessing eCommerce, online banking, or other applications. Imperva Research Labs recently reported **DDoS activity increased by 286% between Q4 2020 and Q1 2021.**

While most organizations recognize the need for DDoS mitigation services, they may be uncertain as to who can deliver the most effective solutions. Many organizations rely on their internet service provider (ISP) for DDoS mitigation because this service often comes as a relatively low-cost add-on to the ISP's existing bandwidth offerings. While an ISP solution is readily available and inexpensive, the DDoS mitigation it provides as part of a service provider's package may not cover all of an enterprise's needs—and may even end up costing more in the long run. The better option often is a security-first vendor specializing in DDoS protection.

Most ISPs focus on their core computing services and consider DDoS protection a loss leader to promote higher sales. As a result, they may provide only the basic protections that cost them the least. These protections are unlikely to be sufficient for all the types of attacks an organization is likely to encounter.

Here are five reasons why you should choose Imperva DDoS Protection over the basic DDoS mitigation services provided by your ISP.

1. Prioritize your infrastructure when it's hit by a volumetric attack

The priority for an ISP is to protect its own infrastructure first and foremost. If they see large amounts of traffic going after a site or a network and they are unable to effectively scrub it, they may block all traffic to the site completely. In this way, the ISPs actually help attackers achieve their aim of shutting down the site.

For example, ISPs typically protect against network/transport layer (Layer 3/4) attacks that send out large UDP, ICMP, or other spoofed-packet floods to saturate the bandwidth of the attacked site. The magnitude of these attacks is measured in bits per second (bps). ISPs protect against these attacks by providing large pipes that can absorb large amounts of traffic. They also use filters and policers to stop DDoS traffic from reaching the site.

However, because these filters and policers are usually on-premises solutions, they allow the attack traffic to reach an organization's pipe before stopping DDoS traffic, which means large attacks can overwhelm the pipe, subsequently making your site unreachable as a result.

Imperva effectively protects a site against all types of attacks of all sizes and because our solutions work in the cloud, they spread the traffic over multiple ISPs and use multiple data centers to leverage massive amounts of bandwidth to absorb volumetric attacks.

2. Protect Against Protocol Attacks

ISPs are also often unable to protect against protocol attacks. These attacks, which include Syn floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more, consume actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and are measured in packets per second (PPS). Further, many standard DDoS services cannot protect against advanced DDoS attacks such as burst attacks, dynamic IP attacks, or multi-vector attacks. This leaves organizations exposed in the face of a sophisticated attacker.

To combat packet-based attacks, a DDoS mitigation vendor like Imperva examines the packets and identifies the protocols (e.g., Transmission Control Protocol (TCP), Network Time Protocol (NTP), Domain Name System (DNS)) they contain and compares that to normal traffic. When the packets for each protocol exceed a predetermined threshold, these solution providers block them and deliver only clean traffic to customers.

3. Fast Time to Mitigation

With every hour of downtime costing organizations tens of thousands of dollars in lost business, the faster the response time the better. In many cases, customers trust their ISP to provide a rapid response when under attack. Yet most free or low-cost DDoS protection from ISPs provides no service level agreement (SLA) at all or a "best effort" SLA that does not commit to attack detection times, mitigation times, or quality of mitigation. The result can be considerable disruption to business and substantial recovery costs. Imperval offers strict SLAs that include specific and measurable metrics for detection, mitigation, and response, and will also explain what service remedies they will take in case the SLAs are breached.

4. Consistent DDoS Protection Across the Globe

Many organizations use different ISPs for different regions or different countries. For example, they may use one ISP in Europe, one in Asia, as well as different ones for the East and West Coasts of the United States. Each of these ISPs will offer their own SLAs and services. Some ISP DDoS mitigation services will protect the line or link, others will also safeguard applications, web servers and DNS servers. The lack of consistent SLAs and DDoS protection services across ISPs makes it impossible for organizations to maintain a coherent DDoS security posture across their global operations. Because Imperva DDoS Protection services are cloud-based, we can provide global organizations with the same services and SLAs across all the ISPs they employ.

5. DDoS Mitigation Expertise

ISPs that provide basic DDoS protection don't specialize in DDoS security. Their expertise is in their respective fields (e.g., internet connectivity, content delivery, cloud computing). However, DDoS attacks are a specific category of cyberattack with distinct characteristics, customer impact, and methods of mitigation. ISPs may not be up to date with the latest attacks, trends or tools or have rich experience dealing with a wide variety of DDoS attacks. In contrast, Imperva mitigates DDoS attacks every day. We have dedicated teams with considerable expertise available 24×7×365 all focused on DDoS security.

With the number of DDoS attacks burgeoning and growing more complex, ISPs who provide inexpensive, but limited DDoS mitigation solutions may no longer meet the needs of a complex enterprise.

Imperva has the expertise to ensure that your organization is instantly protected against all types of DDoS attacks in a consistent manner across your global infrastructure. Imperva DDoS Protection secures all your assets, wherever they are, on premises or in the cloud, for optimal uninterrupted operations.

For more information on Imperva DDoS Protection visit:
imperva.com/products/ddos-protection-services