How to Evaluate DDoS Mitigation Providers: Four Critical Criteria

Akamai
FASTER FORWARD

TABLE OF CONTENTS

Introduction

Distributed Denial of Service (DDoS) attacks continue to make global headlines with ever-growing attack sizes and new attack methods. This dynamic and constantly changing threatscape has sparked an increased demand for mitigation services and with that an influx of service providers are entering the marketplace. However, because many of these services reside in the cloud it is often difficult for providers to assess, evaluate and differentiate DDoS mitigation service providers.

How can you be sure that the DDoS mitigation services provider you bring on board can deliver on the promise to stop the Internet's largest and most sophisticated attacks? This white paper explores four critical criteria on which to evaluate DDoS mitigation providers before signing on the dotted line. Akamai has developed key questions related to each to help you evaluate a provider's threat intelligence, experience, mitigation capabilities and capacity. Our guidance is based onAkamai's practical experience in proven mitigation approaches for different DDoS attack scenarios, as well as on our keen insight into the minds and strategies of cybercriminals and DDoS attackers.

Criteria #1: Threat Intelligence

The more you know about DDoS attacks — and how your DDoS mitigation service provider protects you against them — the more proactively you can manage your DDoS defense strategy. That is why it is so important to stay aware of the latest attack trends, new toolkit development and emerging cyber threats. Your mitigation service provider should provide you with comprehensive threat intelligence on a regular basis, compiled by a dedicated research team of DDoS security experts.

What to ask:

Do you have an internal DDoS threat intelligence research group?

The most credible DDoS mitigation service providers will have an internal research team of expert DDoS engineers that track the rapid changes in attack vectors and toolkits within the DDoS threat landscape. These researchers are key to proactively developing new mitigation strategies and attack countermeasures on a regular basis. The threat intelligence team should publish this intelligence for customers and the public on a regular basis — this will be a good indicator of the class of service provider with which you are dealing. Less sophisticated providers will rely on third-party information as well as off-the-shelf mitigation devices, which may require software updates in order to respond to changes in attack techniques. This type of threat intelligence is no match for information gained from the real-world experience of DDoS experts and technicians on the front lines, working against live attackers, with tools developed to match the threat landscape.

What threat intelligence do you publish and provide to your customers?

Ask to see the threat information the provider is publishing and making available to their customers. The reports should include regular write-ups on the latest DDoS toolkits, new attack vectors and innovative new attack defense measures. What the provider publishes will reveal how serious they are about research and, even more so, how much they invest in their infrastructure to ensure that they can mitigate the latest attack vectors and toolkits. The quality of the threat intelligence can help you determine the quality of the provider's service and how prepared they are to protect your network assets. If they rely only on third-party information, it is likely that they are poorly equipped to deal with emerging attack vectors.

Criteria #2: Front-Line Experience

Nothing beats first-hand experience when you're talking about defeating determined cyber hacktivist groups. These attackers not only challenge a provider's mitigation capabilities for its customers, but they also compel the provider to protect itself against the most malicious forms of cyberattacks. Experienced DDoS mitigation service providers will have evolved their network as a result of their collective experience in successful attack mitigation, making them much better prepared to deal with the unexpected or zero day type of DDoS event. A DDoS mitigation service provider is there for your protection and you depend on them to stop any and all DDoS attackers. They must be able to defend themselves against all types of cyberattacks.

What to ask:

How many years have you been providing DDoS protection service to the public?

Many vendors will try to include their years of in-house DDOS attack experience in their pitch. Protecting their own network, however, is very different than protecting other people's networks. Practice makes perfect, so the more attacks a provider experiences and mitigates, the more accomplished and resilient their network and attack countermeasures will be. Expertise in fighting DDoS attackers — and winning — can only be accomplished by many years of first-hand experience on the front lines against live attackers.

Do you have a large customer base supporting the cost of network and mitigation capacity growth?

A service provider's customer base can tell you a lot about their capabilities and capacity. A provider with a large customer base, including large Fortune 500 companies, likely has the revenue stream and profitability to support high bandwidth capacity as well as the capital to continue to invest and build out their capabilities and develop new countermeasures to emerging attack types. Is the service provider profitable? Small service providers with a small customer base or that have not become profitable will likely not be making the required reinvestment in bandwidth capacity and capabilities to protect you from all types and sizes of attacks.

Criteria #3: Mitigation Capabilities

Regardless of the size of your organization, you need a DDoS mitigation provider with a very robust capability set to defend against all types of current and emerging attack vectors, including the largest size of attack possible on the Internet. It's a fallacy that small companies require less protection than large ones. The fact is that DDoS attackers have used the same highly sophisticated toolkits to take down both the world's largest banks and small community credit unions.

In addition, one size of DDoS protection does not fit all businesses. Depending on the architecture of your network environment, you may need multiple technologies and tools to address particularly vulnerable assets. Therefore, look for a high-end DDoS mitigation services provider with a broad portfolio of capabilities that enables you to select which technologies and methodologies are most appropriate for your network protection today and as your needs change in the future.

What to ask:

What methods of traffic redirection do you support?

A good cloud-based DDoS mitigation service will offer both of the two main capabilities for redirecting web traffic during an attack. The first is based on BGP (border gateway protocol) route advertisement changes, the method by which all routers on the Internet exchange route information. This method of IP path-based redirection covers all ports and protocols, but requires a minimum of /24, which is the smallest route advertisement that can be made on the Internet. The alternative method is a proxy or DNS-based redirection, which is usually the choice for customers that don't have the minimum /24 required for BGP. DNS redirection can protect individual IP addresses and usually offers more robust capabilities for defending against Layer 7 (application layer) attacks. Depending on your network environment, you may have a hybrid architecture in which you need DDoS protection for the data center as well as for third-party cloud assets. Your DDoS mitigation services provider should have proven capabilities to defend it all.

Do you have options for both on-demand and always-on DDoS service options?

Look for a provider who offers both on-demand and always-on DDoS mitigation services to accommodate the broadest range of business requirements. Traditionally, DDoS mitigation services have been sold as on-demand protection, meaning that they were on stand-by and the customer routed traffic to the mitigation provider's cloud or network only when their network came under attack. In response to today's more complex DDoS threat landscape, mitigation services have evolved to the point where companies want to be always-on with all network traffic monitored by the mitigation provider. The always-on method has several advantages, such as faster speed-to-mitigation and improved network performance in some environments. Depending on what network assets you are protecting, the nature of your business and your tolerance for downtime, you may need a combination of both on-demand and always-on services. However, be sure to ask a lot of questions about network latency, traffic performance and the risk of false positives (blocking legitimate traffic by mistake) when considering an always-on service.

Can you protect my DNS servers even if they are located in a third-party hosted environment?

Most DDoS mitigation services can protect DNS servers hosted in your data center. However, many service providers are unprepared to deal with a large and sophisticated DDoS attack on DNS servers hosted in a third-party environment. Keep in mind that once you go to a third-party hosted environment you introduce the concept of shared risk — many customers in one DNS server environment. An attack on one customer causes an outage for the hosting provider; it is likely your business will also be impacted even though your company was not the target of the attack. As a result, it is critical to understand the DDoS mitigation capabilities of your DNS hosting provider because the risk of DDoS attacks is dramatically increased in a shared environment housing multiple customers. You may believe you are at relatively low risk of experiencing a DDoS attack, but your neighbors in the shared environment may actually be high risk.

Do you provide a time-to-mitigate Service Level Agreement (SLA)?

The only acceptable answer is yes. A time-to-mitigate SLA defines how quickly and effectively the service provider will stop a DDoS attack. Other SLAs are secondary and may cover only how quickly the provider will respond and call you back after you report an attack or how long it will take to route on to the service — and have nothing to do with how quickly the provider can stop the attack. Speed is critically important in DDoS defense, as a slow response means more downtime, potential loss of revenue and brand damage.

Do you provide any cloud security services beside DDoS?

Does your potential cloud security service provider offer other security services beyond DDoS, or does it only mitigate DDoS attacks? This question has become more and more relevant as companies move more assets to the cloud — they will require other security capabilities beyond just DDoS. In addition, the escalation of other cyber threats — phishing, data breaches, web application attacks and others — is driving the need for a complete suite of cloud security-service capabilities. Why? Redirecting traffic across the Internet to multiple cloud security providers can be quite complex when addressing multiple types of security issues simultaneously. Therefore, a single provider who can offer a complete portfolio of cloud security services can streamline web security and make it more cost effective.

What types of attacks have you successfully mitigated?

Don't be satisfied with just a list of attack types the provider says they can mitigate, ask to see actual documentation (that they should be releasing on a regular basis) which shows the types of attack, attack vectors and size of the attacks they have successfully mitigated. Your provider should be very transparent in publishing and sharing quarterly statistics with the general public on DDoS attacks they have actually encountered on behalf of their customers. If they are not sharing this data, it will be very difficult to judge their real-world experience and ability to stop DDoS attacks.

Do you offer a fully managed DDoS service? How do you drive the mitigation strategy?

Some hybrid DDoS mitigation service providers have recently emerged, providing self-directed access to a platform with basic mitigation capabilities. Not surprisingly, this is a high-risk approach. DDoS is still a highly specialized area, so you should choose a provider that can analyze traffic and provide a dedicated resource who is with you throughout the entire DDoS attack. Your provider should be the one who is directing the mitigation strategy, communicating with you throughout the event, verifying that over-mitigation is not taking place and refining and fine-tuning mitigation signatures on the fly. The best DDoS mitigation providers will be highly engaged and willing to customize their communications to integrate seamlessly with your incident response plan and can respond to and mitigate new zero-day DDoS attacks.

What types of redundancies are provided in each one of your network and mitigation platforms?

The most comprehensive DDoS mitigation service provider will use multiple network services platforms – BGP, proxy and DNS to address all of the risks associated with today's DDoS threat landscape. Ask about the redundancies and resiliencies of each platform, because each of the platforms is different and they all need to be reliable. For BGP, ask about data center redundancy and how your network traffic would be impacted if the data center were taken offline for maintenance or an attack. In regard to proxy service, you need to understand how many physical servers the provider has and how they are distributed. If one server fails, how does the traffic redirect to other servers? What backups are in place if DNS servers are attacked? And don't forget to ask about DNS redundancy and if the provider is offering an SLA on DNS platform uptime.

Criteria #4: Mitigation Capacity

Mitigation capacity is a key differentiator among DDoS mitigation service providers. The objective of all DDoS attacks is to exhaust your resources (bandwidth, memory and CPU for all devices that process traffic) to create a network or system outage and take down your online presence or applications. The largest expense item for credible DDoS service providers is the cost of bandwidth required to handle today's large DDoS attacks. There is a direct relationship between the amount of network and mitigation capacity provided and the cost of mitigation service. Services providing access to more resources are more expensive — it is that simple. But compared to the cost of purchasing hundreds of gigabits of bandwidth and millions of dollars of mitigation devices in addition to the potential lost revenue and brand damage done by DDoS attacks, the cost of quality services is reasonable.

What to ask:

What is the network and mitigation capacity for each one of your protection platforms?

All of the capabilities of your DDoS mitigation provider are irrelevant if attackers strike with a larger attack than the service's network and mitigation capacity can handle. Remember that reliable DDoS mitigation providers will have different mitigation platforms to deal with different attack vectors. Therefore, ask for the capacity or bandwidth size of each platform and confirm that the capacity of the specific mitigation platform protecting your network exceeds the Internet's largest known attack size. In addition, be sure that your provider continues to make investments in mitigation capacity to always stay one step ahead of new, larger and ever more damaging DDoS attacks.

Are there any fixed caps or fees associated with attack size or number of attacks?

There are many different pricing models in the marketplace, and some mitigation service providers are charging fees for DDoS attacks that exceed a defined size or number of attacks — while others may not. Remember that you have no control over the size and number of attacks that will hit your network. Also, keep in mind that both large global enterprises and smaller companies alike are being attacked using the same DDoS attack types and toolkits. Attackers steal resources from compromised devices, so the cost to them is always zero, regardless of if they launch a 1GB, 20 GB or 100 GB DDoS attack. Are you willing to have your service attack fee set at the discretion of the attacker? Consider fixed fees and attack caps carefully when comparing different mitigation service vendors.

How is your network and mitigation capacity distributed across the globe? Does the service use Anycast or a similar technology to distribute the attack traffic across multiple locations?

Breaking a DDoS attack into smaller segments and fighting them in multiple physical locations is a proven successful mitigation methodology. Providers who use Anycast or a similar technology can segment attack mitigation across the globe by utilizing multiple data centers simultaneously and fighting closer to the attack traffic's origin. This method prevents attack sizes from becoming so large that carriers feel compelled to drop the traffic, both malicious and legitimate. Therefore, breaking the attack into smaller segments allows the provider to scale up to very large size attacks. In addition, a globally distributed mitigation network provides redundancy.

Have you ever experienced a network outage due to a DDoS attack?

Some quick research on the Internet can give you the answer to this question if the service provider is not forthcoming. Check the provider's history of any outages or other incidents that have been reported or covered in the media. Keep in mind that if the service provider did not have the capabilities and capacity to keep their own network online, then they have definite issues with bandwidth or the design of their mitigation platform. Remember, your worst possible outcome is selecting an inferior DDoS mitigation service, paying their service fees and still experiencing downtime due to a DDoS attack.

What is the largest attack you've ever mitigated successfully on each of your protection platforms?

The answer to this question is the gold standard by which you can truly judge the capability of a DDoS mitigation provider. Marketing numbers can be manipulated. Therefore, ask to see graphs of the largest DDoS attack that the provider has successfully mitigated on each mitigation platform – BGP, proxy and DNS. If they don't have a graph of the largest attacks, this indicates that the attack likely exceeded the provider's capacity. If so, the provider was probably forced to rely on upstream blocking of the attack using ACLs by the provider's carrier. This approach can work, but the fact that the mitigation provider does not have enough capacity to block high-bandwidth attacks should raise a red flag. You should expect the provider to have the capacity to stop all sizes and types of attacks.

Have you ever denied service due to defending multiple simultaneous attacks?

The answer to this question should always be no. This is critically important as more new DDoS mitigation service providers begin to enter the marketplace. What is the provider's growth strategy and how do they approach capacity planning? Are they adequately provisioning and adding new bandwidth as their customer base grows? In addition, how many simultaneous large attacks can they handle? How do they prioritize and manage simultaneous attacks? The answers to these questions should give you confidence that your network will be fully protected regardless of how many DDoS attacks the provider is currently fighting.

Conclusion

Choosing a security services provider with DDoS mitigation expertise is one of the most important business decisions you can make — one that can cause serious financial and reputational damage if not made properly. Online businesses brought down by DDoS attacks can lose millions in sales as well as lost customer confidence and trust. This is also true for investor confidence — especially if news of the cyberattack or data breach hits the headlines.

Like a playground bully, DDoS attackers are very aggressive and smart, and they hone in on their opponent's weaknesses to get the upper hand. Cyberattacks unfortunately are a fact of life on the Internet, and online businesses must fight back. Your organization may have the latest cyber security technology and the best IT people, but the fact is that attackers still have you outnumbered with botnets and crowd sourcing capable of launching attack campaigns that can last indefinitely and change signatures daily. Fortunately, you do not have to fight this cyber war alone — but you must take a very serious and informed approach to choosing the right DDoS mitigation services provider who can successfully defend you on the front lines.