AT&T Solution Provider

Choosing a Provider for DDoS Protection

Introduction

Every day, we hear more about distributed denial of service (DDoS) attacks. As an equal opportunity threat, they can impact organizations of all sizes and across all industries, while disabling infrastructure resources, applications and business operations.

Given the high bandwidth capacity needed to handle today's volumetric attacks, the cost and complexity of DDoS protection, and the expertise needed to stay up to date on the latest threats, you may have decided not to tackle DDoS defense on your own. But how do you choose a DDoS defense provider that's right for your company?

The goal of this paper is to make you aware of the key "must have" capabilities your DDoS defense provider should be able to offer you. Use these qualifying questions to gather the knowledge needed to make a more informed decision, and to move forward with a more strategic approach to DDoS defense.

Qualifying Questions for Potential DDoS Defense Providers

How many years have you been fighting attacks on the network?
Defending your business against Internet threats demands a multi-layered approach to security. So, the question to ask isn't: "How long have you been handling DDoS attacks?" It really needs to shift to: "How long have you been defending the network?"

That's the benefit of buying DDoS defense services directly from a Tier 1 network service provider. They have been successfully mitigating network attacks for decades, well before anyone even heard of a DDoS threat.

> Broaden the question from "How long have you been handling DDoS attacks?" to "How long have you been defending the network?"

Further, fighting DDoS attacks is a natural extension of the network security protection and expertise they provide to their customers every day.

What visibility do you have into potential DDoS attacks?
Since Tier 1 providers own and operate vast global networks that transmit huge amounts of traffic every day, they have broader visibility into network activity than Tier 2 and Tier 3 ISPs have, as well as non-ISPs.

This gives them the capability to monitor, collect and analyze more network data to detect abnormalities that may indicate a potential DDoS attack, such as higher amounts of activity on a specific Transmission Control Protocol (TCP) port. They can also discover trends and patterns in suspicious activity by analyzing customer-specific Netflow data and use what they learn to increase DDoS detection and protection.

Do you have the network peering capacity to absorb massive DDoS attacks?
Peering refers to an agreement between two ISPs that their networks will be interconnected to exchange traffic. It is a way to extend network services to more customers and to expand bandwidth capacity, which is critical to warding off DDoS attacks. The more peering capacity your provider has, the better protected you can be.

> The more peering capacity your provider has, the better protected you can be.

This is due to the fact that the characteristics of DDoS events are changing. While these large attacks have grown in volume – capable of flooding your network with traffic exceeding hundreds of gigabits-per-second – they have shrunk in duration. This can be even more devastating, as it means your network has less time to react and scale and has more chance of being overwhelmed by the higher concentration of traffic.

Because Tier 1 providers own and operate their own network, they have more control over DDoS attack mitigation. Further, the extensive peering relationships they have with other providers, combined with the breadth and scale of their own network, means they have the peering capacity to absorb attacks of tremendous size and magnitudes without major service disruptions. Direct connections with peering partners reduce latency, which decreases mitigation times and the time to deliver scrubbed traffic to your network.

DDoS defense providers: How are they different?

While there are no industry-standard definitions for Internet Service Providers (ISPs) or other companies that offer DDoS protection, these are some general differences between them:

Tier 1 ISPs
Operate and control their own IP network. They have direct connections to the global Internet backbone to reduce latency.

Tier 2 ISPs
Typically cover specific regions. To extend reach to other portions of the Internet, they tend to purchase bandwidth from Tier 1 providers.

Tier 3 ISPs
May focus on specific regions and markets. Typically depend solely on Tier 1 ISPs to reach the Internet. Prices can be less, but network speed and reliability can be relatively low.

Non-ISP providers
Companies that offer DDoS protection who may or may not be Tier 2 or Tier 3 providers. They typically rely on Tier 1, Tier 2, or Tier 3 providers for their Internet access and may require on-site equipment or configurations.

What happens if a DDoS attack occurs?
The goal is to proactively eliminate DDoS attacks at the network edge, before they penetrate your private network. If a DDoS attack is detected, your solution should be able to block malicious packets in real-time, without diverting traffic destined to non-attacked hosts.

To do so, traffic that is directed to the server under attack needs to be diverted to a scrubbing facility for cleaning first. To reduce latency, the traffic should not have to be sent across the country for scrubbing.

Instead, your provider should have multiple scrubbing centers with very high bandwidth capacity, strategically located directly at the peering points that connect their network with the networks of other Internet providers. In that way, attacks can be mitigated at that point of entry, before making their way into the core network.

> Help block DDoS attacks at the network edge before they make their way into the core network.

Since all DDoS attempts are different, with some attacking volumetrically and others exploitingTransmission Control Protocol or TCP ports, your provider should have an arsenal of DDoS tools available to detect and combat varying types of events. As the attacker

reacts in real-time to the defensive measures put in place, those tools must be able to adapt to the scope of the attack or to the change in vectors, as the incident progresses.

How do you prevent scrubbed traffic from being exposed to further risks?
Once the traffic is scrubbed, you can still be vulnerable to further threats. This is because some DDoS protection providers send scrubbed traffic over a generic routing encapsulation (GRE) tunnel, which requires the use of the public Internet. The publicly accessible IP address on your end of the tunnel is a risky point of exposure. Smart attackers know they can target your router IP address to launch another DDoS attempt.

Transmitting scrubbed traffic over the public Internet increases the risk of further DDoS attack exposure.

If you choose a Tier 1 network provider for DDoS protection services, they have more control over how and where traffic flows. For example, to prevent Internet-facing exposures, they can use a Virtual Private Network (VPN) to transport data from the scrubbing centers to your routers.

What support do you provide during an attack?
With the business disruptions a DDoS attack can cause, your provider needs to do more than just restore access to valid traffic, they must restore your peace of mind. So, beyond just notifying you of a high-alert attack, your provider should offer you live phone support during an event.

Since many incidents are being perpetrated in real-time by attackers, the characteristics of an event can change at any point during the attack. On-going, interactive communication between you and your provider can help confirm the DDoS protection in place is effectively doing its job of stopping malicious traffic, while allowing valid traffic through.

Is any on-premises equipment required?
If you've made the decision to work with a service provider, your decision was probably driven by the desire to reduce or eliminate on-site equipment to decrease cost and complexity.

Be aware that some non-ISP providers require you to install on-premises solutions, or to configure your WAN router to allow DDoS protection to work for you. This leaves your staff with the added responsibility of maintaining and supporting the equipment, a task and labor cost you may not have expected to incur when outsourcing your DDoS protection.

Cloud services embed DDoS safeguards into the network, eliminating the need for on-premises equipment.

That's why there is a trend in the industry towards security and DDoS defense in the cloud. With protection in the cloud, DDoS safeguards are embedded in the network, so you can avoid staff and capital equipment investments for on-premises mitigation and take advantage of more flexible usage-based pricing plans.

Conclusion

With DDoS attacks becoming larger and more sophisticated, your chosen DDoS defense provider must have the experience, visibility and bandwidth capacity for early and proactive detection and swift mitigation of volumetric DDoS attacks.

As a Tier 1 network provider, AT&T owns one of the largest global networks. Because of that scale, our private peering with 23 major IP backbones, and our highly redundant network, we are in a better position to absorb and defeat DDoS attacks for our customers.

As part of our network security and DDoS defense services, we monitor and analyze petabytes of network activity every day. With the investments made in adaptive tools, robust analytics and five scrubbing complexes, we have the ability to dynamically help block DDoS attack traffic at the peering perimeter before it enters the network core. Scrubbed traffic flows to your network via a VPN. Since AT&T DDoS Defense Service is delivered via the cloud, security is embedded into the network, with no requirements for on-premises equipment.

With more than 100 years of experience securing the AT&T network, approximately 2000 security experts, and the collaborative efforts or our security and network operations teams to correlate and fight DDoS attacks, it makes sense to choose AT&T as your DDoS defense provider. And, you don't have to be an AT&T network customer to take advantage of AT&T DDoS Defense Service.

For more information about AT&T DDoS Defense part of your multi-level approach to network protection, talk to your AT&T Solution Provider.

09/12/14 AB-2998

AT&T Solution Provider