HYBRID DDoS DEFENSES

COMPLETE SERVICE PROVIDER DDoS MITIGATION SOLUTION

NSFOCUS provides a Complete Service Provider DDoS Mitigation Solution that protects both customers and infrastructure; while enabling providers to deliver Managed DDoS Services with a multi-tenant Platform that produces the lowest operating costs in the industry.

Integrated Hybrid Solution

- Fastest-time-to-mitigation

Easy Management with Strong Automation

- Lowest operating cost for complete solution

Multi-Tenant Design Out-of-the-Box

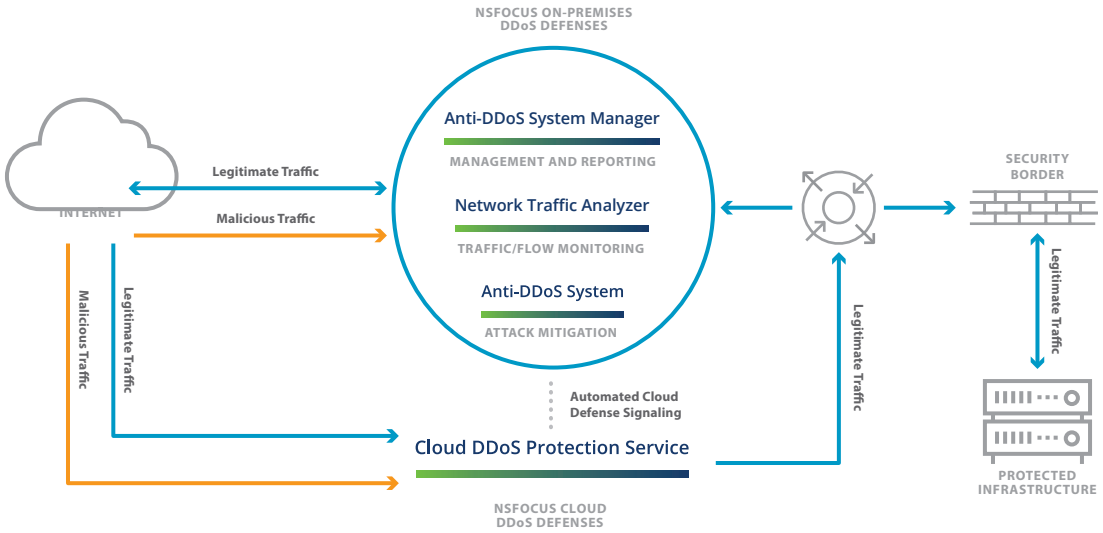
- Prebuilt customer portal, policies, configurations

THE DDoS SOLUTION PROVIDERS NEED – TO OFFER MANAGED DDOS SERVICES

Nearly all industry experts recognize the fact that defeating the broad spectrum of DDoS attacks requires more than just cloud DDoS defenses, and more than just on-premises defenses. It requires both. From volumetric DDoS attacks to low-and-slow DDoS attacks, the best approach to defeat all DDoS attacks requires a combination of on-premises defenses and cloud defenses – called *Hybrid DDoS Defenses*. This approach defeats all DDoS attacks regardless of their size, duration, or frequency.

HYBRID DEPLOYMENT SCENARIO

PROTECT YOUR CUSTOMERS WITH ON-PREMISES DDoS DEFENSES



PROTECT YOUR INFRASTRUCTURE WITH CLOUD DDoS DEFENSES

WHY HYBRID DDoS DEFENSES

When Hybrid DDoS Defenses are implemented, the on-premises defenses deployed in your network are completely capable of *defeating attacks against customers* – up to the point of the your Internet capacity. This is the only limitation to defeating all DDoS attacks, on-premises. If the your capacity is nearly consumed by a massive attack, then cloud defenses must be engaged to *defeat attacks against infrastructure*.

NSFOCUS

BENEFITS

Complete service provider-ready solution

Defeats attacks against your customers and infrastructure

Lowest total cost of ownership (TCO)

Wholly owned single-vendor solution

All-in-one solution, multi-tenancy enabled

Versatility of deployment options

Automated and reliable DDoS mitigation

Low false positives, high performance

Easy to integrate and cohabitate

Network agnostic technology

KEY FEATURES

Automatic hand-off with NSFOCUS Cloud Centers

Shortens time to redirection and cloud mitigation

Flexible connectivity for clean traffic re-injection

Low network latency for effective mitigation

Always-on, on-demand, flat-rate cloud pricing

NSFOCUS

RECOMMENDATIONS FOR MANAGED DDoS SERVICES

Many providers view DDoS attacks as a costly expenditure. Not only are providers required to defend their own infrastructures from massive attacks, but also DDoS attacks threaten the primary "service" providers deliver, which is Internet connectivity. However, there has been a shift in thinking recently whereby providers are beginning to understand that DDoS attacks can be a business enabler. Transferring the costs associated with DDoS attacks to their customers is beginning to make a great deal of sense to providers all over the globe.

As mentioned previously, studies indicate that organizations today would like to see their provider offer DDoS defenses as part of their service offerings. In addition, those same studies indicate that nearly fifty percent of organizations would be willing to purchase Managed DDoS Services for a nominal fee added to their monthly bandwidth premiums. Simply put, service providers are in the perfect place to protect customers, while protecting their infrastructures and services – and profiting from it. NSFOCUS can prove that offering Managed DDoS Services can be revenue-generating.

The recommendation for any provider who desires to offer Managed DDoS Services, must recognize that a combination of integrated defenses is required. NSFOCUS cloud and on-premises defenses work in concert, are completely aware of each other, and are in constant communication. In addition, having both defenses in place reduces the need to engage the cloud for sub-saturation attacks against customers. In other words, if the attacks are smaller in size they can easily be defeated by the on-premises defenses, regardless of their duration or frequency.

Another reason for both defenses is all about protecting the provider's SLAs. If a commercial customer desired to purchase Managed DDoS Services from a provider, they would require that every DDoS attack incurred must be defeated; with little or no impact to the customer, as well as the provider's infrastructure, per the SLA. It's not an either-or equation – both defenses are required to ensure DDoS Defense SLAs are met in nearly every case.

Tier 1 service providers with vast infrastructures and massive amounts of peering bandwidth can obviously defeat large-scale attacks in "their cloud" by deploying DDoS defenses within their own infrastructures. They often operate like a cloud DDoS provider themselves. Today, smaller service providers (Tier 2, 3) and hosting providers can easily do the same. NSFOCUS has many providers who are customers, that offer Managed DDoS Services quite successfully.

Not only can smaller providers deploy their own DDoS defenses on-premises to be offered as a service to their customers, they can also partner with someone who already offers cloud DDoS defenses, for example NSFOCUS. If smaller providers feel they are not ready to deploy on-premises defenses, they can easily "resell" services they obtain from NSFOCUS. Since NSFOCUS offers always-on, on-demand, and flat-rate pricing for their cloud, the possibilities are endless for even the smallest providers.

Although the potential service margins may be smaller when providers resell someone else's service, there's no reason they can't private label the service, or even add additional value by acting as a trusted intermediary between the cloud DDoS provider and the end-customer. Service providers already have a usage and billing infrastructure in place, and are closer to the customer than the cloud DDoS provider. The possibility of offering a one-stop-shop for cloud DDoS defense is a reality for smaller providers, even without owning their own on-premises DDoS defenses.

All providers must fully understand they are not normally the target of DDoS attacks. In most cases their "customers are the target". If providers can defeat all DDoS attacks targeting their customers, they should be able to recognize a return on their investment for doing so. Not only can providers recognize new revenue streams by defeating DDoS attacks, they can also insure attacks do not impact their own infrastructures and their services as a side benefit.

Another interesting aspect of solving the DDoS problem, especially concerning commercial "bandwidth and hosted" customers, is that many are being forced to purchase cloud-based anti-DDoS services from a third party. The reason for this is simple. Customers are experiencing DDoS attacks against their businesses, yet their service providers and hosting providers are not offering solutions to defeat DDoS attacks. In this case, the potential revenue opportunity for providers is going to someone else; since their commercial customers have no other options.