Using Arbor Cloud to Protect Multi-Cloud and Hybrid Environments Against DDoS Attacks

The enterprise trend of digital transformation – migrating digital assets from on-prem data centers to hosted cloud environments – has been underway for several years. Not only are enterprises migrating their assets to the cloud; often they are using more than one cloud hosting provider. But these enterprises are not migrating all their assets to the cloud. Most are opting to keep at least some assets in their own data centers. This approach has business advantages but can make for a complex distributed environment with increased security risks, especially when it comes to protecting critical assets against DDoS attacks. A single-sourced integrated protection solution is a compelling strategy to offset this hybrid environment risk.

The Looming Threat

Hosting a web service or other asset in the cloud does not make it less susceptible to DDoS attacks. Often, the assets hosted by the cloud provider are customer- or employee-facing. As a result, any downtime can be very costly. More important, an outage – especially a customer-facing one – can incur significant reputational damage and bad publicity. Securing cloud environments against DDoS attacks has become more critical than ever.

Complicating matters is the fact that modern DDoS attacks are dynamic, multi-vector, and span layers 3-7. Simply blocking high-volume layer 3 attacks typically is not sufficient and will not defend against the newer and more damaging types of attacks.

Some cloud hosting providers offer DDoS protection services, but these are often rudimentary and inadequate against modern multi-vector attacks. These one-size-fits-all services are also less effective in multi-cloud environments that can require a wide range of tailored protections.

Many enterprises use third party content delivery networks (CDNs) to deliver traffic to cloud-hosted services. These commercial CDNs usually offer a DDoS protection service as well. But like cloud hosting providers, the protections tend to address volumetric layer 3 attacks and are less effective against dynamic multi-vector, multi-layer attacks. These services also may lack a dedicated SOC team capable of partnering with the enterprise to insure a timely response and maximum effectiveness during mitigations.

The Myth of the Safe Cloud

Enterprises may have excellent on-premises protection in their data centers, but they may assume this level of protection is no longer needed or possible once they migrate services to the cloud. Neither of these assumptions are true, nor will the cloud inherently provide comprehensive protection against modern DDoS attacks.

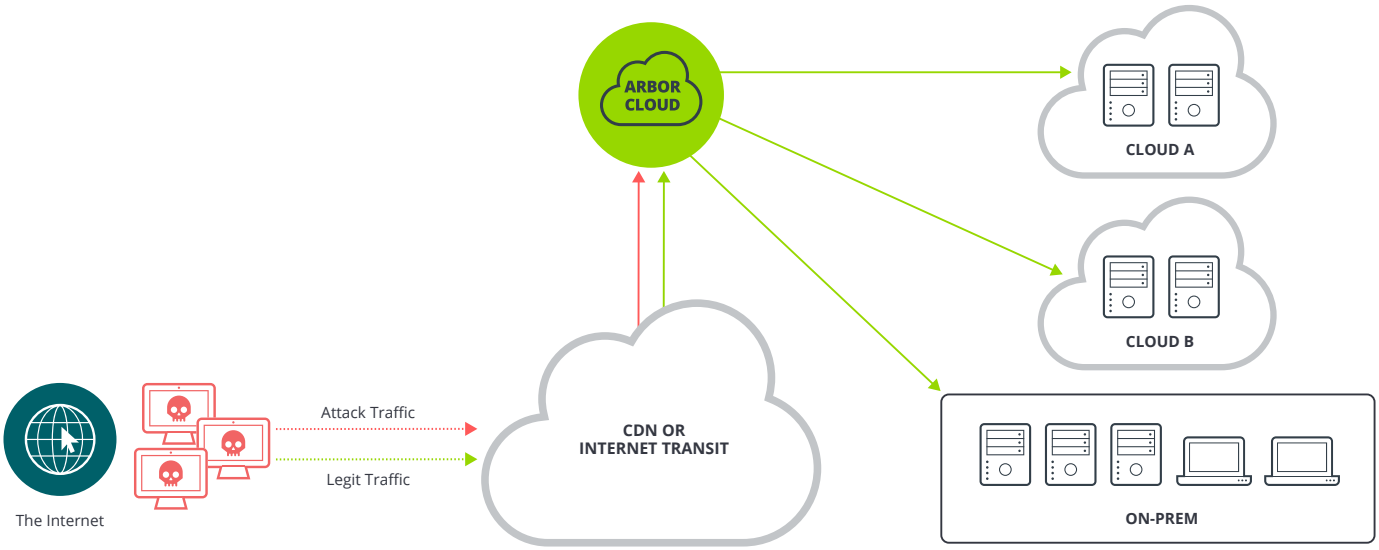

Figure 1: Arbor Cloud protection for hybrid and multi-cloud environments.

A Better Solution

Comprehensive DDoS protection remains critical and achievable before, during and after a cloud migration. Arbor Cloud® provides a single consistent service for protection against all types of DDoS attacks regardless of how digital assets and services are deployed across hybrid, multi-cloud environments. Whether traffic is delivered directly from the internet or via a CDN, Arbor Cloud detects, intercepts, and mitigates DDoS attack traffic, returning only clean traffic to its destination.

On-demand Protection

The Arbor Cloud service can be used on-demand whenever critical assets come under attack and regardless of where they are deployed. For cloud-hosted assets using hosting provider IP addresses, DNS can be used to redirect the affected traffic to Arbor Cloud for mitigation. This traffic can by routed directly to Arbor Cloud from a CDN or from the internet in general.

It is also possible for an enterprise to bring their own IP address space to public cloud providers like AWS and Azure. This allows standard BGP routing to be used to redirect traffic to Arbor Cloud on a global basis. This approach also enables an enterprise to deploy a virtual router in their VPC and set up a Generic Routing Encapsulation (GRE) tunnel termination for receiving clean traffic from Arbor Cloud.

Always-on Protection

Arbor Cloud can also be used in always-on mode. During peacetime, traffic for critical assets is routed to and through Arbor Cloud via DNS or BGP. When an attack occurs, Arbor Cloud automatically detects it within seconds and redirects traffic destined for the attacked hosts to the Arbor Threat Mitigation System™ (TMS) platform running in Arbor Cloud's distributed scrubbing centers.

Summary

Arbor Cloud provides a superior means for protecting critical assets hosted in a single or multi-cloud environment, offering several advantages over less capable protection services:

- Built on Arbor Sightline and TMS, the world's leading DDoS defense solution.
- Leverages NETSCOUT's ASERT Intelligence Feed (AIF) for the most complete and up-to-date global intelligence on current DDoS attack activity and sources, acquired from monitoring over half of the world's internet traffic.
- Globally distributed scrubbing centers to mitigate attacks closest to the source.
- Superior level of service and support from the Arbor Cloud SOC, staffed 7x24 with seasoned industry experts dedicated to DDoS detection and mitigation, including hands-on management of mitigation events.
- Personalized white-glove service: from onboarding to customizing configurations for each deployment, to coordinating mitigation events, to post-event reviews and service reviews to ensure optimal effectiveness and readiness.
- Customization of mitigation templates with support from SOC experts.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECUC_025_EN-2401 02/2024